

GLOBAL INFORMATION SOCIETY WATCH 2014

Communications surveillance in the digital age



ASSOCIATION FOR PROGRESSIVE COMMUNICATIONS (APC)
AND HUMANIST INSTITUTE FOR COOPERATION WITH DEVELOPING COUNTRIES (Hivos)

Global Information Society Watch

2014

Steering committee

Anriette Esterhuysen (APC)
Loe Schout (Hivos)

Coordinating committee

Monique Doppert (Hivos)
Valeria Betancourt (APC)
Mallory Knodel (APC)

Project coordinator

Roxana Bassi (APC)

Editor

Alan Finlay

Assistant editor, publication production

Lori Nordstrom (APC)

Proofreading

Valerie Dee
Stephanie Wildes

Graphic design

Monocromo
info@monocromo.com.uy
Phone: +598 2400 1685

Cover illustration

Matías Bervejillo

Financial support provided by

Humanist Institute for Cooperation with Developing Countries (Hivos)



Global Information Society Watch
Published by APC and Hivos
2014

Creative Commons Attribution 3.0 Licence
(creativecommons.org/licenses/by-nc-nd/3.0)
Some rights reserved.

ISSN: 2224-5162
ISBN: 978-92-95102-15-6
APC-201408-CIPP-R-EN-P-206

Printed in Uruguay

Table of contents

Preface 7
[Edwin Huizing, \(HIVOS\) and Anriette Esterhuysen \(APC\)](#)

Introduction 9
[Gus Hosein - PRIVACY INTERNATIONAL](#)

A principled fight against surveillance 11
[Katitza Rodríguez - ELECTRONIC FRONTIER FOUNDATION](#)

Thematic reports

Digital surveillance19
[Elijah Sparrow - LEAP ENCRYPTION ACCESS PROJECT](#)

The myth of global online surveillance
exempted from compliance with
human rights 25
[Alberto J. Cerda Silva](#)
UNIVERSITY OF CHILE LAW SCHOOL AND ONG DERECHOS DIGITALES

The harms of surveillance to privacy,
expression and association 29
[Jillian York - ELECTRONIC FRONTIER FOUNDATION](#)

Cyber security, civil society and vulnerability
in an age of communications
surveillance 32
[Alex Comninos and Gareth Seneque](#)
JUSTUS-LIEBIG UNIVERSITY GIESSEN AND GEIST CONSULTING

From digital threat to digital
emergency41
[Fieke Jansen, HIVOS – THE DIGITAL DEFENDERS PARTNERSHIP](#)

Intermediary liability and state
surveillance 45
[Elonnai Hickok - CENTRE FOR INTERNET AND SOCIETY \(CIS\) INDIA](#)

Unmasking the Five Eyes’ global
surveillance practices 51
[Carly Nyst and Anna Crowe - PRIVACY INTERNATIONAL](#)

Country reports

Introduction 57

Argentina 60
[Nodo TAU](#)

Australia 64
[Andrew Garton](#)

Bahrain 69
[Ali Abdulham](#)

Bangladesh 72
[Bytes for All Bangladesh](#)

Bolivia 76
[Fundación REDES](#)

Bosnia and Herzegovina 79
[OneWorld Platform for Southeast Europe \(OWPSEE\) Foundation](#)

Brazil 83
[Brazilian Institute for Consumer Defense \(Idec\)](#)

Bulgaria 86
[BlueLink.net](#)

Burundi (East Africa region) 90
[Collaboration on International ICT Policy in East and Southern Africa \(CIPESA\)](#)

Cameroon 94
[PROTEGE QV](#)

Canada 98
[Alternatives](#)

Chile 102
[ONG Derechos Digitales](#)

China106
[Danwei](#)

Colombia 110
[Colnodo](#)

Congo, Republic of 114
[AZUR Développement](#)

Costa Rica	117	Poland	198
Cooperativa Sulá Batsú		Panoptikon Foundation	
Egypt	121	Romania	202
Leila Hassanin		StrawberryNet Foundation and Sapientia	
Ethiopia	125	Hungarian University of Transylvania	
Ethiopian Free and Open Source Software			
Network (EFOSSNET)		Russia	206
Gambia, The	129	Oliver Poole	
Front Page International		Rwanda	210
Hungary	133	Emmanuel Habumuremyi	
Éva Tormássy		Senegal	214
India	137	JONCTION	
Digital Empowerment Foundation (DEF)		Serbia	217
Indonesia	141	SHARE Foundation/SHARE Defense	
Jamaica	143	Slovak Republic	220
University of the West Indies		European Information Society Institute (EISI)	
Japan	147	South Africa	224
Japan Computer Access for Empowerment		Department of Journalism, Film and Television,	
Jordan	151	University of Johannesburg	
Alarab Alyawm		Sudan	228
Kenya	155	Liemia Eljaili Abubkr	
Kenya ICT Action Network (KICTANet)		Switzerland	232
Korea, Republic of	159	Communica-ch	
Jinbonet		Syria	236
Kosovo	163	Karim Bitar	
FLOSSK		Thailand	240
Lebanon	166	Thai Netizen Network	
Mireille Raad		Tunisia	244
Mexico	169	Afef Abrougui	
SonTusDatos		Turkey	248
Nepal	174	Evin Barış Altıntaş	
Development Knowledge Management		Uganda	252
and Innovation Services Pvt. Ltd.		Women of Uganda Network (WOUGNET)	
New Zealand	178	United Kingdom	256
Association for Progressive Communications		Open Rights Group	
(APC) and Tech Liberty		United States of America	262
Nigeria	182	Access	
Fantsuam Foundation		Uruguay	267
Pakistan	185	DATA	
Bytes for All		Venezuela	270
Peru	190	Escuela Latinoamericana de Redes (EsLaRed)	
Red Científica Peruana and Universidad		Yemen	276
Peruana de Ciencias Aplicadas		Walid Al-Saqaf	
Philippines	193	Zimbabwe	280
Computer Professionals' Union		MISA-Zimbabwe	

Preface

The internet is a critical way to push for the progressive realisation of people's rights – but, through communications surveillance, its potential to be used as a tool for collective, democratic action is slowly being eroded. Users have even lost trust in it as a safe platform for day-to-day personal communications.

Using the 13 International Principles on the Application of Human Rights to Communications Surveillance as a basis, this Global Information Society Watch (GISWatch) considers the state of surveillance in 57 countries. Eight thematic reports frame the key issues at stake.

As the reports show, both states and businesses are complicit in communications surveillance. While there is a need for systems to monitor and protect the public from harm, the right to privacy, the transparency and accountability of states and businesses, and citizen oversight of any surveillance system are important advocacy concerns.

These 13 Principles are an important starting point for civil society to achieve this collective action – to push action for democratic oversight of surveillance. We hope this issue of GISWatch contributes towards this change.

Edwin Huizing

EXECUTIVE DIRECTOR, HIVOS

Anriette Esterhuysen

EXECUTIVE DIRECTOR, APC

Introduction

Gus Hosein

Executive director, Privacy International
www.privacyinternational.org

The extent to which we communicate is part of what makes us human. The quest to articulate our needs, desires, interests, fears and agonies motivated drawing, the gesture, the spoken word and its written form. Conversations led to letters, couriers led to the post, followed on by telegraphs, telephones, mobiles and internet working. We now relay our most intimate thoughts and interests over communications media. Yet with new revelations and innovations, we are seeing the growing ambitions of governments and companies to track, monitor, analyse and even monetise the communicative actions that are core to our being. To protect human autonomy in modern society, it is essential for us to govern communications surveillance.

Social and technological changes have increased the power and pervasiveness of surveillance. First, nearly everything we do today is a communicative act that is digitally observable, recordable, and most likely logged, and analysed from the earliest of stages, retrospectively, and in real time. Even our movements are logged by service providers.

Second, unlike our ephemeral spoken words amongst friends in a room, nearly every communication can now be collected, analysed, retained and monetised. It is now possible to capture the communications of an entire nation – the modern equivalent of listening to every private and public conversation in rooms, in homes and offices, town halls, public squares, cafés, pubs and restaurants across the nation.

Third, every communication generates increasingly sensitive metadata – data related to the communications – that is captured, logged, rendered accessible, and mined to draw lists of suspects and targets, and to understand our relationships and interactions.

Fourth, nearly every communication today involves a third party – the post office, the mobile phone company, the search engine, and the under-sea cable company, who are likely to be tasked with surveillance on behalf of the state.

Fifth, all of this surveillance can now be done in secret – the tampered envelope is now replaced with perfect, secretive replications of communications, captured at a number of points in a network.

Because of these structural changes to communications and the ways we live our lives, there is a new urgency to govern the capabilities of governments to trample on privacy.

- Following us or knowing everywhere we have been is now possible, as our mobile phones routinely connect with nearby mobile phone cell towers. Governments seek to access these logs even as companies seek to data-mine the information for profiling and “big data” analyses.
- Web surfing, the modern equivalent of a walk down the high street and around the public square, is now monitored by analytics companies and, in turn, governments. Both are keen to understand our interests and desires. Consequently, identifying everyone at a public event or in a given area now requires only accessing records from nearby cell towers, or even launching a police-run mobile base station that identifies every proximate mobile device. The powers of “stop and show your papers” will be replaced with the automated and secretive deployment of device scanners.
- While we previously needed secret police and informants to identify people’s known associates, governments can routinely generate lists of relationships and track interactions by monitoring our communications metadata from chat, text messaging, social networks, emails, and of course, voice communications. This also helps generate lists of previously unknown suspects or targets. “Guilt by association” could be assessed by who you follow on Twitter, and friends of friends on Facebook.
- And whereas before governments needed to train spies to infiltrate our friendships and other networks, and to search our homes and go through our files, they can merely compromise our computers and mobile phones, surreptitiously turn on our cameras and microphones, and gain access to all our correspondence, documents, images and videos, and even passwords.

Despite all these dramatic changes in capabilities, unprecedented in the history of surveillance and technology, governments are every day seeking to establish new and greater powers, complaining that they are losing capabilities, or “going dark”. Yet this is the golden age of surveillance. It is made possible by ambitious intelligence agencies and police services, poorly regulated by politicians who are resistant to understanding technology and human rights. It is spurred by a surveillance industry that develops and sells new technologies to governments across the world. And it is enabled by companies who fail to secure our communications infrastructure, acquiesce to government demands, and do not resist bad policy that make available for access ever larger stores of information on us, generated to profit from our relationships with our friends, families and colleagues.

We must not presume that this is only about communications privacy. As nearly everything involves communication in modern society, communications surveillance can itself generate previously unseen power for the watchers over the watched: individuals, groups and even societies. Because of this, the true debate over surveillance resides in questions of the rule of law: Are some institutions and capabilities above such a totemic principle? When it comes to modern governance, how do our existing governance structures meet the challenges of a new increasingly interconnected society? Or national security: Can effective and identifiable lines be drawn around such an amorphous concept to give clarity to the public?

We have barely scratched the surface on any of these questions, and within all of this we find ourselves racing to the future where the boundaries of privacy will be further tested, innocuous information increasingly revelatory, and the power to surveil increasing in its power and scope.

Nonetheless, I believe that in an open and democratic debate, societies will choose to regulate such power. The challenge is that the debate must be forced upon our governments. Fortunately we now have evidence of some of their secret capabilities, thanks to the incredible contribution from

Edward Snowden, and due to investigations into the surveillance industry that markets new capabilities to governments. We must now act upon this knowledge. We must engage with regulators to ensure that they are aware of the weaknesses in their regulated industries.

We must reach out to the legal community so that they understand the risks that surveillance poses to the justice system and the rule of law. We need to work more with technology communities so that they are inspired to build more secure and privacy-enhancing systems. The media and civil society organisations need to be made aware of how surveillance is targeted at journalists and agents of change. We must engage with industry so they understand the dangers of their choices over design of technologies and services and the limited autonomy they provide customers that set new standards for abuse by others. And parliamentarians and policy makers must be informed of the very real roles we expect them to play in the regulation of agencies and the safeguarding of the right to privacy of their citizens. Regulatory structures should never be created to act as false flags of legitimacy: rubber stamps have never been acceptable as a form of regulation, and yet the public is being faced with committees and courts operating in exactly that way.

Ultimately the debate around how to regulate such power requires a public presence within it. Society relies on its members to represent its best interest. The answers to these puzzling and fundamental questions are within us – no one else is going to force the government to understand our needs and expectations other than ourselves. Quite possibly the most important regulatory role lies with the public in guaranteeing that those who watch the watchers know that they are not doing so in isolation. Transparency is a core goal to all of this. Vigilance over the operation of all structures cannot waver: from the intelligence agency in its operations, to the court that authorises its operations, to the committee that oversees the powers and processes to access such power. At the top of this pile is the public: hawkish in its oversight and loud in its judgment.

A principled fight against surveillance

Katitza Rodríguez

Electronic Frontier Foundation
www.eff.org

Years before Edward Snowden leaked his first document, human rights lawyers and activists were concerned about a dramatic expansion in law enforcement and foreign intelligence agencies’ efforts to spy on the digital world. It had become evident that legal protections had not kept pace with technological developments – that the state’s practical ability to spy on the world had developed in a way that permitted it to bypass the functional limits that have historically checked its ability to spy. These concerns culminated in the International Principles on the Application of Human Rights to Communications Surveillance,¹ a set of principles intended to guide policy makers, activists and judges to better understand how new surveillance technologies have been eating away at our fundamental freedoms and how we might bring state spying back in line with human rights standards.

Over a year and a half in the making, the final version of the Principles appeared on 20 July 2013, in the first weeks of what we might call the Snowden era. An updated version was issued in May 2014. The Snowden revelations, once they started rolling in, affirmed the worst of our concerns. Intelligence services as well as law enforcement had taken it upon themselves to spy on us all, with little consideration for the societal effects. Lawmakers and even the executive had little comprehension of the capabilities of their own spymasters, and how our digital networks were being turned against all individuals everywhere. The need for the Principles was confirmed in spades, but the long and difficult job of applying them to existing practices was just beginning.

Since then, the Principles have, we hope, been a lodestar for those seeking solutions to the stark reality exposed by Snowden: that, slipping through the cracks of technological developments and outdated legal protections, our governments have adopted practices of mass surveillance that render many of our most fundamental rights effectively

meaningless. The Principles have been signed by over 470 organisations and individual experts, and have played a central guiding role in a number of the rigorous debates on the need to limit states’ increasingly expansive surveillance capacities. Their impact is already evident in, for example, the US president’s Review Group on Intelligence and Communications Technologies report, the Inter-American Commission on Human Rights report² and the Office of the United Nations High Commissioner for Human Rights’ recent report on the right to privacy in the digital age.³ Their influence has also manifested in some of the administrative and legislative attempts to address surveillance problems post-Snowden. Perhaps most importantly, they have functioned as a rallying point for campaigning and advocacy initiatives around the world.

Below, we spell out some of the key features of the Principles. A more detailed explanation of the legal grounding for our conclusions in human rights jurisprudence can be found in a Legal Analysis and Background Materials document generated in support of the Principles.⁴

Core definitions in international human rights law

The Principles begin with defining two core concepts that spell out the “what” and the “how” of measured surveillance. The first concept focuses on the type of data to be protected, while the second one ensures that a broad range of surveillance activity constitutes an interference with privacy rights. Outdated definitions of these two terms have led to expansive surveillance practices, as wide swaths of sensitive data or surveillance activities have been deemed outside the scope of legal protections. These definitional changes are designed to re-focus privacy protections away from artificial examinations of the kind of data or method of interference, and back on the ultimate effect on the privacy of the individual.

² www.oas.org/en/iachr/expression/docs/reports/2014_04_22_%20IA_2013_ENG%20_FINALweb.pdf

³ www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf

⁴ <https://en.necessaryandproportionate.org/LegalAnalysis>

¹ <https://en.necessaryandproportionate.org/text>

Protected information

The Principles make clear that it is time to move beyond the fallacy that information *about* communications does not pose as serious a threat to privacy as the content of communications. Information about communications, also called metadata, subscriber information or non-content data, can include the location of your mobile phone, click-stream data,⁵ search logs, or anonymous online activity. Individually, these can be just as invasive as reading your email or listening to your phone calls. When combined and analysed *en masse*, the picture painted by such data points can be far more revealing than the content of the communications they accompany. In spite of this reality, pre-internet age (in fact, postal service-based!) legal conceptions have persisted in some legal systems, offering less or, in some instances, no protection at all to information that is not classified as “content”. What is important is not the kind of data that is collected, but its effect on the privacy of the individual.

As explained in the Legal Analysis and Background Materials which have been prepared for the Principles:

The Principles use the term “protected information” to refer to information (including data) that *ought* to be fully and robustly protected, even if the information is not currently protected by law, is only partially protected by law, or is accorded lower levels of protection. The intention, however, is not to make a new category that itself will grow stale over time, but rather to ensure that the focus is and remains the capability of the information, alone or when combined with other information, to reveal private facts about a person or her correspondents. As such, the Principles adopt a singular and all-encompassing definition that includes any information relating to a person’s communications that is not readily available to the general public.

This concern has been addressed by the latest report of the Office of the High Commissioner for Human Rights (OHCHR), which made clear that:

From the perspective of the right to privacy, this distinction between [content and metadata] is not persuasive. The aggregation of information commonly referred to as “metadata” may give an insight into an individual’s behaviour, social relationships, private preferences and identity that go beyond even that conveyed by accessing the content of a private communication.

Given the revealing nature of metadata and content alike, states should be restrained from unchecked interference with any protected information: from revealing a speaker’s identity if it is not public; from wantonly vacuuming up the websites or social media one has visited; from stockpiling information on all the people one has communicated with; and tracking the “when”, “from where”, and “for how long” of all our digital activities. In the pre-internet age, the much more limited amount and kind of “metadata” available to law enforcement was treated as less sensitive than content, but given current communications surveillance capabilities, this can no longer be the case.

Communication surveillance

Much of the expansive state surveillance practices confirmed during the past year depend on confusion over whether actual “surveillance” has occurred and thus whether human rights obligations even apply. Some have suggested that if information is merely collected and kept but not looked at by humans, no privacy invasion has occurred. Others argue that computers analysing all communications in real time for key words and other selectors does not amount to “surveillance” for purposes of triggering legal privacy protections. Still others seek to reduce privacy protections to “harmful uses” of information. Such legal variations can mean the difference between reasonable and carefully targeted investigations and a surveillance state built on the continuous mass surveillance of everyone.

In the digital age, where the most sensitive portions of our lives are constantly communicated over digital networks, it has never been more important to ensure the integrity of our communications. It means little whether the interference takes the form of real-time monitoring of internet transmission, hacking into individuals’ mobile devices, or mass harvesting of stored data from third party providers. The mere recording of internet transactions – even if ultimately unviewed – can have serious chilling effects on the use of our most vital interactive medium. We have to ensure that all acts of communications surveillance are within the scope of human rights protections and, hence, are “necessary and proportionate”.

On this front, the OHCHR report made clear that:

[A]ny capture of communications data is potentially an interference with privacy and, further, that the collection and retention of communications data amounts to an interference with

privacy whether or not those data are subsequently consulted or used. Even the mere possibility of communications information being captured creates an interference with privacy, with a potential chilling effect on rights, including those to free expression and association.

To remedy this issue, the Principles define “communications surveillance” as encompassing the monitoring, interception, collection, analysis, use, preservation and retention of, interference with, or access to information that includes, reflects or arises from a person’s communications in the past, present or future.

Scope of application

The Principles also address a long-standing problem arising from narrow interpretations adopted by some states regarding the extraterritorial application of their human rights obligations. Some have argued that the obligation to respect privacy and other human rights of individuals effectively stops at their national borders. In a world of highly integrated digital networks, where individual interactions and data routes defy any semblance of territorial correspondence, such distinctions are meaningless. The Principles therefore apply to surveillance conducted within a state *or* extraterritorially, and regardless of the purpose for the surveillance – including enforcing law, protecting national security, gathering intelligence, or another governmental function.

The OHCHR’s report explicitly underscores the principle of non-discrimination:

Article 26 of the International Covenant on Civil and Political Rights provides that “all persons are equal before the law and are entitled without any discrimination to the equal protection of the law” and, further, that “in this respect, the law shall prohibit any discrimination and guarantee to all persons equal and effective protection against discrimination on any ground such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status.”

In this regard, the OHCHR’s report stresses the importance of “measures to ensure that any interference with the right to privacy complies with the principles of legality, proportionality and necessity regardless of the nationality or location of individuals whose communications are under direct surveillance.”

The 13 Principles

The substantive Principles are firmly rooted in well-established human rights law. Generally, any limits on human rights should be necessary, proportionate and for a set of permissible purposes. These limits must be set out in law, and cannot be arbitrary.

Under international human rights law, each right is divided in two parts. The first paragraph sets out the core of the right, while the second paragraph sets out the circumstances in which that right may be restricted or limited. This second paragraph is usually called the “permissible limitations” test.

Regarding the right to privacy, the UN Special Rapporteur on Counter-Terrorism⁶ and the UN Special Rapporteur on Freedom of Expression⁷ have stated that the “permissible limitations” test under Article 19 of the International Covenant on Civil and Political Rights (ICCPR), among other articles, is equally applicable to Article 17 of the ICCPR, which prohibits the arbitrary or unlawful interference with privacy rights.

The OHCHR report has neatly summarised these obligations with respect to Article 17 of the ICCPR:

To begin with, any limitation to privacy rights reflected in article 17 must be provided for by law, and the law must be sufficiently accessible, clear and precise so that an individual may look to the law and ascertain who is authorized to conduct data surveillance and under what circumstances. The limitation must be necessary for reaching a legitimate aim, as well as in proportion to the aim and the least intrusive option available. Moreover, the limitation placed on the right (an interference with privacy, for example, for the purposes of protecting national security or the right to life of others) must be shown to have some chance of achieving that goal. The onus is on the authorities seeking to limit the right to show that the limitation is connected to a legitimate aim. Furthermore, any limitation to the right to privacy must not render the essence of the right meaningless and must be consistent with other human rights, including the prohibition of discrimination. Where the limitation does not meet these criteria, the limitation would be unlawful and/or the interference with the right to privacy would be arbitrary.

⁶ UN Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms While Countering Terrorism, A/HRC/13/37.

⁷ UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression, A/HRC/23/40.

⁵ en.wikipedia.org/wiki/Clickstream

Legality: No secret laws

The principle of legality is a fundamental aspect of all international human rights instruments and the rule of law. It is a basic guarantee against the state's arbitrary exercise of its powers. For this reason, any restriction on human rights must be prescribed by law. The meaning of "law" implies certain minimum qualitative requirements of clarity, accessibility and predictability. Laws limiting human rights cannot be secret or vague enough to permit arbitrary interference.

On that front, the OHCHR made clear that:

To begin with, any limitation to privacy rights reflected in article 17 must be provided for by law, and the law must be sufficiently accessible, clear and precise so that an individual may look to the law and ascertain who is authorized to conduct data surveillance and under what circumstances.

The need to meaningfully and publicly explain rights-infringing practices – while important in all contexts – is key to any effective check on communications surveillance, as such practices tend to be surreptitious and difficult to uncover. Given the highly technical and rapidly evolving nature of communications surveillance, it is also incumbent that laws are interpreted publicly and not through secret processes effectively free from public scrutiny. The state must not adopt or implement a surveillance practice without public law defining its limits. Moreover, the law must meet a standard of clarity and precision that is sufficient to ensure that individuals have advance notice of, and can foresee, its application. When citizens are unaware of a law, its interpretation, or the scope of its application, it is effectively secret. A secret law is not a legal limit on human rights.

In her landmark report, UN High Commissioner for Human Rights Navi Pillay made clear that:

[S]ecret rules and secret interpretations – even secret judicial interpretations – of law do not have the necessary qualities of "law". Neither do laws or rules that give the executive authorities, such as security and intelligence services, excessive discretion; the scope and manner of exercise of authoritative discretion granted must be indicated (in the law itself, or in binding, published guidelines) with reasonable clarity. A law that is accessible, but that does not have foreseeable effects, will not be adequate. The secret nature of specific surveillance powers brings with it a greater risk of arbitrary exercise of discretion which, in turn,

demands greater precision in the rule governing the exercise of discretion, and additional oversight.

Legitimate aim

Laws should only permit communications surveillance by specified state authorities to achieve a legitimate aim that corresponds to a predominantly important legal interest that is necessary in a democratic society.

Under international human rights law, any restriction on our fundamental freedoms must generally pursue a permissible purpose or "legitimate aim." These purposes or aims are often enumerated within the article itself. The Principles therefore require that communications surveillance only be undertaken in pursuit of a predominantly important legal interest. Such interests have been described by Germany's highest court as "the life, limb and freedom of the individual or such interests of the public a threat to which affects the basis or continued existence of the state or the basis of human existence."

The OHCHR has similarly affirmed, in its 2014 report, that "any limitation to privacy rights reflected in article 17 of the ICCPR must be necessary for reaching a legitimate aim." The report elaborates:

Surveillance on the grounds of national security or for the prevention of terrorism or other crime may be a "legitimate aim" for purposes of an assessment from the viewpoint of article 17 of the Covenant. The degree of interference must, however, be assessed against the necessity of the measure to achieve that aim and the actual benefit it yields towards such a purpose.

Finally, communications surveillance cannot be employed in a manner that discriminates on the basis of grounds such as race, colour, sex, language, religion or national origin, as such discrimination constitutes an illegitimate purpose.

Necessity, adequacy and proportionality

International human rights law makes clear that any interference with our fundamental freedoms must be "necessary in a democratic society". In its General Comments No. 27, the Human Rights Committee clearly indicates that it is not sufficient that such restrictions serve a legitimate aim, they must also be necessary to it.⁸ Restrictive measures must also be adequate or appropriate to achieving their

protective function. They must also be the least intrusive options amongst those which might be expected to achieve the desired result, and they must be proportionate to the interest to be protected. Finally, any restrictive measure which undermines the essence or core of a right is inherently disproportionate and a violation of that right.

Applying these foundational principles to the context of communications surveillance, the Principles affirm that:

Necessity: Often, a surveillance objective might be achieved using far less intrusive mechanisms. While it is by no means necessary to exhaust other options, it should be recognised that communications surveillance is inherently invasive and should not be a tool of first recourse.

Adequacy: It is not sufficient to show that a given surveillance practice is necessary for achieving a given objective; it must also be adequate and appropriate to it. As noted by the High Commissioner, at minimum, communications surveillance which interferes with privacy "must be shown to have some chance of achieving [its] goal."

Proportionality: Communications surveillance should be regarded as a highly intrusive act that interferes with human rights and poses a threat to the foundations of a democratic society. Communications surveillance for investigative purposes, in particular, should only occur once the state has convinced an objective third party – a judge – that a serious threat to a legitimate interest exists and that the communications mechanism in question will yield information that will assist with that serious threat.

No voluntary cooperation: Current digital networks and interactions entrust vast amounts of personal and sensitive data in the hands of a wide range of third party intermediaries, including internet service providers (ISPs), email providers, hosting companies and others. Through their discretionary decisions to comply (or not) with state surveillance requests, these intermediaries can dramatically impact on the privacy rights of all. Such voluntary sharing bypasses due process and poses a serious threat to the rule of law. The Necessary and Proportionate Principles therefore prohibit any state communications surveillance activities in the absence of judicial authorisation.

No repurposing: Contrary to many official statements, the modern reality is that state intelligence agencies are involved in a much broader scope of activities than simply those related to national security or counterterrorism. The Necessary and Proportionate Principles state that communications surveillance (including the collection of

information or any interference with access to our data) must be proportionate to the objective they are intended to address. And equally importantly, even where surveillance is justified by one agency for one purpose, the Principles prohibit the unrestricted reuse of this information by other agencies for other purposes.

The OHCHR report also emphasises this point, noting that:

The absence of effective use limitations has been exacerbated since 11 September 2001, with the line between criminal justice and protection of national security blurring significantly. The resultant sharing of data between law enforcement agencies, intelligence bodies and other State organs risks violating article 17 of the Covenant [on Civil and Political Rights], because surveillance measures that may be necessary and proportionate for one legitimate aim may not be so for the purposes of another.

Integrity of communications and systems

No law should impose security holes in our technology in order to facilitate surveillance. Undermining the security of hundreds of millions of innocent people in order to ensure surveillance capabilities against the very few bad guys is both overbroad and short-sighted, not least because malicious actors can use these exploits as readily as state agents. The assumption underlying such provisions – that no communication can be truly secure – is inherently dangerous, akin to throwing out the baby with the bathwater. It must be rejected.

The OHCHR report supports that conclusion, stating that:

The enactment of statutory requirements for companies to make their networks "wiretap-ready" is a particular concern, not least because it creates an environment that facilitates sweeping surveillance measures.

Notification and right to an effective remedy

Notification must be the norm, not the exception. Individuals should be notified that access to their communications has been authorised with enough time and information to enable them to appeal the decision, except when doing so would endanger the investigation at issue. Individuals should also have access to the materials presented in support of the application for authorisation. The notification principle has become essential in fighting illegal or overreaching surveillance. Any delay in notification has to be based upon a showing to a court, and tied

⁸ Human Rights Committee, General Comment 27, Freedom of movement (Art. 12), UN Doc CCPR/C/21/Rev.1/Add.9 (1999). www.unhcr.org/refugees/comm/hrc/27.htm

to an actual danger to the investigation at issue or harm to a person.

Before the internet, the police would knock on a suspect's door, show their warrant, and provide the individual a reason for entering the suspect's home. The person searched could watch the search occur and see whether the information gathered went beyond the scope of the warrant. Electronic surveillance, however, is much more surreptitious. Data can be intercepted or acquired directly from a third party such as Facebook or Twitter without the individual knowing. Therefore, it is often impossible to know that one has been under surveillance, unless the evidence leads to criminal charges. As a result, the innocent are the least likely to discover that their privacy has been invaded. Indeed, new technologies have even enabled covert remote searches of personal computers and other devices.

The OHCHR report lays out four characteristics that effective remedies for surveillance-related privacy violations must display:

Effective remedies for violations of privacy through digital surveillance can thus come in a variety of judicial, legislative or administrative forms. Effective remedies typically share certain characteristics. First, those remedies must be known and accessible to anyone with an arguable claim that their rights have been violated. Notice (that either a general surveillance regime or specific surveillance measures are in place) and standing (to challenge such measures) thus become critical issues in determining access to effective remedy. States take different approaches to notification: while some require post facto notification of surveillance targets, once investigations have concluded, many regimes do not provide for notification. Some may also formally require such notification in criminal cases; however, in practice, this stricture appears to be regularly ignored.

The 2014 OHCHR report continues, stressing the importance of a “prompt, thorough and impartial investigation”; a need for remedies to actually be “capable of ending ongoing violations”; and noting that “where human rights violations rise to the level of gross violations, [...] criminal prosecution will be required.”

Safeguards for international cooperation

Privacy protections must be consistent across borders at home and abroad. Governments should not bypass national privacy protections by relying on secretive informal data-sharing agreements with foreign states or private international companies. Individuals should not be denied privacy rights simply because they live in another country from the one that is surveilling them. Where data is flowing across borders, the law of the jurisdiction with the greatest privacy protections should apply.

More to be done

The Necessary and Proportionate Principles provide a basic framework for governments to ensure the rule of law, oversight and safeguards. They also call for accountability, with penalties for unlawful access and strong and effective protections for whistle-blowers. They are starting to serve as a model for reform around the world and we urge governments, companies, NGOs and activists to use them to structure necessary change.

But while the Principles are aimed at governments, government action is not the only way to combat surveillance overreach. All of the communications companies, internet and telecommunications alike, can help by securing their networks and limiting the information they collect and retain. Online service providers should collect the minimum amount of information for the minimum time that is necessary to perform their operations, and effectively obfuscate, aggregate and delete unneeded user information. This helps them in their compliance burdens as well: if they collect less data, there is less data to hand over to the government. Strong encryption should be adopted throughout the entire communications chain and, where possible, for data in storage.

It is clear that under the cloak of secrecy, malfunctioning oversight and the limited reach of outdated laws, the practice of digital surveillance in countries from the far North to the far South has overrun the bounds of human rights standards. We all hope to see activists around the world showing exactly where a country has crossed the line, and how its own policy makers and the international community might rein it back. We must call for surveillance reform to ensure that our national surveillance laws and practices comply with human rights standards and to ensure that cross-border privacy is in place and effectively enforced. Working together, legal plus technical efforts like deploying encryption, decentralisation of services and limiting information collected, can serve as a foundation for a new era of private and secure digital communications.

Thematic reports

Digital surveillance

Elijah Sparrow

LEAP Encryption Access Project

<https://leap.se>

This report examines the properties that make digital communication prone to surveillance and provides a general overview of where and how this surveillance takes place. For our purpose here, any internet or phone-based communication is considered to be digital communication, but we exclude from consideration other forms of surveillance such as direct observation or photography.

The properties of digital communication

It is no easy task to pinpoint what we mean when we say “surveillance”. As a first approximation, David Lyon defines surveillance as “the focused, systematic, and routine attention to personal details for purposes of influence, management, protection, or direction.” This definition tries to convey the way in which surveillance has historically functioned as a necessary aspect of maintaining modern society,¹ for example, in sorting citizens from non-citizens, the sick from the healthy, the credit worthy from the credit risks. He then immediately goes on to note that surveillance is often not focused, systematic or routine at all – for example, in the case of dragnet surveillance that captures information from the digital communication of everyone without any evidence of its efficacy. What are we to make of surveillance in a digital age, where the capture and processing of personal information by powerful actors is not just routine but ubiquitous? Increasingly, surveillance does not seem an activity undertaken for simple “influence, management, protection or direction”, but instead seems to be much more, constituting the core security strategy of many nation-states and the core business model for the largest internet firms, credit card companies, and advertisers.

Most historians of surveillance likely agree with Lyon’s assertion that “digital devices only increase the capacities of surveillance or, sometimes, help to

foster particular kinds of surveillance or help to alter its character.”² It is worthwhile, however, to ask what precisely is different about “digital”, and how this transformation of surveillance scale and character might represent something substantially new.

Perfect digital copy

A good analogy for the key difference between analogue and digital communication is to compare speech with the printed word. Without modern audio equipment, it is difficult for a human to reproduce speech exactly, but it is very easy to reproduce written words. Like written words, digital information is encoded into discrete and reproducible components. Because of this, digital information is always copied perfectly, unlike analogue communication, where data was conveyed via imprecise and ephemeral voltage or frequency levels. More to the point, digital information can only be copied. You cannot move digital information from one place to another without making a perfect copy. The copy operation frequently fails, but the process is always audited for errors and repeated until the copy is perfected.

Many points of capture

When communication is digital, surveillance lies at its very heart. Because every possible step in the transmission and reception of digital communication results in a perfect copy, the information at every step is exposed for easy capture. As we transition to all communication being digital, we move into a world with an explosion in the potential sites of surveillance capture. At the same time, the relatively centralised nature of the core backbone of the internet makes it possible to monitor most of the world’s traffic from a few key locations.³ Also, the

² Ibid., p. 15.

³ Although most people think of the internet as decentralised, it is more accurate to describe the topology as polycentric. The backbone core of the internet that carries nearly all the traffic is owned by a handful of “Tier 1” carriers, making it possible to capture most of all internet traffic by listening at the points of exchange between these carriers. This is less true of traffic from the large internet sites, such as Google, Facebook and Netflix, as they have recently installed content delivery networks “inside” the networks of the large internet service providers.

¹ Lyon, D. (2007). *Surveillance Studies: An Overview*. Cambridge: Polity Press, p. 14.

rapidly falling cost of sensors to convert real-world inputs into digital signals has resulted in a proliferation of these sensors in our environment, from our consumer devices to agriculture to sensor networks designed to improve urban life.

Data immortality

Although your personal device might fail, information stored on servers in digital formats effectively lives forever. Physical storage mediums often have short life spans, but information is nearly always stored in duplicate, so that when one physical device begins to fail the information is automatically mirrored to another storage device. Error-correcting protocols ensure that this endless copying never results in an imperfect copy. As the amount of storage available per dollar continues to grow exponentially, there is often no need to ever throw anything away, even for very large datasets.

Automation

The capture, storage and analysis of digital information is largely automated, unbound by the limitations of available human labour. The former East German secret police employed as many as two million informants,⁴ but today it would require only a handful of off-the-shelf network monitoring devices, placed in key locations, to far surpass the Stasi's reach. The result of this automation is that both state intelligence services and internet businesses that monetise user information have taken the general approach of capturing everything, when practical, with the idea that the data might be useful in the future.

To be sure, there are limits to how much information can be captured and effectively analysed. These limits, however, have been pushed back faster and farther than most observers expected, as both nation-states and private firms have invested heavily in ways to store and process more data.

High confidentiality

In the past, when surveillance was labour intensive and available only at a few specific sites in the communication process, it was possible to establish a legal framework that adequately sanctioned and controlled the when, where, who and why of state surveillance. Digital communication has destroyed this in two ways: first, the barriers to entry for capturing information for surveillance are very low; and second, the only way to prevent nearly everyone from doing so is to encrypt the data, but this also prevents state-sanctioned surveillance. Data is

either widely vulnerable to surveillance by a variety of actors, many nefarious, or it is secure, encrypted, and eludes state control. In practice, of course, this is still not entirely the case, because most security products are deeply flawed and determined state actors and criminal organisations are able to bypass these systems. The poor quality of existing security products is changing rapidly, however, as more people become aware of the level of surveillance in their lives and seek out increased security.

One potential middle ground that could allow sanctioned surveillance but prevent unsanctioned compromise is the so-called “key escrow” technology, such as the type promoted by the United States (US) government in the 1990s under the Clipper Chip programme. In practice, this technology has not proven itself to be secure, and widespread adoption would require making normal cryptography illegal, a move only likely in the most repressive contexts.

So far, the mathematics behind common encryption standards, such as OpenPGP or AES, have generally held strong and those seeking to decrypt confidential communication are fighting an uphill battle. Typically, attacks against encrypted communication exploit other weaknesses, but are unable to break the encryption itself.⁵

Low anonymity

If communication can theoretically be made highly confidential without much effort, the opposite is true of anonymity. It is possible, for example, to identify a unique fingerprint of the radio signals produced by all wireless digital devices. In general, every electronic device emits electromagnetic radiation that can be used to identify it and often to eavesdrop remotely.⁶ Even our web browsers advertise to every web server a set of attributes that can comprise a unique fingerprint.⁷

Government and private sector organisations often argue that the certain datasets they collect and maintain are anonymous because they do not include the real names of people. In reality, re-

searchers have been able to de-anonymise nearly every such dataset when given an opportunity.⁸ For certain types of information, like location and relationships, it often requires only a few points of data to unmask a person's identity by correlating with another dataset in which real names are known.

The rise of packet-switched networks, like the internet, has also made anonymity difficult. The historical transition from analogue to digital was accompanied by a similar transition in networking from circuit switching to packet switching. Where once a single continuous circuit was required to make a phone call, now a phone call is digitised and converted into millions of tiny packets, routed through equipment that handles millions of other calls. Every packet contains a source and destination headers so that each device in the network knows where to forward the packet on to. Packet-based routing has revolutionised communication as much as digitisation has by allowing the massive investment in old copper cables to be re-purposed for digital networks that can transport millions of times more data. One consequence of packet-switched networks is that it is extremely easy, at many points and times in the network, to determine the flow of who is communicating with whom.

All digital data carried over a network is converted into packets, with different communication protocols layered on top, such as phone calls, email and financial exchanges. These higher-level communications involve their own, and distinct, information regarding the from, to and when of the relationship, but the general idea is the same. This type of transactional or relationship data, recently dubbed “metadata” in the press, is structured and efficient to store, lending itself to various types of powerful analysis that can reveal surprising information from seemingly innocuous data.

Attempts to mask these associations with tricks such as onion routing and data mixing are mostly experimental, make communication much slower, and are rarely used.⁹ Because the success of these

anonymising networks is dependent on their scale, anyone seeking anonymity in their digital communication is fighting an uphill battle until such approaches become commonplace.

In brief, surveillance of digital communication is ubiquitous, automatic, and effectively lives forever. In the future, people will likely find it easy to encrypt the content of their communication, but their pattern of communication and relationships will likely be difficult to keep from being exposed.

A brief taxonomy of digital communication surveillance

In examining where surveillance of digital communication takes place, we divide surveillance into two categories: attack or capture.

Points of attack

Attacks are attempts to subvert the way a computing system is supposed to work. Attacks might be legal and ordered by a court, carried out by a government without legal authorisation, or entirely extralegal. Attacks might be carried out by private contractors, government agents, or organised crime. Regardless of who is carrying out the attack, and for what purpose, attacks share many common characteristics.

Network interposition: In a man-in-the-middle (MiTM) attack, the attacker interposes themselves in the communication stream between two parties in order to modify the data. Modified traffic can be used to steal authentication information, modify web applications, or inject Trojans into the target's device. Although network interposition attacks are typically associated with powerful surveillance agencies like the US National Security Agency (NSA) and Government Communications Headquarters (GCHQ) in the United Kingdom (UK), even small governments with very limited resources have made effective use of MiTM attacks against dissidents (for example, the Tunisian government in the lead-up to the Jasmine Revolution of 2011).¹⁰ Regardless of the physical location of the target, a MiTM attack can be launched from nearly anywhere, even on a modest budget, due to critical vulnerabilities in the protocol that negotiates routes on the internet.¹¹ Mobile devices are also vulnerable to MiTM attacks

⁴ Koehler, J. (2000). *Stasi: The untold story of the East German secret police*. Boulder: Westview Press.

⁵ One of the top cryptographers in the world, Adi Shamir, has said “cryptography is bypassed, not penetrated.” This is not to imply that systems are generally secure. Far from it – they are usually entirely insecure, but rarely because of a fundamental flaw in the cryptography. Peter Gutmann's excellent presentation “Crypto Won't Save You Either” covers most of the major security problems in recent memory and details how attackers simply bypassed encryption: www.cs.auckland.ac.nz/~pgut001/pubs/crypto_wont_help.pdf

⁶ Elliot, M. (2013). Noise Floor: Exploring the World of Unintentional Radio Emissions. Presentation at DEF CON 21. Video: www.youtube.com/watch?v=5N1C3WB8coo, slides: https://docs.google.com/presentation/d/1Z_IRt6R2FL7POeY4J-pYGLDAIADEHprQY13f-NVlFwE

⁷ Eckersley, P. (2010). *How Unique Is Your Web Browser?* <https://panopticklick.eff.org/browser-uniqueness.pdf>

⁸ One of the first examples of surprising de-anonymisation concerned the “anonimised” dataset released by Netflix for a competition to improve their recommendation engine. Narayanan, A., & Shmatikov V. (2008). *Robust De-anonymization of Large Sparse Datasets*. www.cs.utexas.edu/~shmat/shmat_oako8netflix.pdf

⁹ Onion routing is a process where a communication stream is routed through many computers, each one unaware of all the others except for their immediate peers. It is used in low-latency anonymisation networks like Tor. Data mixing is a process where many asynchronous packets of data or messages are combined into a common flow, and then potential routed through multiple mixing nodes. Data mixing is used in high-latency anonymisation networks like Mixmaster. Both processes attempt to anonymise communication by using many servers, but each approach makes different trade-offs.

¹⁰ O'Brien, D. (2011, January 5). Tunisia invades, censors Facebook, other accounts. *Committee to Protect Journalists*. <https://cpj.org/blog/2011/01/tunisia-invades-censors-facebook-other-accounts.php>

¹¹ Pilosov, A., & Kapela, T. (2008). Stealing The Internet: An Internet-Scale Man in the Middle Attack. Paper presented at DEF CON 16. <https://www.defcon.org/images/defcon-16/dc16-presentations/defcon-16-pilosov-kapela.pdf>

from cheap “IMSI catchers”, widely used by law enforcement.¹²

Physical compromise: The large intelligence agencies have top-secret product catalogues of hundreds of high-tech equipment that can be hidden inside a device or modify a device to allow eavesdropping,¹³ sometimes installed in new equipment before it reaches the customer.¹⁴ But an attacker seeking to physically compromise a device does not need the budget of the NSA: for a few dollars, anyone can order online a tiny USB dongle that snaps between a keyboard and a computer and allows the attacker to record every key stroke.¹⁵ Because physical compromise is very difficult to detect, computing devices that have been physically in the possession of an attacker should not be trusted.

Remote exploit: Software, in general, is full of unknown security vulnerabilities waiting to be discovered. Most of the time, these vulnerabilities are identified by responsible researchers who notify the software authors so that a fix can be made available or an update automatically applied. Attackers are able to take advantage of the gap in time between when a vulnerability is fixed and when this fix is actually applied in order to exploit the flaw and hijack a computer or steal information. If a vulnerability is first discovered by an attacker it is called a “0-day”, because there have been zero days since the vulnerability has been known to the public or the software developers. Various governments, as well as some criminal organisations, spend large amounts of money developing 0-days and purchasing them on the black market.¹⁶

Social engineering: Attackers often rely on fooling humans rather than computer systems, a process called “social engineering”. Humans can be remarkably easy to trick. For example, when researchers scattered random USB memory sticks in

a parking lot, most of the people who found them plugged them into their organisation’s private network,¹⁷ an extremely insecure practice that can result in a MITM attack or provide an easy entry for a Trojan.¹⁸ One highly effective and low-cost form of social engineering is called “spear phishing”, where the attacker uses some bit of personal information about the target to trick the target into opening a hostile Trojan. Many people, for example, would open an email attachment that appears to come from a friend or colleague. Social engineering can also be as simple as impersonating someone on the phone.

Software updates: In some cases, the software update system designed to apply security fixes to a device can itself be the delivery pathway for a Trojan or other malicious code. Sadly, few update systems are very secure.¹⁹ The United Arab Emirates, for example, used the BlackBerry update mechanism in order to install remote surveillance capabilities on all BlackBerry customers in the country (without the knowledge of or approval from BlackBerry).²⁰

Third-party compromise: With the recent rise of cloud computing, nearly all users rely on third parties to keep some or all of their sensitive information safe. As consolidation has resulted in fewer third parties holding an ever larger cache of personal data, attackers and governments have turned their attention to these third parties as an efficient, centralised source of surveillance data.²¹ The daily parade of data-breach headlines is evidence of the grossly inadequate security practices by many of these third parties.

Trojans: A Trojan is a type of computer virus disguised as a benign programme, or it may even be hidden inside a modified version of a common application. In a “phishing” attack, the target installs

the Trojan themselves, fooled into believing the application is legitimate. When used by governments, the Trojan is often installed manually when the device is out of the possession of its owner or via man-in-the-middle network attacks. Although many Trojans are created by those sending “spam” or organised crime, Trojans are also big business: one Trojan developed by Hacking Team, an Italian surveillance company, is used by over 60 governments and allows the operator access to nearly all aspects of a target’s mobile device.²²

Usability error: At present, most software that allows you to communicate securely is highly sensitive to mis-configuration or misuse, providing many opportunities for attack. Many chat applications, for example, have a default setting that will allow an attacker to bypass secure connections between the client and the server.²³ In 2008, the default setting in Thunderbird caused thousands of German users to silently drop transport encryption when their internet service provider (ISP) accidentally disrupted the secure connection negotiation (since fixed).²⁴ The very concepts required for confidential communication, such as public and private key or key fingerprints, are deeply confusing for many users.²⁵

Points of capture

Rather than an attack that exploits a flaw, some forms of surveillance are an incidental or core function of the system itself.

Devices: Nearly every end-user computing device that facilitates digital communication retains a wealth of personal information as part of its normal operation. Particularly in the case of mobile devices, this information likely includes web browsing history, location history, call records, photographs, and a record of messages sent and received. User devices also often store a copy of authentication credentials that can be used to gain access to information stored by third parties. Some devices are very small or even invisible: for example, an “embedded system” containing a rudimentary computing logic and memory capacity can be found in

USB memory sticks, some RFID chips,²⁶ and appliances. Despite their simplicity, these embedded systems can be programmed to record information about the user, as in the case of the 2006 World Cup where the event tickets themselves contained an RFID chip that both reported personal information to authorities whenever the ticket passed a scanner and also recorded on the ticket itself a history of locations the ticket had been.²⁷

Device emissions: As noted previously, every device, and many applications, emit unique signatures that can be used to track the location, behaviour or internal workings of a device. These unique signatures take many forms: by design, web browsers present uniquely identifying information to every website they visit; by design, every mobile phone has a unique and unchangeable tracking identifier that is logged by cell phone towers; by accident, devices emit unique electromagnetic radiation that can remotely reveal the screen contents; by accident, central processing units (CPUs) emit low level noise that a remote listener can use to extract private keys;²⁸ and so on. What counts as a device will soon become difficult to define, as consumer goods such as clothing, watches, appliances and tickets start to include tiny embedded systems – even food²⁹ may soon be tracked via RFID.

Networks: Surveillance can take place at every step in a data packet’s journey from source to destination. Networks may be monitored close to an endpoint, as when an IMSI catcher is used to monitor the traffic of a target mobile device, at the ISP level, or at the level of the internet backbone where most traffic eventually flows. Because the internet is polycentric, relying on a handful of large carriers for connections among ISPs, a small number of strategic listening posts are able to monitor a high percentage of all traffic. Typically, large intelligence agencies monitor traffic near the backbone, small governments will monitor all the traffic in and out of their country (typically at the ISP level), and everyone takes part in monitoring close to the endpoint (including organised crime). The US and UK use network surveillance to build very large databases of

12 Stein, J. (2014, June 22). New Eavesdropping Equipment Sucks All Data Off Your Phone. *Newsweek*. www.newsweek.com/your-phone-just-got-sucked-255790

13 Appelbaum, J., Horchert, J., & Stöcker, C. (2013, December 29). Shopping for Spy Gear: Catalog Advertises NSA Toolbox. *Der Spiegel International*. www.spiegel.de/international/world/catalog-reveals-nsa-has-back-doors-for-numerous-devices-a-940994.html

14 Greenwald, G. (2014, May 12). How the NSA tampers with US-made internet routers. *The Guardian*. www.theguardian.com/books/2014/may/12/glenn-greenwald-nsa-tampers-us-internet-routers-snowden

15 As of this writing, there are dozens of key loggers available on Amazon.com, most for less than USD 100 and many with remote wireless access.

16 Menn, J. (2013, May 10). Special Report - U.S. cyberwar strategy stokes fear of blocback. *Reuters*. in.reuters.com/article/2013/05/10/usa-cyberweapons-idINDEE9490AX20130510

17 The fault here is not really human error, but human error only in the context of very poorly designed operating system security. Edwards, C., et al. (2011, June 27). Human Errors Fuel Hacking as Test Shows Nothing Stops Idiocy. *Bloomberg News*. www.bloomberg.com/news/2011-06-27/human-errors-fuel-hacking-as-test-shows-nothing-prevents-idiocy.html

18 Greenberg, A. (2014, July 31). Why the Security of USB Is Fundamentally Broken. *Wired*. www.wired.com/2014/07/usb-security

19 Cappos, J., et al. (2008). *A Look in the Mirror: Attacks on Package Managers*. https://isis.poly.edu/~jcappos/papers/cappos_mirror_ccs_o8.pdf

20 Coker, M., & Weinberg S. (2009, July 23). RIM Warns Update Has Spyware. *Wall Street Journal*. online.wsj.com/news/articles/SB12482717241712239

21 Gellman, B., & Poitras L. (2013, June 6). U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program. *Washington Post*. www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0coda8-cebf-11e2-8845-d970ccbo4497_story.html

22 Zetter, K. (2014, June 24). Researchers Find and Decode the Spy Tools Governments Use to Hijack Phones. *Wired*. www.wired.com/2014/06/remote-control-system-phone-surveillance

23 By specification, chat applications that support the XMPP chat standard must use StartTLS for secure connections, but StartTLS will downgrade to plain text and insecure connections if the TLS negotiation fails (which is not hard for an attacker to cause). Only if the chat application is configured to notify the user of this downgrade, or prevent it, will the user be assured of a secure connection. This same vulnerability exists in many email clients.

24 Heise Security. (2008). Eingriff in E-Mail-Verschlüsselung durch Mobilfunknetz von O2. heise.de/-206233

25 Whitten, A., & Tygar J.D. (1999). *Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0*. www.gaudior.net/alma/johnny.pdf

26 RFID (radio frequency identification) is a technology that allows an item to report a globally unique identifier when the tiny RFID chip is passed near a scanner. Some RFID chips, however, also contain embedded systems with a small degree of computing logic and memory capacity.

27 Blau, J. (2006, May 26). Security Scores Big at World Cup Tournament. *PCWorld*. www.pcworld.com/article/125910/article.html

28 Genkin, D., et al. (2013). *RSA Key Extraction via Low-Bandwidth Acoustic Cryptanalysis*. www.cs.tau.ac.il/~tromer/acoustic

29 Gatto, K. (2011, May 31). The NutriSmart system would put RFIDs into your food for enhanced information. *PhysOrg.com*. phys.org/news/2011-05-nutrismart-rfids-food.html

metadata in order to build a social network graph of everyone who communicates digitally³⁰ as well as the full content of some 200 million text messages a day³¹ (it is almost certain that other intelligence agencies attempt similar surveillance, but it is not yet documented publicly). Some countries have data retention laws that require ISPs to keep records of certain metadata, such as the sites that a user visits and their IP address, for up to seven years.³² For a smaller country, however, it is entirely possible for a government to retain the content of communication as well, including all text messages and all phone conversations, using inexpensive commercially available equipment.

Third parties: All digital communication leaves a record with third-party intermediaries (except in special circumstances).³³ Third parties may include email providers, telephone carriers, ISPs, credit card companies, online retail, computer backup or file storage, and many mobile app developers (since many apps will store user data on the server). Much of the third-party tracking is carried out for the purpose of advertising and market research, some of which is visible, in the case of loyalty discount cards, while some is invisible to the user, such as ad targeting. Third-party advertising networks are able to track a user's internet behaviour, even when the user switches devices, because most websites and mobile applications use one or more of the same advertising and tracking networks. Although intended for commercial use, government surveillance agencies are able to use tracking data sent to advertising networks³⁴ and application data sent to computer servers³⁵ as a rich source of surveillance of personal information.

Digital surveillance grows up

Digital surveillance is still in its infancy. Governments collect more data than they know how to effectively process, facial recognition is still not accurate, and tracking databases are full of false information. For some, this is a comfort: no matter how much the surveillance net expands, it will be full of holes (and also false positives, with sometimes tragic personal results for those falsely convicted).³⁶

Unfortunately, we are living in an age where the management and processing of information has become an essential component of industry, agriculture, public health, military, and soon education – in other words, nearly every aspect of state management and private business. These systems all need information to function, and surveillance designed to feed these systems more information is getting better all the time. Digital surveillance may be in its infancy, but it is working hard to grow up fast.

Despite the rather dire picture painted by this brief tour of digital surveillance, those who are concerned by the rapid maturation of surveillance and expansion into more aspects of social life have cause for hope. The struggle for the future of digital communication – who can control the flow of bits and who can assign identity to those bits – is being actively fought on the terrains of politics, law and technology. While all these terrains are important, new advances in the technology of encryption, usability and open protocols have the potential to offer powerful protection to the common user in the near future.

The myth of global online surveillance exempted from compliance with human rights

Alberto J. Cerda Silva

University of Chile Law School and ONG Derechos Digitales
www.derecho.uchile.cl, https://www.derechosdigitales.org

Introduction

Since mid-2013 there have been continuing revelations about the implementation by the United States (US) government of a series of programmes that constitute a system for global mass online surveillance. The initiative involves several agencies, primarily led by the National Security Agency (NSA), in close cooperation with companies that provide services through the internet. The system, which mostly targets foreigners and overseas communications, has affected private communications everywhere, from heads of state to ordinary web users.

These revelations about a system for global mass online surveillance have raised human rights concerns. Over time, these concerns have been rejected by suggesting that human rights have no application on the matter because they lack specific norms, have a narrow scope, or are irrelevant to non-state actors. These arguments have built a myth that online cross-border surveillance would be exempted from compliance with human rights law. This report challenges these misconceptions by, first, restating the full application of human rights law over global mass online surveillance and, second, calling attention to the current limitations of human rights law for achieving actual enforcement of human rights worldwide.

Human rights law on surveillance

Throughout the 1990s, there was a belief that the internet was a *laissez-faire* environment exempted from any governmental control, regulation and restriction. This misconception was fuelled by libertarian ideas that overstate the borderlessness, openness and virtual anonymity of the internet.¹ These features, however, rather than preventing any regulatory approach, merely challenge the efficiency of regulations, raising the difficulty of international

harmonisation of regulations. Through the years, the internet has become an environment heavily regulated in which several layers of regulation and laws overlap, one of them being international human rights law. In fact, as some recent resolutions by the United Nations make clear, human rights are fully applicable to the online environment.²

Although human rights are wholly applicable to the internet, it has been suggested that online surveillance has no implications from a human rights viewpoint, since there is no specific rule on the matter in any international instruments on human rights. This argument, however, rests on a short-sighted and literal interpretation of the law. Those instruments, rather than dealing with specific risks, set forth general rules and principles that must be applied in numerous concrete circumstances. In the particular case of mass online surveillance, it raises concerns related to several rights, such as privacy, due process, protection of personal data, equal protection, and judicial protection, among others.

Ruling that surveillance has implications for human rights does not mean that surveillance should be outlawed, since its practice may be allowed in certain circumstances. On the contrary, it opens an analysis to determine if a given measure of surveillance is in compliance with human rights. In other words, human rights are not absolute and could be subject to certain limitations – and, some practices of surveillance that limit certain human rights could be permissible.

However, countries are not completely free to limit human rights; on the contrary, they must comply with certain rules established by international law on the matter.³ First, limitations require

³⁰ Greenwald, G., & Ackerman S. (2013, June 27). How the NSA is still harvesting your online data. *The Guardian*. www.theguardian.com/world/2013/jun/27/nsa-online-metadata-collection

³¹ Ball, J. (2014, January 16). NSA collects millions of text messages daily in 'untargeted' global sweep. *The Guardian*. www.theguardian.com/world/2014/jan/16/nsa-collects-millions-text-messages-daily-untargeted-global-sweep

³² The Wikipedia page on data retention has the most up-to-date overview of the current state of retention laws around the world. https://en.wikipedia.org/wiki/Telecommunications_data_retention

³³ It takes a very careful design to create a system that does not leak communication records to intermediaries. Even most peer-to-peer systems will leak relationship or timing information in the traffic. As of this writing, probably the most effective system designed to leave no useful information with intermediaries is a program called "Pond", although it is still experimental, hard to use, and has few users. See: https://pond.imperialviolet.org

³⁴ Soltani, A., et al. (2013, December 10). NSA uses Google cookies to pinpoint targets for hacking. *Washington Post*. www.washingtonpost.com/blogs/the-switch/wp/2013/12/10/nsa-uses-google-cookies-to-pinpoint-targets-for-hacking

³⁵ Ball, J. (2014, January 27). Angry Birds and 'leaky' phone apps targeted by NSA and GCHQ for user data. *The Guardian*. www.theguardian.com/world/2014/jan/27/nsa-gchq-smartphone-app-angry-birds-personal-data

³⁶ Starr, G. (2014, June 26). What Your Cell Phone Can't Tell the Police. *The New Yorker*. www.newyorker.com/online/blogs/newsdesk/2014/06/what-your-cell-phone-cant-tell-the-police.html

² United Nations General Assembly, Resolution on the promotion, protection and enjoyment of human rights on the Internet, UN Doc. A/HRC/20/L.13, 29 June 2012; United Nations Resolution adopted by the General Assembly on 18 December 2013: The right to privacy in the digital age, UN Doc. A/RES/68/167 (21 January 2014); and United Nations General Assembly, The promotion, protection and enjoyment of human rights on the Internet, UN Doc. A/HRC/26/L.24, (20 June 2014). See also the Report of the Office of the United Nations High Commissioner for Human Rights: The right to privacy in the digital age, UN Doc. A/HRC/27/37, 30 June 2014.

³ Kiss, A. C. (1981). Permissible limitations on rights. In Louis Henkin (Ed.), *The International Bill of Rights: The Covenant on Civil and Political Rights*. New York: Columbia University Press, pp. 290-310.

an enabling law, that is, an act passed by the legislature.⁴ Second, limitations must have a legitimate purpose. In fact, human rights could be subject to limitations for several reasons, including national security, public safety and order, as well as public health and morals. According to the Universal Declaration of Human Rights, limitations are permissible “for the purpose of securing due recognition and respect for the rights and freedoms of others.”⁵ Third, limitations must be proportional, that is, there must be certain balances between the imposed restriction and its attempted purpose.⁶ And fourth, when adopting limitations, countries must establish appropriate safeguards to prevent the misuse and abuse of restrictions regarding human rights.

While the US has authorised the NSA's system for global mass online surveillance in domestic law, it fails to meet any other requirement set forth by international human rights law. First, although it seems justified on the grounds of legitimate purpose, international law proscribes any limitation that discriminates arbitrarily, such as those based on distinctions of religion, political or other opinion, and national or social origin, among others.⁷ Second, the system does not meet the test of proportionality, since even if adequate for fulfilling its purpose, it is unnecessary because there are less severe means of achieving the intended objective, and it is disproportional because the detrimental effects on human rights of implementing a system for global mass online surveillance exceed its potential benefits. And third, the evidence has shown that the safeguards provided by law, mainly through judicial control in implementing policies, were neither sufficient nor appropriate, since they were completely overcome by the actual implementation of the system.

In sum, although a system for global mass online surveillance, similar to that implemented by the NSA, may be in compliance with a given country's domestic law, it certainly violates international human rights law by arbitrarily discriminating

against its target population, by being unnecessary and disproportional, and by lacking appropriate safeguards.

Protection beyond citizenship and territory

Another misconception that has been used to justify mass online surveillance, especially overseas, involves narrowing the scope of human rights law by arguing that it does not provide protection to either foreigners or non-resident subjects. In the case of the NSA's initiative, this argument states that the US Constitution would only recognise the fundamental rights of citizens and, therefore, foreigners would be excluded from protection.⁸ As a result, while domestic law provides for some safeguards in favour of nationals (which have proved deficient), they are virtually non-existent for alien citizens. Although this conception may be consistent with domestic law, it runs notoriously short on meeting international human rights law.

Limiting human rights protection to citizens also infringes human rights law. In fact, all international instruments on the matter recognise that these rights belong to everybody, disregarding their nationality or citizenship. As the Universal Declaration of Human Rights states, they are inalienable rights of “all members of the human family” that “human beings shall enjoy.”⁹ Excepting certain political rights that are attached to citizenship, such as voting and being elected, all other human rights belong to people without permissible exceptions based on being a citizen of a given country. On the contrary, international instruments on human rights law expressly forbid distinctions of any kind, not only based on race, colour, sex or language, but also on religion, political or other opinions, as well as national or social origin, among other statuses.¹⁰

Related to the argument that attempts to exempt compliance with human rights in the case of surveillance over foreigners, it has been argued that no government is required to guarantee rights other than those of people under its own jurisdiction and, therefore, there is no duty to respect human rights of people overseas. This narrow conception argues that one state cannot be compelled to promote, protect and respect human rights within other states, since this is a primary competence of the state that exercises jurisdiction over the territory. Additionally, this conception rests on

the literal interpretation of the word “territory”, as the physical space under the exclusive control of a given state that forces compliance with human rights law. This argument is, however, deceptive and anachronistic.

Human rights law was created after the Second World War in order to develop binding international laws that would prevent a recurrence of the atrocities experienced. The law was not limited to violations committed by governments against their own nationals in their own territory, but also people from other jurisdictions, sometimes in territories that were not under exclusive control. It is true that a state may not be able to promote and protect human rights in other jurisdictions than its own, but it certainly can (and must) respect those rights by constraining its own officials from violating them on and off its territory. Moreover, in the case of a system of global online surveillance, it is not clear in which country's territory human rights violations take place.

However, the main problem with narrowing the scope of human rights to a physical territorial space is that, in a globalised world with noticeable improvements in transport and communications, one confronts an impermissible loophole from a teleological perspective that looks into the purpose of human rights law rather than the narrower wording of a human rights treaty. The extraterritorial application of human rights is the only one that provides meaning to human rights in the current state of affairs.¹¹ Even if limited, this extraterritorial effect of international human rights law has been upheld by international courts, as well as domestic courts, such as the United Kingdom courts that recently held liable its soldiers for human rights violations committed against civilians in Afghanistan. A teleological interpretation of human rights obligations is the only one that could make sense in a digital age, in which a violation of those rights could be committed remotely, between one country and another.

Non-state actors' responsibility

Another misconception about the human rights implications of surveillance argues that those rights are only enforceable against state actors, but not against non-state actors and, therefore, private actors spying on people are not subject to human rights scrutiny. This belief is anchored in the fact that international instruments on human rights set forth obligations only on state parties, since they have standing as legal entities before international law. In addition, this argument points out that, although human rights philosophy has been there for a while, international instruments crystallised them as a reaction against the experiences of totalitarian states that led to the horrors of the Second World War, in which governments infringed their own citizens' rights. In this view, preventing violations committed by private parties is not a matter of concern for international human rights law, but an issue left to the discretion of each country's domestic law. This argument is, however, misleading.

Although international instruments on human rights primarily set forth obligations on states, they have at the very least indirect effects on non-state actors, such as corporations involved in surveillance. In fact, those instruments demand that states not only respect but also promote and protect human rights.¹² Because of this, in addition to restraining states from violating human rights, international law imposes on states a duty to encourage and to safeguard those rights from infringing actions of third parties. As a matter of fact, case law by human rights courts has made explicit that the state is not only responsible for its own actions, but also for failing to protect those rights when violations are committed by non-state actors, such as paramilitary forces.¹³ It follows, naturally, that since the state is internationally responsible for human rights, even if non-state actors violate them, the state has a duty to enforce those rights against infringing non-state actors in domestic law. Therefore, the state must take actions in order to prevent human rights violations by both state and non-state actors.

In order to comply with the obligation of ensuring that surveillance does not infringe on the right to privacy, as well as other human rights, countries have adopted diverse paths. Some countries have prevented illegal surveillance by: adopting laws that regulate in detail the processing of personal

4 Inter-American Court of Human Rights, Advisory Opinion OC-6/86 of 9 May 1986, “Laws” in article 30 of the American Convention on Human Rights, para. 38.

5 Universal Declaration of Human Rights, Article 29 (2).

6 Barak, A. (2012). *Proportionality: Constitutional Rights and Their Limitations*. Cambridge: Cambridge University Press.

7 American Declaration of the Rights and Duties of Man, articles I and II; Universal Declaration of Human Rights, articles 1 and 2; European Convention on Human Rights, article 14; International Covenant on Civil and Political Rights, article 2; International Covenant on Economic, Social and Cultural Rights, article 2; American Convention on Human Rights, article 1; Charter of Fundamental Rights of the European Union, article 21; and African Charter on Human and Peoples' Rights, article 2.

8 Cole, D. (2003). Are Foreign Nationals Entitled to the Same Constitutional Rights As Citizens?, *Thomas Jefferson Law Review*, 25, 367-388.

9 Universal Declaration of Human Rights, Preamble.

10 See note 7.

11 United Nations Human Rights Committee, General Comment No. 31[80] Nature of the General Legal Obligation Imposed on States Parties to the Covenant, 29 March 2004, UN Doc. CCPR/C/21/Rev.1/Add.13 (26 May 2004), para. 10. See also: Moreno-Lax, V., & Costello, C. (2014). The Extraterritorial Application of the EU Charter of Fundamental Rights: From Territory to Facticity, the Effectiveness Model. In S. Peers, T. Herve, J. Kenner, & A. Ward (Eds.), *The EU Charter of Fundamental Rights: A Commentary*. Oxford: Hart Publishing, pp. 1657-1683; and Grabenwarter, C. (2014). *European Convention on Human Rights: Commentary*. Oxford: Beck/Hart.

12 United Nations Human Rights Committee, General Comment No. 31[80] Nature of the General Legal Obligation Imposed on States Parties to the Covenant, 29 March 2004, UN Doc. CCPR/C/21/Rev.1/Add.13 (26 May 2004), paras. 1-8.

13 Inter-American Court of Human Rights, Velasquez Rodriguez Case (Series C) No. 4, para. 172, 29 July 1988.

information by state and non-state actors; regulating the commercialisation of dual-use technology (i.e. goods that can be used for both legitimate and illegitimate purposes, such as spyware and communication intercepting devices); rejecting any evidence obtained that infringed on human rights, such as the illegal interception of communications; and punishing the most outrageous acts of intrusions on privacy. This legislative approach provides a certain level of legal certainty, but has some limitations, mainly the fact that it does not grant comprehensive protection.

Countries with a modern constitutional framework have adopted a different path for protecting human rights in domestic forums. They have incorporated international instruments on human rights into their domestic constitutions and made those rights enforceable against both state and non-state actors. This is the case in Latin American countries, in which there are a number of court decisions based on constitutional grounds that nullify data retention laws, grant privacy in online communications, prevent rights-abusive processing of personal data, and limit video surveillance to proportional circumstances. This constitutional protection of human rights grants comprehensiveness, although it is usually followed by legislative acts that detail concrete implications in more complex cases.

The internet has become crucial for our lives, and it will be even more important as more people connect, accessing more services, and for longer periods of time. The internet is, however, an environment essentially controlled by private actors: from entities that assign technical sources¹⁴ to those that adopt technical standards, from those that provide

the backbones and telecommunication services, to those that offer access and content. The fact that the internet is under private control should not be an excuse for preventing the realisation of human rights in the online environment and, therefore, states are required to promote and protect human rights against the abuse of non-state actors. This does not prevent the adoption of an international instrument on corporate human rights responsibility, particularly for cases in which a government cannot or does not want to enforce this through domestic remedies.¹⁵

The actual problem: Human rights enforcement

International human rights law provides rules applicable to a system for global mass online surveillance. What the case of the NSA shows, instead, is a different problem in current international law. There is a loophole in the enforcement of human rights with respect to those recalcitrant countries that fail to adjust their domestic laws and policy measures to human rights standards.¹⁶ Domestic mechanisms of enforcement may help, if available, but they are insufficient when resolving issues based on mere parochial law standards, or a narrow-minded legal approach. There are certain mechanisms available in international forums, but they tend to be political rather than legal in nature. Unfortunately, in the case of the NSA, the US has not recognised the jurisdiction of any international courts. Therefore, it seems unfeasible that any legally binding decision on the matter of whether a system for global mass online surveillance violates international human rights law will be made.

The harms of surveillance to privacy, expression and association

Jillian York
Electronic Frontier Foundation
www.eff.org

Freedom is the freedom to say that two plus two make four. If that is granted, all else follows.

GEORGE ORWELL, 1984

On 5 June 2013, the *Washington Post* and the *Guardian* simultaneously published documents that would rock the world. The documents, leaked by ex-National Security Agency (NSA) contractor Edward Snowden, were not the first disclosures about the United States' vast surveillance complex, but have arguably had the most impact.

Before last year, awareness of digital surveillance in the US – and indeed, in much of the world – was minimal. Disclosures made by WikiLeaks in 2011 can be credited for an uptick in reporting on surveillance¹ – particularly in the Middle East – but did little to inspire research on the societal impact of it.

The knowledge, or even the *perception*, of being surveilled can have a chilling effect. A 2012 industry study conducted by the World Economic Forum found that in high internet penetration countries, a majority of respondents (50.2%) believe that “the government monitors what people do on the Internet.” At the same time, only 50% believe that the internet is a safe place for expressing their opinions, while 60.7% agreed that “people who go online put their privacy at risk.”²

A member survey conducted by writers' organisation PEN American Center in December 2013 discovered that, since the publication of the first NSA leaks, 28% of respondents have “curtailed or avoided social media activities,” while another 24% have “deliberately avoided certain topics in phone

or email conversations.” Perhaps even more worryingly, a full 16% have avoided writing or speaking on certain topics.³

Surveillance affects us in myriad ways. It infringes on our personal freedoms, submits us to state control, and prevents us from progressing as a society.

The equal rights to privacy, speech and association

When we talk about surveillance, it often follows that we speak of the importance of privacy, of being free from observation or disturbance, from public attention. In the US, privacy is a fundamental right, enshrined in the Fourth Amendment to the Constitution.

Of course, this is no coincidence – under King George II, the American colonisers found themselves at the mercy of writs of assistance, court-issued orders that allowed the King's agents to carry out wide-ranging searches of anyone, anytime; a precursor to the modern surveillance state.⁴ Once issued, an individual writ would be valid for the King's entire reign, and even up to six months past his death.

It was only after the death of King George II that a legal challenge was mounted. When a customs officer in Boston attempted to secure new writs of assistance, a group of Boston merchants, represented by attorney James Otis, opposed the move. Otis argued that the writs placed “the liberty of every man in the hands of every petty officer,” an argument that founding father John Adams later claimed “breathed into this nation the breath of life.” It was from this societal shift that the Fourth Amendment was born.

The opposition to surveillance, however, is not borne only out of a desire for privacy. In the United States, the First Amendment – that which

¹⁵ United Nations General Assembly, Resolution on elaboration of an international legally binding instrument on transnational corporations and other business enterprises with respect to human rights, UN Doc. A/HRC/26/L.22/Rev.1, 25 June 2014.

¹⁶ Louis Henkin, *International Human Rights Standards in National Law: The Jurisprudence of the United States*, in Benedetto Conforti and Francesco Francioni (eds.), *Enforcing International Human Rights in Domestic Courts* (Martinus Nijhoff Publishers, 1997), pp. 189–205.

¹⁴ Such as IP addresses and domain names.

¹ CNet. (2011, December 1). Wikileaks disclosure shines light on Big Brother. *CBS News*. www.cbsnews.com/news/wikileaks-disclosure-shines-light-on-big-brother

² Dutton, W., Law, G., Bolsover, G., & Dutta, S. (2013). *The Internet Trust Bubble: Global Values, Beliefs, and Practices*. Davos: World Economic Forum. www3.weforum.org/docs/WEF_InternetTrustBubble_Report2_2014.pdf

³ The FDR Group. (2013). *Chilling Effects: N.S.A. Surveillance Drives U.S. Writers to Self-Censor*. New York: PEN America. www.pen.org/sites/default/files/Chilling%20Effects_PEN%20American.pdf

⁴ Snyder, D. (n/d). *The NSA's "General Warrants": How the Founding Fathers Fought an 18th Century Version of the President's Illegal Domestic Spying*. San Francisco: Electronic Frontier Foundation. <https://www.eff.org/files/efile/node/att/generalwarrantsmemo.pdf>

prohibits the creation of law “respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances”⁵ – is often debated, but rarely restricted. It is a set of rights that is paramount in US culture; as Supreme Court Justice Hugo L. Black once stated:

First in the catalogue of human liberties essential to the life and growth of a government of, for, and by the people are those liberties written into the First Amendment of our Constitution. They are the pillars upon which popular government rests and without which a government of free men cannot survive.⁶

Article 19 of the Universal Declaration of Human Rights similarly provides for the right to freedom of opinion and expression, to “seek, receive and impart information and ideas through any media and regardless of frontiers.”⁷

Documents leaked by Edward Snowden in 2013 have demonstrated the extraordinary breadth of the US’s and other governments’ mass surveillance programmes, programmes which constitute an intrusion into the private lives of individuals all over the world.

The violation of privacy is apparent: indiscriminate, mass surveillance goes against the basic, fundamental right to privacy that our predecessors fought for. The negative effects of surveillance on the fundamental freedoms of expression and association may be less evident in an era of ubiquitous digital connection, but are no less important.

In a 2013 report, Frank La Rue, Special Rapporteur to the United Nations on the promotion and protection of the right to freedom of opinion and expression, discussed the ways in which mass surveillance can harm expression. He wrote:

Undue interference with individuals’ privacy can both directly and indirectly limit the free development and exchange of ideas. Restrictions of anonymity in communication, for example, have an evident chilling effect on victims of all forms of violence and abuse, who may be reluctant to report for fear of double victimization.⁸

The harmful effects of surveillance on expression and association are undeniably linked – the right to organise is imperative for political expression and the advancement of ideas. In the US, although the two rights are linked in the First Amendment, historically, they have sometimes been treated separately.

In a landmark 1958 case, *NAACP v. Alabama*, the Supreme Court of the US held that if the state forced the National Association for the Advancement of Colored People (NAACP) to hand over its membership lists, its members’ rights to assemble and organise would be violated.⁹ This case set the precedent for the Supreme Court’s foray into the constitutionally guaranteed right to association after decades of government attempts to shun “disloyal” individuals.

Justice John Marshall Harlan wrote for a unanimous court:

This Court has recognized the vital relationship between freedom to associate and privacy in one’s associations. Compelled disclosure of membership in an organization engaged in advocacy of particular beliefs is of the same order. Inviolability of privacy in group association may in many circumstances be indispensable to preservation of freedom of association, particularly where a group espouses dissident beliefs.¹⁰

Today, the data collected by the NSA’s various surveillance programmes poses a similar threat to the collection of membership lists. The vast majority of what the NSA collects is *metadata*, an ambiguous term that in this case describes the data surrounding one’s communications. That is to say, if the content of one’s phone call is the data, the metadata could include the number called, the time of the call, and the location from which the call was made.

The danger in metadata is that it allows the surveiller to map our networks and activities, making us think twice before communicating with a certain group or individual. In a surveillance state, this can have profound implications: Think of Uganda, for example, where a legal crackdown on lesbian, gay, bisexual and transgender (LGBT) activists is currently underway. Under surveillance, a gay youth seeking community or health care faces significant risks just for the simple act of making a phone call or sending an email.

In many countries, there has long been a legal distinction between the content of a message (that is, the message itself), and the “communications

data”, or metadata. This distinction is based on the traditional model of postal mail, where information written on the outside of an envelope is distinguished from the content of the envelope. This distinction is, however, rendered nearly meaningless by modern surveillance methods, which can capture far more than the destination of a communication, and *en masse*.¹¹

In order to argue effectively for and reclaim the right to associate freely without surveillance, it is imperative that such a distinction be made. Digital metadata is different from analogue metadata and its wide-scale capture creates a chilling effect on speech and association. It is time for fresh thinking on the impact of the culture of surveillance on our daily habits.

Changing culture, changing habits

The way that we interact on the internet is undoubtedly changing as a result of our knowledge of mass surveillance. Fortunately, fear and withdrawal are not the only reaction to this knowledge; our habits are changing as well. A September 2013 Pew survey found that 86% of internet users have taken steps to “remove or mask their digital footprints” – steps ranging from clearing cookies to encrypting their email. A further 55% of users have taken steps to avoid observation by *specific* people, organisations, or the government.¹²

Corporations – lambasted for their alleged cooperation with the NSA – are responding to the increased public awareness of mass surveillance as well. In early 2013, before the Snowden revelations, encrypted traffic accounted for 2.29% of all peak hour traffic in North America; now it spans 3.8%. In Europe and Latin America, the increase in encrypted traffic is starker: 1.47% to 6.10% and 1.8 to 10.37%, respectively.¹³

It is also telling that journalism organisations have stepped up in the wake of the Snowden

revelations, putting into place systems that will protect future whistleblowers. Jill Abramson, former executive editor of the *New York Times*, stated in 2013 that “[surveillance has] put a chill on really what’s a healthy discourse between journalists and our sources, and it’s sources who risk going to prison.”¹⁴ This realisation has led several publications – including the *Guardian* and the *Washington Post* – to implement a whistleblower platform called SecureDrop, which allows sources to share information with media organisations anonymously and securely.

Similarly, the public discussion around the use of encryption is also growing, as is the funding and development of privacy-enhancing technologies. Governmental and quasi-governmental organisations, such as the US State Department and Broadcasting Board of Governors, as well as non-profits such as the Freedom of the Press Foundation, have increased funding toward tools that can be used to thwart surveillance attempts.

The aforementioned Pew study found that 68% of internet users believe laws are insufficient in protecting their privacy online.¹⁵ Numerous attempts have been made globally to effect change through legal and political channels. The 13 Principles for the Application of Human Rights to Communications Surveillance,¹⁶ developed prior to the Snowden revelations, provides a framework for policy making at the state level. Many of the Principles’ 400-plus signatories are utilising the document in their policy advocacy.

As awareness of mass surveillance increases among the populace, it follows that new tactics for opposing it will arise. Given the complex nature of digital spying and the interlinked set of rights it affects, this is imperative. Ending mass surveillance requires consideration not only of its effect on privacy, but its impact on expression and association as well.

5 U.S. Constitution, Amendment I.

6 Ball, H. (1996). *Hugo L. Black: Cold Steel Warrior*. Oxford: Oxford University Press.

7 Universal Declaration of Human Rights, article 19.

8 United Nations Human Rights Council. (2013) *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue*. A/HRC/23/40. un.org/A/HRC/23/40

9 N.A.A.C.P. v. Alabama. 357 U.S. 449 (1958).

10 Ibid.

11 Electronic Frontier Foundation, Article 19. (2014). *Necessary & Proportionate International Principles on the Application of Human Rights to Communications Surveillance: Background and Supporting International Legal Analysis*. <https://necessaryandproportionate.org/files/legalanalysis.pdf>

12 Rainie, L., Kiesler, S., Kang, R., & Madden, M. (2013). *Anonymity, Privacy, and Security Online*. Washington, D.C.: Pew Research Center. www.pewinternet.org/files/old-media//Files/Reports/2013/PIP_AnonymityOnline_090513.pdf

13 Finley, K. (2014, May 16). Encrypted Web Traffic More Than Doubles After NSA Revelations. *Wired*. www.wired.com/2014/05/sandvine-report/

14 Gold, H., & Byers, D. (2013, October 18) Abramson: ‘Nobody won’ the shutdown; N.Y. Times: ‘Obama emerged the winner’. *Politico*. www.politico.com/blogs/media/2013/10/abramson-nobody-won-the-shutdown-ny-times-obama-emerged-175413.html

15 Rainie, L., Kiesler, S., Kang, R., & Madden, M. (2013). Op. cit.

16 Access, Article 19, Asociación Civil por la Igualdad y la Justicia, Asociación por los Derechos Civiles, Association for Progressive Communications, Bits of Freedom, Center for Internet & Society India... (2013, July 10). *13 Principles for the Application of Human Rights to Communications Surveillance*. <https://en.necessaryandproportionate.org/text>

Cyber security, civil society and vulnerability in an age of communications surveillance

Alex Comninos and Gareth Seneque

Justus-Liebig University Giessen and Geist Consulting¹
Comninos.org

Introduction

Cyber security is increasingly important to internet users, including stakeholders in governments, the private sector and civil society. As internet users increase, so does the amount of malware,² fuelled by ubiquitous smartphones and social networking applications offering new vectors for infection. Botnets – networks of infected devices controlled by malicious operators – are used as proxies to commit criminal acts including fraud and identity or data theft. According to the antivirus company Symantec, in 2013 data breach incidents resulted in the exposure of 552 million personal identities.³ In May 2014, eBay announced that hackers had gained access to the personal data of 145 million customers and urged all customers to change their passwords.⁴ Infrastructures connected to the internet, such as power grids, are also vulnerable, and severely lacking security updates. A growing “internet of things”, which includes ubiquitous devices from sensors in homes and cars to medical technology, presents a plethora of new vulnerabilities to cyber security incidents.

Increasingly, states are establishing military “cyber units” or “cyber commands”, many of which have offensive hacking capabilities.⁵ Michael Hayden, a former director of both the CIA and the National Security Agency (NSA) has stated that Stuxnet, a state-sponsored computer worm discovered in 2011 and designed to attack and incapacitate nuclear reactors in the Natanz facility in Iran, marked

“the crossing of the Rubicon” (a point of no return) for the use of state-sponsored malware.⁶ A number of similar worms, some of which have implemented Stuxnet’s source code, have arisen.⁷

Civil society organisations and human rights defenders are becoming victims of surveillance software. Some of this software is sold to law enforcement and intelligence agencies in repressive regimes. “Remote Access Trojans” can be bought both legally and on the black market, as well as downloaded for free, and are used to control mobile devices, laptops and computers remotely, capturing all the information input/viewed by the user. Such software has been used to target activists in Bahrain and Syria.⁸

Edward Snowden’s disclosures of documentary evidence regarding mass surveillance by the NSA, Government Communications Headquarters (GCHQ) in the United Kingdom, and other intelligence agencies of the “Five Eyes”⁹ countries have shown just how vulnerable the average netizen’s communications are to interception and surveillance. The disclosures have also demonstrated how surveillance activities can negatively affect the cyber security of all internet users.

It is tempting to think that more “cyber security” would be a means of countering the global privacy invasion caused by mass surveillance. However, cyber security discourse is dominated by states and corporations and focuses mainly on their security, rather than the security of civil society and of internet users. Civil society needs a vision of cyber security that puts the digital security of internet users at the centre of its focus. Attaining cyber security that protects human rights, including the

right to privacy, while also ensuring an open and secure internet, will not be possible unless dominant discourses on cyber security radically change.

The problems with “cyber security”

The term “cyber security” often lacks clear definition. It is used as an umbrella concept covering a range of threats and responses¹⁰ involving national infrastructure, internet infrastructure, applications and software, and users. Sometimes it is even used to refer to the stability of the state and political structures. The inexact terminology of cyber security “mixes legitimate and illegitimate concerns and conflates different types and levels of risk.” This “prevents genuine objective scrutiny, and inevitably leads to responses which are wide-ranging and can easily be misused or abused.”¹¹ Cyber security not only leads to overly broad powers being given to the state, it also “risks generating a consensus that is illusory” and not useful for the problems at hand.¹² We need to carefully unpack the relevant issues and develop “a clear vocabulary of cyber security threats and responses,” so as to enable “targeted, effective, and rights-respecting policies.”¹³ If we do not, cyber security can be used by governments as a justification to censor, control or surveil internet use.

Viewing cyber security as an issue of national security is perilous and unhelpful. We should distinguish between, and not conflate, on the one hand, protecting computers, networks and information, and on the other hand using technological tools to achieve security objectives. Using “cyberspace as a tool for national security, both in the dimension of war fighting and the dimension of mass surveillance, has detrimental effects on the level of cyber security globally.”¹⁴ When cyber security is framed as a national security issue, issues regarding technology and the internet are *securitised* – brought onto the security agendas of states. This may be counter-productive. The state, law enforcement, military and intelligence agencies may not have the best skills or knowledge for the job. State actors may have a con-

flict of interest in securing information: militaries, for example, may want to develop offensive weapons, while intelligence agencies may rely on breaking or circumventing information insecurity in order to surveil better. Cyber security may also be used to protect state secrets, and criminalise whistleblowers as cyber security threats. Focusing on the state and “its” security, “crowds out consideration for the security of the individual citizen, with detrimental effects on the security of the whole system.”¹⁵

Cyber security often disproportionately focuses on the protection of information, databases, devices, assets and infrastructures connected to the internet, rather than on the protection of connected users. Technological infrastructures and the assets of corporations are put at the centre of analysis, rather than human beings. Human beings are seen as a threat in the form of bad “hackers” or as a weak link in information systems, making mistakes and responding to phishing or “social engineering” attacks.¹⁶ Putting humans at the centre of cyber security is important. A definition of cyber security as purely protecting information avoids ethical challenges. Cyber security should not protect some people’s information at the expense of others. It should also not protect information about state secrets in order to enable mass surveillance and privacy invasion of individual users.

Cyber security and vulnerability

Cyber security discourse should focus more on information security *vulnerabilities*, rather than on threats and responses. This focus would help to delineate what constitutes a cyber security issue, avoid cyber security escalating to a counter-productive national security issue, and place a practical focus on the protection of all internet users.

A security vulnerability, also called a “bug”, is a piece of software code that contains an error or weakness that could allow a hacker to compromise the integrity, availability or confidentiality of information contained, managed or accessed by that software.¹⁷ When a vulnerability is discovered, a malicious hacker may make an “exploit”¹⁸ in order

¹ Alex Comninos is a doctoral candidate in the Department of Geography at Justus-Liebig University Giessen; Gareth Seneque is a Unix architect at Geist Consulting.

² Malware is malicious software that includes viruses, Trojan horses and spyware.

³ Symantec 2014 Internet Security Threat Report, Volume 19. www.symantec.com/security_response/publications/threatreport.jsp

⁴ Perloth, N. (2014, May 21). eBay Urges New Passwords After Breach. *New York Times*. www.nytimes.com/2014/05/22/technology/eBay-reports-attack-on-its-computer-network.html

⁵ Comninos, A. (2013). *A cyber security agenda for civil society: What is at stake?* Johannesburg: APC. www.apc.org/en/node/17320

⁶ Healy, J. (2013, April 16). Stuxnet and the Dawn of Algorithmic Warfare. *The Huffington Post*. www.huffingtonpost.com/jason-healey/stuxnet-cyberwarfare_b_3091274.html

⁷ Bencsáth, B. (2012). Duqu, Flame, Gauss: Followers of Stuxnet. Presentation at the RSA Conference Europe 2012, Amsterdam, the Netherlands, 10 October. www.rsaconference.com/writable/presentations/file_upload/br-208_bencsath.pdf

⁸ McMillan, R. (2011, August 7). How the Boy Next Door Accidentally Built a Syrian Spy Tool. *Wired*. www.wired.com/wiredenterprise/2012/07/dark-comet-syrian-spy-tool

⁹ The “Five Eyes” countries are Australia, Canada, New Zealand, the United Kingdom and the United States, which are part of a multilateral agreement on cooperation in signals intelligence.

¹⁰ Center for Democracy and Technology. (2013). *Unpacking “Cybersecurity”: Threats, Responses, and Human Rights Considerations*. <https://cdt.org/insight/unpacking-cybersecurity-threats-responses-and-human-rights-considerations>

¹¹ Kovacs, A., & Hawtin, D. (2014). Cyber Security, Surveillance and Online Human Rights. Discussion paper written for the Stockholm Internet Forum, 27-28 May. www.gp-digital.org/publication/second-pub

¹² OECD. (2012). *Non-governmental Perspectives on a New Generation of National Cyber security Strategies*, p 6. [dx.doi.org/10.1787/5k8zq925x138-en](https://doi.org/10.1787/5k8zq925x138-en)

¹³ Center for Democracy and Technology. (2013). Op. cit.

¹⁴ Dunn Cavelty, M. (2014). Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities. *Science and Engineering Ethics*, April.

¹⁵ Ibid.

¹⁶ Dunn Cavelty, M. (2014). Op. cit. Wikipedia defines social engineering as “psychological manipulation of people into performing actions or divulging confidential information.” [https://en.wikipedia.org/wiki/Social_engineering_\(security\)](https://en.wikipedia.org/wiki/Social_engineering_(security)) A common example is phishing.

¹⁷ For a definition upon which this is based, see Microsoft, Definition of a Security Vulnerability: technet.microsoft.com/en-us/library/cc751383.aspx

¹⁸ An exploit is a “is a piece of software, a chunk of data, or a sequence of commands that takes advantage of a bug, glitch or vulnerability in order to cause unintended or unanticipated behavior,” and does not require advanced technical skills to use. [https://en.wikipedia.org/wiki/Exploit_\(computer_security\)](https://en.wikipedia.org/wiki/Exploit_(computer_security))

to compromise data or access to a computer. Malware – viruses and Trojan horses – require exploits (or collections of exploits) that take advantage of vulnerabilities. Expertise in fixing vulnerabilities is improving but not keeping up with the pace of the growth. Compared to 15 years ago, all popular and contemporary desktop operating systems (Windows, Linux and Mac) offer regular automated security updates which fix or “patch” known vulnerabilities. While we are finding more vulnerabilities in code and viruses than ever before, we are also getting better at finding them. At the same time we keep producing more software code, meaning that the net number of vulnerabilities is increasing.¹⁹

Viruses and botnets, including Stuxnet and other state-sponsored malware, require vulnerabilities to work. Finding and fixing vulnerabilities contributes to a safer and secure internet, counters surveillance and can even save lives. For example, a vulnerability in Adobe’s Flash software was recently used against dissidents in Syria.²⁰

There are two categories of vulnerabilities, each requiring different user and policy responses: zero-days and forever-days. Zero-days are vulnerabilities for which there is no available fix yet, and may be unknown to developers. Forever-days are vulnerabilities which are known of, and either do not have a fix, or do have a fix in the form of a patch or an update, but they are for the most part not applied by users.

Zero-day vulnerabilities

When a zero-day is found, the original software developer should be notified so that they may find a fix for the vulnerability and package it as a patch or update sent out to users. Furthermore, at some stage, users of the affected software that are rendered vulnerable should also be informed, so they can understand if they are or have been vulnerable and take measures to recover and mitigate for the vulnerability.

Throughout the history of computers, “hackers”²¹ have sought to use technology in ways that were not originally intended. This has been a large source of technological innovation. Hackers have applied this logic to computer systems and have bypassed

security and found vulnerabilities for fun, fame, money, or in the interests of a more secure internet. It is because of people that break security by finding vulnerabilities that we can become more secure. A problem for cyber security is that “good” (or “white hat”) hackers or “security researchers” may not be incentivised to find zero-days and use this knowledge for good. Rather than inform the software vendor, the project involved, or the general public of a vulnerability, hackers may decide not to disclose it and instead to sell information about a vulnerability, or package it as an *exploit* and sell it.

These exploits have a dual use: “They can be used as part of research efforts to help strengthen computers against intrusion. But they can also be weaponised and deployed aggressively for everything from government spying and corporate espionage to flat-out fraud.”²² There is a growing market for zero-days that operates in a grey and unregulated manner. Companies sell exploits to governments and law enforcement agencies around the world; however, there are concerns that these companies are also supplying the same software to repressive regimes and to intelligence agencies. There is also a growing black market where these exploits are sold for criminal purposes.²³

Forever-day vulnerabilities

Forever-days (or “i-days”/“infinite-days”) are also a serious cyber security problem. Forever-day vulnerabilities either take a long time to get fixed, or never get fixed, or are fixed but users do not update or patch the relevant software. While they can affect internet users, they can also affect industrial control systems (ICSs), which control infrastructures such as power grids and power plants, as well as machinery in factories, for example, in pharmaceutical plants. ICSs require large investments in equipment that is supposed to last for many years. Operators of ICSs usually cannot afford to update their systems regularly. In addition to zero-days, well-documented forever-day vulnerabilities in Siemens controllers allowed the Stuxnet virus to infect the Natanz nuclear reactors in Iran.²⁴ Forever-days

in ICSs raise the spectre of “cyber war”, in which, for example, “terrorists” could attack and cripple power lines. The solution however requires software updates, rather than military involvement.

Windows XP is perhaps one of the most important cyber security threats this year for government, civil society and critical national infrastructures connected to the internet. Many industrial control systems are running on Windows XP. The security updates for Windows XP expired this year, meaning that computers running XP will be exposed to thousands of vulnerabilities.²⁵ It is hard for governments and civil society to say goodbye to Windows XP, especially in the developing world, and in low-budget environments. The software is easy to use, runs on old computers, can be customised, runs modern web browsers, and allows its users to fully participate in the information society using a 13-year old operating system. In April 2014, XP use still accounted for over 18% of desktop PC use.²⁶ The UK and Dutch governments and some corporations have recognised the severity of the problem, and are actually paying Microsoft for private updates.²⁷

The Heartbleed vulnerability

April 2014 marked an important watershed for awareness of vulnerabilities, with what has been described as one of the most catastrophic security vulnerabilities ever discovered: Heartbleed.

Heartbleed was a vulnerability in an open source software project called OpenSSL, which is used to establish encrypted connections between websites and browsers. According to *Forbes* magazine, “Some might argue that it is the worst vulnerability found (at least in terms of its potential impact) since commercial traffic began to flow on the Internet.”²⁸ The vulnerability allowed a potential hacker to steal private encryption keys from a web server, and by doing so, to hijack login credentials or decrypt sensitive information, leaving two-thirds of the web

open to eavesdropping.²⁹ The vulnerability existed for over two years, making a large proportion of the internet vulnerable. Heartbleed has not just had negative effects. It is the first vulnerability with its own logo,³⁰ and coverage of it extended far beyond technical audiences, engendering understanding of vulnerabilities among people who would usually not be aware of them. It has also resulted in more human and financial investment into OpenSSL development and alternatives.³¹

Open source software promises, in theory, to make software less vulnerable, as the code is open for anyone to review and to look for vulnerabilities. Open source software, however, will not provide security unless there are enough eyes on the code. Heartbleed was an open source project, and anyone could review the code, but it was underfunded and understaffed, and there were not enough reviewers of the code from outside the project. Symptomatic of this, the update that would introduce Heartbleed was finalised an hour before midnight on New Year’s Eve 2011, and would go unnoticed for two years.

The relevance of Snowden’s disclosures to cyber security

The scope and reach of the NSA’s surveillance is important. The NSA’s surveillance posture is – as has been repeated by General Keith Alexander, and is reflected in the NSA slide in Figure 1 – to “collect it all”:³² from undersea cable taps, to Yahoo video chats, to in-flight Wi-Fi, to virtual worlds and on-line multiplayer games like Second Life and World of Warcraft. The NSA has at least three different programmes to get Yahoo and Google user data. This shows that they try to get the same data from multiple mechanisms.³³ With the GCHQ under the MUSCULAR programme it hacked into the internal data links of Google and Yahoo³⁴ for information

19 McGraw, G. (2012). Cyber War, Cyber Peace, Stones, and GlassHouses. Presentation at the Institute for Security, Technology, and Society (ISTS), Dartmouth College, Hanover NH, USA, 26 April. www.ists.dartmouth.edu/events/abstract-mcgraw.html, www.youtube.com/watch?v=LCULzMa7iqs

20 Fisher, D. (2014, April 28). Flash zero day used to target victims in Syria. *Threat Post*. threatpost.com/flash-zero-day-used-to-target-victims-in-syria

21 “Hacker” is used here in its original usage to refer to people who playfully use technological systems, rather than in its current pejorative and widely used usage.

22 Gallagher, R. (2013, January 16). Cyberwar’s gray market. *Slate*. www.slate.com/articles/technology/future_tense/2013/01/zero_day_exploits_should_the_hacker_gray_market_be_regulated.html; Grossman, L. (2014, July 21). World War Zero: How Hackers Fight to Steal Your Secrets. *Time*. time.com/2972317/world-war-zero-how-hackers-fight-to-steal-your-secrets

23 Gallagher, R. (2013, January 16). Op. cit.

24 Zetter, K. (2011, August 4). Serious security holes found in Siemens control systems targeted by Stuxnet. *Ars Technica*. arstechnica.com/security/2011/08/serious-security-holes-found-in-siemens-control-systems-targeted-by-stuxnet Stuxnet also made use of four zero-days; see Kushner, D. (2013, February 26). The Real Story of Stuxnet. *IEEE Spectrum*. spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet

25 Windows XP Embedded (XPe), which should be the preferred operating system for ICSs, should receive updates till 2016. There is a suggested but unofficial workaround to make XP receive XPe updates, which may be useful for those with no other option (see: arstechnica.com/information-technology/2014/05/update-enabling-windows-xp-registry-hack-is-great-news-for-xp-die-hards).

26 Newman, J. (2014, May 1). Windows XP refuses to go down without a fight. *PC World*. www.pcworld.com/article/2150446/windows-xp-usage-wont-go-down-without-a-fight.html

27 Gallagher, S. (2014, April 6). Not dead yet: Dutch, British governments pay to keep Windows XP alive. *Ars Technica*. arstechnica.com/information-technology/2014/04/not-dead-yet-dutch-british-governments-pay-to-keep-windows-xp-alive

28 Steinberg, J. (2014, April 10). Massive Internet Security Vulnerability – Here’s What You Need To Do. *Forbes*. www.forbes.com/sites/josephsteinberg/2014/04/10/massive-internet-security-vulnerability-you-are-at-risk-what-you-need-to-do

29 Goodin, D. (2014, April 8). Critical crypto bug in OpenSSL opens two-thirds of the Web to eavesdropping. *Ars Technica*. arstechnica.com/security/2014/04/critical-crypto-bug-in-openssl-opens-two-thirds-of-the-web-to-eavesdropping

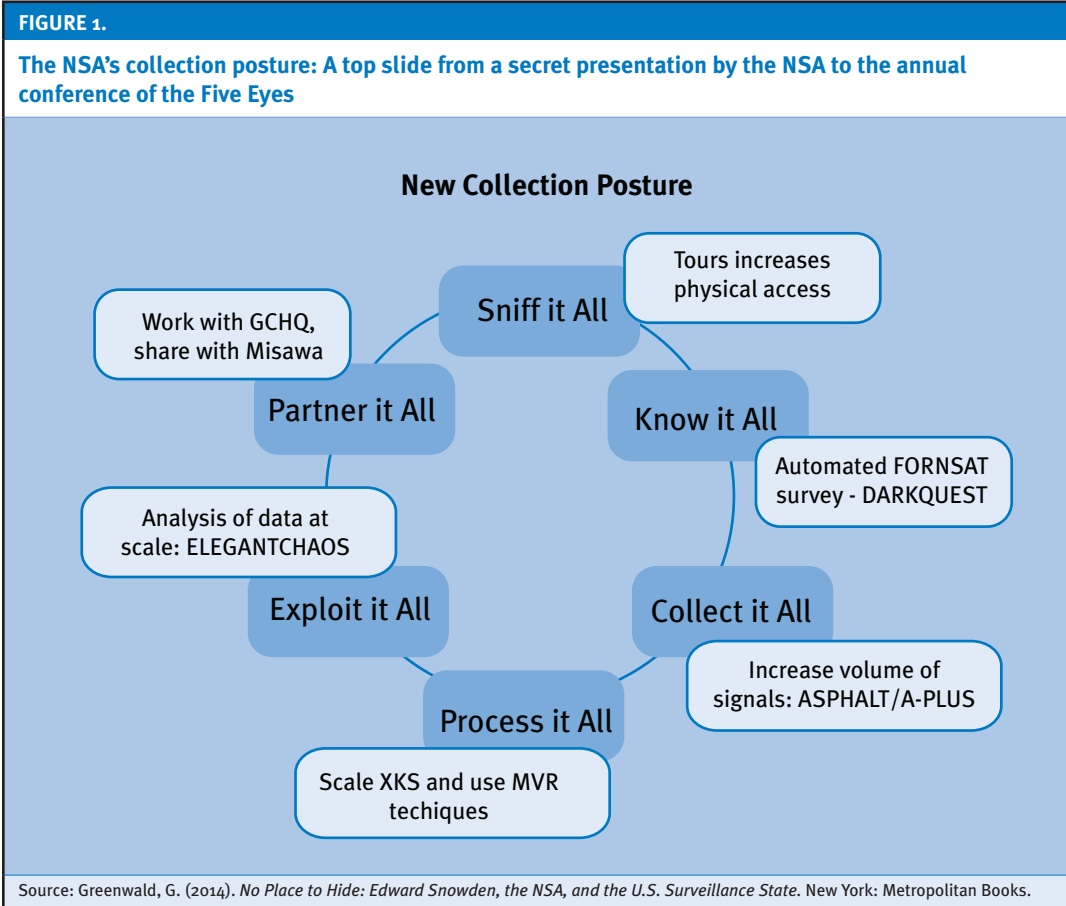
30 heartbleed.com/heartbleed.svg

31 There are two new “forks” or versions of OpenSSL that promise to be more secure. One is called BoringSSL and is developed by Google, and one is called LibreSSL and is developed by the OpenBSD Project.

32 Greenwald, G. (2014). *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*. New York, Metropolitan Books, p. 97.

33 Schneier, B. (2014). NSA Surveillance and What To Do About It. Presentation at the Stanford Center for Internet and Society, Stanford CA, USA, 22 April. https://youtube.com/watch?v=3ygt_loOgyl

34 Gellman, B., & Soltani, A. (2013, October 30). NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say. *The Washington Post*. www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html



that it could mostly have gotten through the PRISM programme. In addition to highlighting the NSA's massive institutional overreach and global privacy invasion, Snowden's disclosures also highlight the many points at which our data is insecure, and the vast numbers of vulnerabilities to surveillance that exist throughout our digital world. However, while the NSA is the largest threat in the surveillance game, it is not the only threat. Governments all around the world are using the internet to surveil their citizens. Considering the rate of technological change, it is not unforeseeable that the methods, tools and vulnerabilities used by the NSA will be the tools of states, cyber criminals and low-skilled hackers of the future. Regardless of who the perceived attacker or surveillance operative may be, and whether it is the NSA or not, large-scale, mass surveillance is a growing cyber security threat.

It has also been disclosed that the NSA and GCHQ have actively worked to make internet and technology users around the world less secure. The NSA has placed backdoors in routers running vital

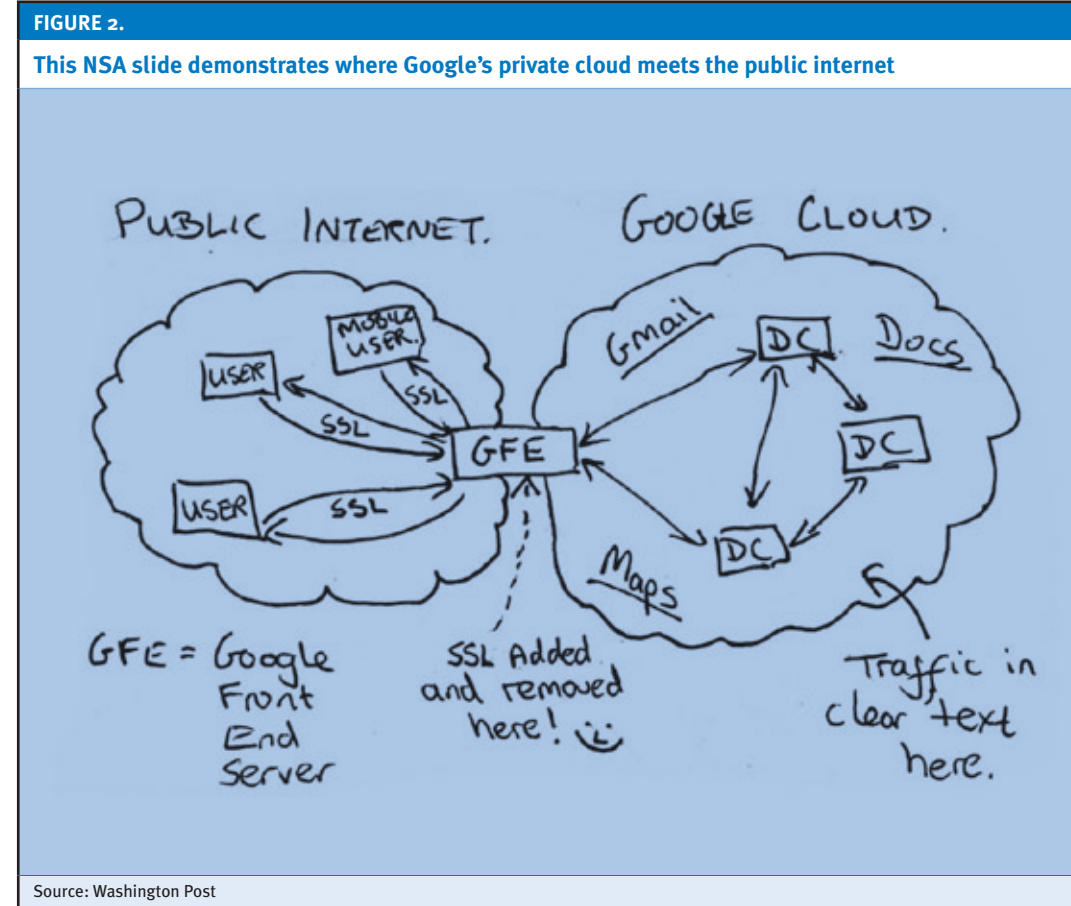
internet infrastructures.³⁵ The GCHQ has impersonated social networking websites like LinkedIn in order to target system administrators of internet service providers.³⁶ The NSA has been working with the GCHQ to hack into Google and Yahoo data centres.³⁷ The NSA also works to undermine encryption technologies, by covertly influencing the use of weak algorithms and random number generators in encryption products and standards.³⁸ The NSA in its own words is working under the BULLRUN programme to "insert vulnerabilities into commer-

35 Gallagher, S. (2014, May 14). Photos of an NSA "upgrade" factory show Cisco router getting implant. *Ars Technica*. arstechnica.com/tech-policy/2014/05/photos-of-an-nsa-upgrade-factory-show-cisco-router-getting-implant

36 Faviar, C. (2013, September 20). Snowden docs now show Britain, not NSA, targeted Belgian telco. *Ars Technica*. arstechnica.com/tech-policy/2013/09/snowden-docs-now-show-britain-targeted-belgian-telco-not-nsa

37 Gellman, B., & Soltani, A. (2013, October 30). Op. cit.

38 Guess, M. (2013, September 11). New York Times provides new details about NSA backdoor in crypto spec. *Ars Technica*. arstechnica.com/security/2013/09/new-york-times-provides-new-details-about-nsa-backdoor-in-crypto-spec



cial encryption systems, IT systems, networks, and endpoint communications devices used by targets" and to "influence policies, standards and specifications for commercial [encryption] technologies."³⁹ The NSA is also believed to hoard knowledge about vulnerabilities rather than sharing them with developers, vendors and the general public,⁴⁰ as well as even maintaining a catalogue of these vulnerabilities for use in surveillance and cyber attacks.⁴¹ None of these activities serve to make the internet more secure. In fact, they do the very opposite.

39 New York Times. (2013, September 5). Secret Documents Reveal N.S.A. Campaign Against Encryption. *New York Times*. www.nytimes.com/interactive/2013/09/05/us/documents-reveal-nsa-campaign-against-encryption.html

40 Electronic Frontier Foundation. (2014, July 1). EFF Sues NSA, Director of National Intelligence for Zero Day Disclosure Process. *EFF*. <https://www.eff.org/press/releases/eff-sues-nsa-director-national-intelligence-zero-day-disclosure-process>

41 Appelbaum, J., Horchert, J., & Stöcker, C. (2013, September 29). Shopping for Spy Gear: Catalog Advertis NSA Toolbox. *www.spiegel.de/international/world/catalog-advertis-nsa-has-backdoors-for-numerous-devices-a-940994.html*

As US Congresswoman Zoe Lofgren commented: "When any industry or organisation builds a backdoor to assist with electronic surveillance into their product, they put all of our data security at risk. If a backdoor is created for law enforcement purposes, it's only a matter of time before a hacker exploits it, in fact we have already seen it happen."⁴²

The fact that the NSA is actively working to make the internet insecure points to the contradictions in its dual mandate: simultaneously securing and breaking cyber security. On the one hand it is tasked with securing information and communications networks (falling under its "Information Assurance" mandate), and on the other hand it is tasked with surveilling information and communications networks (its "Signals Intelligence" mandate).⁴³ Similar tensions exist within the US military, which

42 National Insecurity Agency: How the NSA's Surveillance Programs Undermine Internet Security. Panel discussion at the New America Foundation, 8 July 2014. <https://youtube.com/watch?v=K1ox5vwnJZA>

43 Ibid.

is tasked with both defending national networks from hacking attacks as well as with conducting offensive hacking attacks. The US “cyber command”, the military command for the “cyber domain”, is under the stewardship of the NSA commander. This conflict of interest in the NSA’s dual role has not been addressed in current NSA reform. Tasked with “national security”, intelligence agencies like the NSA have a conflicting mandate that cannot enable them to actually provide US citizens with cyber security, in the same way that states are for example able to provide us with physical security. It will always be against the interests of intelligence agencies to assure the provision of secure technologies that cannot be eavesdropped on. This is exacerbated by a cyber security-surveillance industrial complex of government agencies and private contractors selling hacking and surveillance products, with revolving doors between the two. We need to be very wary of intelligence agencies being given roles as stewards of cyber security.

Similarly, we cannot look to corporations for protection. Through mechanisms of intermediary liability, corporations are pressured by governments into cooperating with governments in surveillance programmes like PRISM, or the “Snoopers Charter” in the United Kingdom.⁴⁴ It would also not be within the interests of many tech companies to protect privacy and security to the extent that data is fully encrypted, not just during transit, but also in storage. Google’s “Chief Internet Evangelist” Vint Cerf stated at the Internet Governance Forum in 2011 that this would not be in Google’s interest, as “we couldn’t run our system if everything in it were encrypted because then we wouldn’t know which ads to show you.”⁴⁵

Recommendations

Civil society needs to articulate an agenda for cyber security that puts the security of human beings at the centre of the debate.

Making cyber security a national security issue can be counterproductive due to its potential for abuse. Cyber security also may be better dealt with by the technical community, the private sector and civil society. The state and military may not always be best suited to dealing with cyber security, and

intelligence agencies may have a conflict of interest in ensuring cyber security.

Civil society needs to be wary of putting too much trust in either governments or corporations for assuring cyber security. Responsibility for cyber security should be distributed and not concentrate power too much in one particular place.⁴⁶

Cyber security starts at home. Security is a collective effort that comes with collective responsibilities. If we are insecure, if we do not encrypt our communications, then those who we communicate with are also insecure. We therefore have a responsibility towards ourselves, but also towards others to secure our communications. All users should run modern operating systems and software that receive security updates, run an antivirus, and try to encrypt as much communications as possible.

Widespread use of encryption and privacy tools. Encryption protects communications from a multitude of cyber threats, including surveillance, theft and hacking. Encryption cannot fully protect us from surveillance, as it does not hide the metadata (for example, who the sender and recipient of the email are). Through metadata, a picture of our associations may be drawn, and anonymity tools provide another measure of protection from this. Edward Snowden’s revelations have taught us that there are some tools that do work. PGP encryption is effective at encrypting email communications. The anonymity tool TOR, if used correctly, will work to anonymise communications and provide an extra layer of privacy on top of encryption. The lengths to which the NSA and GCHQ have gone (mostly unsuccessfully) to crack TOR is evidence of this. These tools can be complicated to use, but with a little training they are within the reach of many internet users.⁴⁷

Encryption as resistance against mass surveillance. Encryption may not always work in the future, as quantum computers may decrypt our stored communications.⁴⁸ Snowden’s revelations have also shown us how easy it is for intelligence agencies (like the NSA) to influence encryption

standards and implementation. Vulnerabilities in software will always allow cryptography and anonymisation tools to be bypassed,⁴⁹ and it is always easier to hack someone than to crack encryption. Widespread use of encryption, however, increases the cost of mass surveillance. It can be an effective way of containing and restricting mass surveillance, as it increases the cost to whomever is doing the spying, through the need for increased processing, capture and storage of data. Widespread use of encryption could force intelligence agencies like the NSA or GCHQ to focus on targeted interception, rather than bulk collection.⁵⁰ Encryption is becoming increasingly more widespread after Snowden’s revelations. Yahoo, late to encryption, has finally turned on encryption as default for connections to its mail client. Both Google and Yahoo have begun encrypting internal links in their network. Widespread use of encryption and privacy tools does not just protect us from the NSA; they also help to mitigate a whole range of cyber security threats, from espionage to fraud to cyber attacks on activists and dissidents.

The wider use of up-to-date free/libre and open source software. The use of free/libre and open source software (FLOSS or FOSS) is another way in which we can increase our cyber security. FLOSS software is open source, which means that the source code is available for anyone to read. Vulnerabilities can be found more easily in open source code than they can in proprietary software. It is harder for malicious actors to purposively insert vulnerabilities (“backdoors”) in FLOSS software. The example of Heartbleed has taught us that there are not always enough eyes reviewing security-critical software code, and that human investment in security-critical open source software and in open source code review is needed.

We have also identified a common use case which highlights the potential benefits of a shift to open source software: Windows XP. As Microsoft no longer provides security updates, XP users will be open to thousands of vulnerabilities, the quantity of which will only grow over time. The push to migrate users off this platform will continue, with governments/business (particularly in developing countries) increasingly adopting FLOSS as an

alternative.⁵¹ GNU/Linux, a FLOSS operating system, can run on old computers and still receive security updates, which are free of charge and shared between new and old systems. GNU/Linux allows for security updates that are mainly software based, and can mitigate the need for buying new hardware.

More explicit focus needs to be placed on vulnerabilities in cyber security discourse. Security researchers need to be incentivised to disclose vulnerabilities in software and hardware to the vendors involved or the users infected, rather than selling this information to intelligence agencies, cyber criminals and other malicious actors. An example of positive incentivisation may be “bug bounty” programmes, which reward security researchers with fame, recognition and money for finding and disclosing vulnerabilities to the software vendors involved. Microsoft, Google, Twitter and many other big-tech companies are starting to employ such programmes. As malicious actors may always offer more money for vulnerabilities, it may be necessary to investigate regulating the market in zero-days.⁵² This should be done carefully, however, without criminalising security researchers and putting them at risk for doing beneficial work.

It is also essential for governments and civil society to also be concerned with forever-day vulnerabilities. The use of Windows XP should immediately cease, and industrial control systems controlling national infrastructures like power grids should be immediately migrated to systems receiving modern security updates, or firewalled or air-gapped from the internet.

Cyber security is augmented by strong data protection rules. These rules should include requirements that companies or organisations encrypt and secure data, should regulate the sharing of data with third parties, and should have requirements that companies inform clients and customers when there are data breaches that have affected their security.

Information sharing. The proposed Cybersecurity Information Sharing Act (CISA) in the US requires private sector companies to hand over information about cyber threats to the Department of Homeland Security: According to *The Guardian*:

⁵¹ See en.wikipedia.org/wiki/List_of_Linux_adapters for a list of organisations who have moved over to Linux, an open source operating system.

⁵² A proposal for such regulation is outlined in Gaycken, S., & Lindner, F. (2012). Zero-Day Governance: an (inexpensive) solution to the cyber security problem. Paper submitted to Cyber Dialogue 2012: What Is Stewardship in Cyberspace?, Toronto, Canada, 18-19 March. www.cyberdialogue.citizenlab.org/wp-content/uploads/2012/2012papers/CyberDialogue2012_gaycken-lindner.pdf

⁴⁴ Grice, A. (2014, July 11). Emergency data law: David Cameron plots to bring back snoopers’ charter. *The Independent*. www.independent.co.uk/news/uk/politics/emergency-data-law-government-railroading-through-legislation-on-internet-and-phone-records-9596695.html

⁴⁵ Soghoian, C. (2011, November 2). Two honest Google employees: our products don’t protect your privacy. *Slight Paranoia*. paranoia.dubfire.net/2011/11/two-honest-google-employees-our.html

⁴⁶ Ron Deibert has made this argument in: Deibert, R. (2012). *Distributed Security as a Cyber Strategy: Outlining a Comprehensive Approach for Canada in Cyberspace*. Calgary: Canadian Defence and Foreign Affairs Institute. www.cdfai.org/PDF/Distributed%20Security%20as%20Cyber%20Strategy.pdf

⁴⁷ Guidelines on securing oneself online are available at securityinabox.org, cryptoparty.org, or en.flossmanuals.net/basic-internet-security

⁴⁸ There are concerns around how encrypted information, captured and stored, could in the future be decrypted as quantum computing advances (ushering in an age of “post-quantum cryptography”); however, this is a long-term consideration. See: Arcieri, T. (2013, July 9). Imperfect Forward Secrecy: The Coming Cryptocalypse. *Tony Arcieri*. tonyarcieri.com/imperfect-forward-secrecy-the-coming-cryptocalypse

⁴⁹ At the time of writing, researchers have revealed that there are serious vulnerabilities in the TOR, I2P and TAILS anonymisation tools, but have not revealed the details. Regarding TOR, this is because of legal concerns, and regarding I2P and TAILS, the researcher has not fully disclosed the details.

⁵⁰ Schneier, B. (2014, February 10). NSA Surveillance and What To Do About It. Presentation at MIT, Cambridge MA, USA, 10 February. bigdata.csail.mit.edu/node/154

It is written so broadly it would allow companies to hand over huge swaths of your data – including emails and other communications records – to the government with no legal process whatsoever. It would hand intelligence agencies another legal authority to potentially secretly re-interpret and exploit in private to carry out even more surveillance on the American public and citizens around the world. And even if you find out a company violated your privacy by handing over personal information it shouldn't have, it would have immunity from lawsuits – as long as it acted in “good faith”. It could amount to what many are calling a “backdoor wiretap”, where your personal information could end up being used for all sorts of purposes that have nothing to do with cybersecurity.

Information sharing, while infringing our privacy, is also a threat to cyber security: as more information is shared with third parties, it becomes harder to secure. Furthermore, surveillance is not a solution to the problems of cyber security, as this report has shown. If we want to meaningfully talk about interventions in information sharing and cyber security, then we should talk about vulnerabilities. Rather than information about “threats” or about the personal lives of internet users being shared, information about vulnerabilities that affect our security need to be shared with all stakeholders – governments, developers, vendors and internet users – in a responsible manner, so that this information cannot be hoarded and used to weaken all of our cyber security.

From digital threat to digital emergency

Fieke Jansen

Hivos, the Digital Defenders Partnership
www.digitaldefenders.org

Introduction

In recent years there has been a crackdown on internet freedom and increased targeting of the communication of journalists, bloggers, activists and citizens. During times of social or political crisis, communication lines have been shut down and critical forms of expression are met with censorship, harassment and arrests. Our communication is under surveillance, intercepted and collected without our knowledge or active consent, and is used for the profiling of people and spying on networks by governments and commercial companies. These acts of censorship and targeted surveillance are undermining our freedom of speech and our basic human rights, and lead to digital emergencies for those who are targeted. In this fast-changing political and technological environment there is an urgent need to understand the risks, protect those critical internet users who are being targeted, and expose surveillance practices.

Challenges, threats and digital emergency

The first time people started uttering the term “digital emergency” was when former Egyptian president Hosni Mubarak pulled the internet kill switch during the protests in 2011, leaving Egypt without internet communication.¹ However, digital emergencies are not only related to an internet kill switch: for the Digital Defenders Partnership² a digital emergency is an urgent need for assistance arising from digital threats to the security of an individual or organisation. A digital threat can include cyber attacks, vulnerabilities to communication infrastructure, unsafe data use, compromising of devices, stealing of equipment, legal proceedings

or weak digital security practices. There are three levels at which to distinguish digital attacks and communication surveillance that can lead to a digital emergency: infrastructure, censoring of content and profiling of people.

Infrastructure

Communication is often referred to as the interaction that happens between people, a stream of words whether they take place on- or offline. Yet very few of us realise that all digital communication runs on a physical communications infrastructure that consists of several “layers” made, owned or operated by different commercial and state entities. The Open systems interconnection model distinguishes seven different layers in the internet architecture that range from the physical layer (e.g. copper and fibre optical cables) up to the application layer (e.g. https and email protocol).³ Depending on a state's technical capabilities, access to the infrastructure, as well as to service providers, surveillance and censorship methods may differ. In some cases a government can engage in sea-cable tapping, which requires direct access to the physical infrastructure layer, or use an application layer exploit, where internet or mobile traffic is monitored through exploiting a vulnerability in the transport layer encryption (https), as in the case of Heartbleed.⁴ Partial network interference, called throttling, is also possible.

The fact that infrastructure is made, owned or operated by different entities makes our communication vulnerable to censorship and surveillance. Since Mubarak pulled the internet kill switch in 2011, other mobile and internet blackouts in Pakistan, Syria and other places have become more visible. These usually take place in times of military, political or social unrest.^{5, 6}

¹ Aljazeera. (2011, January 28). When Egypt turned off the internet. *Aljazeera*. www.aljazeera.com/news/middleeast/2011/01/2011128796164380.html

² Digital Defenders Partnership, a programme that aims to mitigate digital threats to human rights defenders, bloggers, journalists and activists in internet repressive and transitional environments. <https://digitaldefenders.org>

³ https://en.wikipedia.org/wiki/OSI_model

⁴ The Heartbleed bug. heartbleed.com

⁵ Article 19 (2012). Pakistan: Government must stop 'kill switch' tactics. Statement by Article 19. www.article19.org/resources.php/resource/3422/en/pakistan:-government-must-stop-%27kill-switch%27-tactics

⁶ Franceschi-Bicchierai, L. (2013, August 29). Does Syria Have an Internet Kill Switch? *Mashable*. www.mashable.com/2013/08/29/syria-internet-kill-switch

In April 2014 the Heartbleed vulnerability, a critical flaw in OpenSSL, was discovered. As one analyst put it: “[OpenSSL] is a software which is used to secure hundreds of thousands of websites, including major sites like Instagram, Yahoo, and Google. This security exploit can give attackers access to sensitive information like logins and passwords, as well as session cookies and possibly SSL keys that encrypt all traffic to a site.”⁷ Other than the security hole there were two major problems with Heartbleed. The first was that the National Security Agency (NSA) in the United States knew about this vulnerability for at least two years and used it to intercept communication traffic instead of fixing this global security problem.⁸ Secondly, after the vulnerability was discovered, the bigger internet companies fixed the problem quickly while internet companies with less security expertise lagged behind, leaving their clients vulnerable for a longer period of time.

It is important to realise that Heartbleed is only one example of a vulnerability used for monitoring of communication. At the end of 2013 the German newspaper *Der Spiegel* reported on the NSA’s Tailored Access Operations unit (TAO). *Der Spiegel* uncovered that TAO has multiple methods to intercept communications between people, which required them to install backdoors on, among others, internet exchange points (IXPs), internet service providers (ISPs), modems, computers and mobile phones. To increase the ability to intercept communication traffic the NSA chose to compromise the security of the entire internet and mobile infrastructure for intelligence purposes.^{9, 10} Both Heartbleed and Tailored Access Operations are examples of the government using infrastructural vulnerabilities for surveillance instead of fixing the problem, leaving us all more exposed to exploitation.

Censoring of content

States have different ways to censor content; technical blocking, search result removal, take-down

of content and induced self-censorship.¹¹ Technical blocking can target specific websites, domains or IP addresses, or use keyword blocking which automatically looks for specific words and blocks access to websites where these keywords are found. Government can also request the blocking of specific search results. Google’s transparency report states: “Governments ask companies to remove or review content for many different reasons. For example, some content removals are requested due to allegations of defamation, while others are due to allegations that the content violates local laws prohibiting hate speech or adult content.”¹² Take-down of content is used when states, companies and others can demand the removal of websites or content through the court.

However, in the last two years we have seen other ways in which non-state groups use the terms and conditions of social media platforms to take down content. Syria activists believe that the Syrian Cyber Army, a collection of computer hackers who support the government of Syrian President Bashar al-Assad,¹³ is using Facebook’s terms and conditions to take down content published by the Syrian opposition. Facebook’s community standards are guidelines to protect the community and do not allow content that can be described as graphic content, nudity, bullying and more.¹⁴ If a user believes that a post on Facebook violates these terms they can report it as abuse, which is called flagging. The Syrian Cyber Army is allegedly using this complaint procedure to flag content which shows human rights violations by the Syrian regime as inappropriate and graphic content, after which it can be taken down.¹⁵ This is particularly problematic since the Syrian opposition moved to social media after a crackdown on the traditional media – and the country’s citizens.

There are also cases where a state does not need to have legal jurisdiction over social media sites to request the take-down of content. In May 2014 Twitter censored tweets in Russia and Pakistan. In the case of Pakistan, Twitter caved in to pressure from the government to censor specific tweets that were deemed blasphemous or unethical. In Russia, Twitter took down the content of a Ukrainian

Twitter account which, according to Eva Galperin of the Electronic Frontier Foundation (EFF), is “plainly political... These actions are highly problematic as independent media in Ukraine is increasingly under attack.”¹⁶ In both countries, Twitter does not have formal representation and there is no legal jurisdiction over the service, yet still the service providers complied with government requests.

Profiling of people

Much of our behaviour is already leaving digital traces – even actions that seem as harmless as walking down the street. Traffic and surveillance cameras are monitoring us, our mobile phones are registering our whereabouts every moment of the day and we voluntarily post our private lives on public proprietary platforms. This might seem innocent at first, but there have been numerous instances where a mobile phone has been used to locate someone, and online behaviour and information are used for profiling.

During the protests in Ukraine in the beginning of 2014 a collective message was sent to mobile phone users near the scene of violent clashes in Kiev: “Dear subscriber, you are registered as a participant in a mass riot,” it said.¹⁷ In the end the protestors toppled the regime of ex-president Viktor Yanukovich, yet the records of who was near the square still remain. Mobile phone companies have the capabilities to track and collect the following information on you through your phone: phone calls, text messages, data services you use, and your approximate location, and may share that information with the government. A mobile is a goldmine of information: your phone book with all your contacts in it, call history, text messages, locations and previous locations, data from any application you are using, and photos and videos. In addition, governments and phone companies can see which phones are close to yours, which other “people” or phones are in the room.

Regimes have also used malignant viruses to profile political actors and their networks. The most well known cases are of the commercial malware

Hacking Team¹⁸ and FinFisher¹⁹ that were – and might still be – deployed in countries like Ethiopia, Bahrain, Mexico and Turkmenistan. Privacy International published one of FinFisher’s brochures, which states: “The product is known as FinFisher and is delivered onto computers, it then harvests information from the computer, from passwords and web browsing sessions, to Skype conversations. It can even switch on a computer’s webcam and microphone remotely.”²⁰

Challenges

In mitigating these different threats there are a number of challenges we have encountered, specifically when you approach censorship and communications surveillance from a human rights defenders or journalist perspective.

The majority of digital threats are invisible and abstract. While a virus on your computer or phone can grant someone access to your physical surroundings by turning on the camera or microphone, we do not see it and therefore the threat remains abstract. The second challenge is that secure communication is always a trade-off between security and convenience. Security measures are seen as cumbersome and a distraction from the priorities of the day. When in the trenches, short-term wins and threats are more pressing than the intangible nature of communications surveillance and long-term exposure – especially when installing and using certain tools can be more inconvenient and time consuming than using unsecure communication methods.

When a digital emergency happens, it is difficult to know where to turn, who to ask for help and how to solve the problem. Very few organisations have done work on the prevention of digital emergencies. If we live in an earthquake-affected area, we have flashlights, water and emergency plans ready; but even with all the knowledge of different digital threats and communication surveillance, similar contingency plans to mitigate digital threats are few and far between. If NGOs, human rights defenders or media organisations recognise

7 Zhu, Y. (2014, April 8). Why the web needs perfect forward secrecy more than ever. *Electronic Frontier Foundation*. <https://www.eff.org/deeplinks/2014/04/why-web-needs-perfect-forward-secrecy>

8 Riley, M. (2014). NSA said to have used Heartbleed bug for intelligence for years. *Bloomberg*. www.bloomberg.com/news/2014-04-11/nsa-said-to-have-used-heartbleed-bug-exposing-consumers.html

9 Appelbaum, J., Horchert, J., & Stocker, C. (2013, December 29). Shopping for Spy Gear: Catalog Advertises NSA Toolbox. *Der Spiegel*. www.spiegel.de/international/world/catalog-reveals-nsa-has-back-doors-for-numerous-devices-a-940994.html

10 Appelbaum, J. (2013). To Protect and Infect: The militarization of the internet. Presentation given at the 30C3, Hamburg, Germany, 29 December. <https://www.youtube.com/watch?v=vILAlhwUgIU>

11 <https://opennet.net/about-filtering>

12 Google. (2014). *Transparency report: Requests to remove content*. <https://www.google.com/transparencyreport/removals/government/>

13 https://en.wikipedia.org/wiki/Syrian_Electronic_Army

14 <https://www.facebook.com/communitystandards>

15 Pizzi, M. (2014, February 4). The Syrian Opposition is Disappearing From Facebook. *The Atlantic*. www.theatlantic.com/international/archive/2014/02/the-syrian-opposition-is-disappearing-from-facebook/283562

16 Galperin, E. (2014, May 21). Twitter steps down from the free speech party. *Electronic Frontier Foundation*. <https://www.eff.org/deeplinks/2014/05/twitter-steps-down-free-speech-party>

17 Walker, S., & Grytsenko, O. (2014, January 21). Text messages warn Ukraine protesters they are ‘participants in mass riot’; Mobile phone-users near scene of violent clashes in Kiev receive texts in apparent attempt by authorities to quell protests. *The Guardian*. www.theguardian.com/world/2014/jan/21/ukraine-unrest-text-messages-protesters-mass-riot

18 Marczak, B., Guarnieri, C., Marquis-Boire, M., & Scott-Railton, J. (2014). *Hacking Team and the Targeting of Ethiopian Journalists*. Toronto: The Citizen Lab. <https://citizenlab.org/2014/02/hacking-team-targeting-ethiopian-journalists>

19 Marquis-Boire, M., Marczak, B., Guarnieri, C. & Scott-Railton, J. (2013). *For Their Eyes Only: The Commercialization of Digital Spying*. Toronto: The Citizen Lab. <https://citizenlab.org/2013/04/for-their-eyes-only-2>

20 https://www.privacyinternational.org/sii/gamma_group

the problem and want to increase their security, they have few funds to spend on prevention or do not know where to start. There is a lack of technical knowledge and skills in the human rights and media community.

How can you mitigate the threats and where do you find support?

There are a number of ways to be more prepared for a digital emergency as an individual or organisation. Prevention is key: try to increase the overall digital security awareness and practices of your organisations,²¹ establish a relationship with a technical person you trust and can turn to for immediate advice, make a thorough threat analysis,

and establish some protocols and procedures in case you are targeted. If you think you are suffering a digital attack, turn to a trusted technical expert or international organisation or make a self-assessment.²²

Conclusion

The field of digital emergency support for human rights defenders, journalists and bloggers around the world is still emergent. The intangible nature and rapidly changing technical environment makes it difficult to mitigate digital threats. It is crucial to understand what the different threats are and work on prevention. If you are in the midst of a digital attack, turn to a trusted technical expert or international organisation for support.

Intermediary liability and state surveillance

Elonnai Hickok

Centre for Internet and Society (CIS) India
www.cis-india.org

Introduction

On 30 June 2014, The Right to Privacy in the Digital Age: Report of the Office of the United Nations High Commissioner for Human Rights (OHCHR) was published.¹ The Report recognises the relationship between service providers and surveillance and the increasing trend of privatised surveillance, noting:

There is strong evidence of a growing reliance by Governments on the private sector to conduct and facilitate digital surveillance. On every continent, Governments have used both formal legal mechanisms and covert methods to gain access to content, as well as to metadata. This process is increasingly formalized: as telecommunications service provision shifts from the public sector to the private sector, there has been a “delegation of law enforcement and quasi-judicial responsibilities to Internet intermediaries under the guise of ‘self-regulation’ or ‘cooperation’”.²

This report will explore how legal requirements, practices and policies pertaining to intermediary liability are feeding into this growing trend through the incorporation of requirements for intermediaries that facilitate surveillance. In doing so, this report will explore aspects of intermediary liability policies and practices, and how these pertain to and enable state surveillance. Lastly, the report will look at gaps that exist in policies pertaining to privacy, surveillance and intermediary liability.

Intermediaries and privacy

Online communications, interactions and transactions are an integral component of our everyday lives. As such, intermediaries – including, though not limited to, search engines, social networks,

cyber cafés, and internet and telecommunication service providers – play a critical role with respect to user privacy. As individuals utilise intermediary platforms on a daily and routine basis, from searching for information on the internet, to posting updates to a social media account, to using voice-over-internet-protocol (VoIP) services to connect with friends and colleagues, or using the services of a cyber café, intermediaries host, retain and have access to vast amounts of personal data of their users across the world, irrespective of jurisdiction. In this context, company practices and a country’s legal regulations have a far-reaching impact on the rights – specifically privacy and freedom of expression – of both national and foreign users.

Intermediaries, governments and surveillance

The Right to Privacy in the Digital Age also notes that the internet and associated technologies allow governments to conduct surveillance on an unprecedented scale. This was highlighted by the revelations by Edward Snowden, which demonstrated the scope of access that the United States (US) government had to the data held by internet companies headquartered in the US. The revelations also underscore the precarious position that companies offering these services and technologies are placed in. Though the scope and quantity of data collected and held by an intermediary vary depending on the type of intermediary, the services offered and the location of its infrastructure, governments have recognised the important role of intermediaries – particularly in their ability to assist with state surveillance efforts by providing efficient access to vast amounts of user data and identifying potentially harmful or threatening content. Within this, there is a shift from reactive government surveillance that is based on a request and authorised order, to partially privatised surveillance, with companies identifying and reporting potential threats, retaining information, and facilitating access to law enforcement. Indeed, the OHCHR in the Right to Privacy in the Digital Age notes that the surveillance revealed by Snowden was facilitated in part

²¹ Tactical Tech Collective and Front Line Defenders, Security in a Box <https://securityinabox.org/> and Electronic Frontier Foundation, Surveillance Self-Defense <https://ssd.eff.org/risk>

²² Digital First Aid Kit digitaldefenders.org/wordpress/launch-of-the-digital-first-aid-kit or on GitHub <https://github.com/RaReNet/DFAK>

¹ www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf

² Ibid.

by “strategic relationships between Governments, regulatory control of privacy companies, and commercial contracts.”³

Intermediary liability and state surveillance

As described by the US-based Center for Democracy and Technology,⁴ intermediary liability relates to the legal accountability and responsibility that is placed on intermediaries with respect to the content that is hosted and transmitted via their networks and platforms. Specifically, intermediary liability addresses the responsibility of companies with respect to content that is deemed by the government and/or private parties to be objectionable, unlawful or harmful. The Center for Democracy and Technology points out that, depending on the jurisdiction, intermediary liability requirements and provisions can be used to control illegal content online, but also can be misused to control legal content as well. As described by UK-based Article 19, provisions relating to intermediary liability can be broken down into three basic models: strict liability, where intermediaries are fully liable for third-party content; safe harbour, where intermediaries can be provided immunity from liability by meeting defined requirements; and broad immunity, where intermediaries are given immunity for third party content.⁵ As pointed out by Frank La Rue in the Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, legal frameworks that hold intermediaries (rather than the individual) liable for content, transfer the role of monitoring the internet to the intermediary.⁶ Some jurisdictions do not have specific legal provisions addressing intermediary liability, but do issue court or executive orders to intermediaries for the restriction of content, as well as placing obligations – including technical obligations – on service providers via operating licences.

Legal provisions and orders pertaining to intermediary liability are not always limited to removing or disabling pre-defined or specified content. Requests for the removal of content can be accompanied with requests for user information – including IP address and basic subscriber information. Some jurisdictions, such as India, have

incorporated retention mandates for removed content and associated information in legal provisions addressing intermediary liability.⁷ Other jurisdictions, like China, require service providers to have tracking software installed on their networks, collect and retain user identification details, monitor and store user activity, report illegal activity to law enforcement, and have in place filtering software to restrict access to banned websites.⁸

Some jurisdictions are also recognising that the traditional means of seeking information from intermediaries are inefficient and often slow – particularly if the intermediary is foreign, and accessing information requires the government to follow a Mutual Legal Assistance Treaty (MLAT) process.⁹ Perhaps in response to challenges posed by jurisdiction, some governments have sought “collaborations” with intermediaries to restrict illegal and offensive speech as well as identify perpetrators of the same. For example, in 2007 in India, the Mumbai Police negotiated with Google to establish a “direct line of contact”¹⁰ with the company, which, according to news items, would allow access to IP addresses of users posting “objectionable” content on Google’s social networking site, Orkut.¹¹ Such collaborations combine elements of intermediary liability and surveillance, and can be prone to misuse if they lack apparent oversight, legislative grounding or accountability. In this context, intermediary liability is not only about content online, but also encompasses the collection and disclosure of data associated with that content and of users producing and viewing such content.

7 The Information Technology (Intermediaries Guidelines) Rules, 2011, Rule 3(4). [deity.gov.in/sites/upload_files/dit/files/GSR314E_10511\(1\).pdf](http://deity.gov.in/sites/upload_files/dit/files/GSR314E_10511(1).pdf)

8 Frydnamm, B., Hennebel, L., & Lewkowicz, G. (2007). *Public Strategies for Internet Co-Regulation in the United States, Europe, and China*. Brussels: Université Libre de Bruxelles. www.philodroit.be/IMG/pdf/BF-LH-GL-WP2007-6.pdf

9 Mutual Legal Assistance Treaties are formal agreements reached between governments to facilitate cooperation in solving and responding to crimes. A critique of the MLAT process has been that it is slow and inefficient, making it a sub-optimal choice for governments when faced with crimes that demand immediate response. For more information see: Kindle, B. (2012, February 14). MLATS are powerful weapons in financial crime combat, even for private sector. *Association of Certified Financial Crime Specialists*. www.acfcs.org/mlats-are-powerful-weapons-in-counter-financial-crime-combat-even-for-private-sector Some intermediaries, such as Facebook, have specified that foreign governments seeking user account data must do so through the MLAT process or letters of rogatory. For more information see: <https://en-gb.facebook.com/safety/groups/law/guidelines>

10 Pahwa, N. (2007, March 14). Updated: Orkut to Share Offender Data With Mumbai Police; Google’s Clarification. *Gigaom*. gigaom.com/2007/03/14/419-updated-orkut-to-share-offender-data-with-mumbai-police-googles-clarifi

11 Chowdhury, S. (2014, July 30). Mumbai Police tie up with Orkut to nail offenders. *The Indian Express*. archive.indianexpress.com/news/mumbai-police-tie-up-with-orkut-to-nail-offenders/25427

Types of content and surveillance measures

Certain types of content – namely child pornography/adult content, national/cyber security and copyright – can attract greater obligations on the intermediary to proactively facilitate surveillance and in some cases take on the role of law enforcement or the judiciary. The degree to which such obligations are backed by legal provisions varies and can range from statutory requirements, to policy initiatives, to forms of collaboration between governments, intermediaries, and self-regulatory organisation. The types of obligations and measures also vary.

Reporting of illegal content: Some of these measures are focused on the reporting of illegal or prohibited content. For example, in the US, by law, service providers must report to law enforcement any and all information with regards to child pornography. This is mandated by the Protection of Children from Sexual Predators Act, 1998.¹² Similarly, in India, under the rules defining procedural safeguards for intermediary liability, intermediaries must report cyber security incidents and share related information with the Indian Computer Emergency Response Team.¹³

Voluntary disclosure of illegal content and activity: Other measures support the voluntary disclosure of identified illegal content and activity and associated information to law enforcement. For example, under the 2002 Cyber Security Enhancement Act in the US, law enforcement can encourage service providers to reveal information pertaining to an “emergency matter”. The Act further provides the service provider immunity from legal action if the disclosure was made in good faith with the belief that it was a matter of death or serious physical injury.¹⁴

Databases of repeat offenders: Requirements that governments are seeking to impose on service providers may also directly conflict with their obligations under national data protection standards. For example, in the context of proposed legal requirements for identifying and preventing copyright offenders under the UK Digital Economy Act, in a public statement, the service provider Talk-Talk noted that the company would be required to maintain a database of repeat offenders – an action that might be illegal under the UK Data Protection Act.¹⁵ As of July 2014, service providers, rights hold-

ers and the government have developed a form of collaboration where rights holders will “track” the IP addresses of suspected offenders. The addresses will be shared with the applicable UK service provider, who will then send a series of warning notices to the user.¹⁶ This system is potentially dangerous as it allows for proactive monitoring of individuals’ IP addresses by private parties (the rights holders) and then subsequent action by another private entity (the service provider). At no point does this system define or envision safeguards, accountability or oversight mechanisms.¹⁷

Measures that facilitate surveillance: Other requirements do not directly impose surveillance obligations on service providers, but can facilitate surveillance. For example, in the UK, service providers must now offer broadband filters for “adult content” automatically switched on. Users who do not wish to have the filter on are required to “opt out” of the filter.¹⁸ These measures can make it easy to track and identify which user is potentially viewing “adult content”.

Types of intermediaries and surveillance measures

Depending on services offered and jurisdiction, intermediaries can be subject to differing types and scopes of surveillance requirements. For example:

Cyber cafés: In jurisdictions like India,¹⁹ cyber cafés are faced with legal requirements that can facilitate surveillance – such as the collection and retention of government-issued user identification, retention of user’s browser history, and provision of assistance to law enforcement and other authorities when required. Cyber cafés are also strictly subject to the laws of the jurisdiction of operation.

Service providers: Similarly, service providers, even when multinational, must abide by the laws where they are operating. Unlike intermediaries such as multinational social networks or search engines, service providers are subject to the requirements found in operating licences that pertain to intermediary liability and surveillance. For example, in India, internet and telecommunication service providers are required to take “necessary measures to prevent objectionable, obscene, unauthorised,

3 Ibid.

4 <https://cdt.org>

5 Article 19. (2013). *Internet Intermediaries: Dilemma of liability*. London: Article 19. www.article19.org/data/files/intermediaries_ENGLISH.pdf

6 Frank La Rue, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, United Nations General Assembly, 17 April 2013. www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf

16 Ibid.

17 Jackson, M. (2013, August 9). UK Government to Finally Repeal ISP Website Blocking Powers. *ISPreview*. www.ispreview.co.uk/index.php/2013/08/uk-government-to-finally-repeal-isp-website-blocking-powers.html

18 Miller, J. (2014, July 23). New broadband users shun UK porn filters, Ofcom finds. *BBC*. www.bbc.com/news/technology-28440067

19 Information Technology (Guidelines for Cyber Cafe) Rules 2011, Rule 4, Rule 5, Rule 7. ddpolic.gov.in/downloads/miscellaneous/cyber-cafe-rules.pdf

or any other content, messages, or communications infringing copyright, intellectual property etc. in any form, from being carried on [their] network, consistent with the established laws of the country.” Furthermore, if specific instances of infringement are reported by enforcement agencies, the service provider must disable the content immediately.²⁰ In the case of India, requirements for the provision of technical assistance in surveillance and retention of call detail records²¹ and subscriber information are also included in the operating licences for service providers.²²

Social networks: Social networks such as LinkedIn, Facebook and Twitter – which are often multinational companies – are not necessarily subject to the legal intermediary liability requirements of multiple jurisdictions, but they are frequently faced with requests and orders for user information and removal of content requests. To address these pressures, some companies filter content on a country basis. In June 2014 LinkedIn was criticised in the media for complying with orders from the Chinese government and filtering content in the region.²³ Similarly, Twitter was criticised by civil society for withholding content in Russia and Pakistan in May 2014, though in June 2014 the company reversed its decision and reinstated the withheld content.²⁴ Social media platforms are also frequently and increasingly used by law enforcement and the state for collecting “open source intelligence”.²⁵

Technology, intermediary liability and state surveillance

When intermediaries implement legal requirements for the blocking or filtering of content, they do so by employing different techniques and technologies such as key word filtering software, firewalls, image scanning, URL databases, technologies that enable deep packet inspection, etc.²⁶ Similarly, complying with legal mandates for interception or monitoring of communications also requires intermediaries to install and use technology on their networks. As pointed out by La Rue, technologies used for filtering also facilitate monitoring and surveillance as they have the ability to identify and track words, images, websites and types of content, as well as identify individuals using, producing or associated with the same.²⁷ For example, YouTube offers copyright holders the option of YouTube’s “Content ID” system to manage and identify their content on the platform. Actions that copyright owners can choose from include muting audio that matches the music of copyrighted material, blocking a video from being viewed, running ads against a video, and tracking the viewer statistics of the video. These options can be implemented at a country-specific level.²⁸

Removing the service provider from surveillance

While some governments are placing obligations on intermediaries to assist with surveillance, other governments are removing such obligations from service providers through surveillance measures that seek to bypass service providers and allow governments and security agencies to directly intercept and access information on communication networks, or measures that require service providers to allow security agencies a direct line into their networks. For example, India is in the process of implementing the Central Monitoring System, which is envisioned to allow security agencies to directly intercept communications without the assistance of service providers. Though this system removes obligations on service providers to assist and be involved in specific instances of surveillance, it also removes a potential safeguard – where

service providers can challenge or question extra-legal or informal requests for surveillance. In the 2014 Vodafone Law Enforcement Disclosure Report, the company notes that in select countries, law enforcement and authorities have direct access to communications stored on networks.²⁹

The question of jurisdiction

Jurisdiction and the applicability of local law is a tension that arises in the context of intermediary liability and surveillance. Some facets of this tension include: to what extent do legal restrictions on content apply to multinational platforms operating in a country? To what extent can states access the communications passing or being stored in its territory? And to what extent do domestic protections of fundamental rights – including freedom of expression and privacy – apply to foreigners as well as nationals? The OHCHR in *The Right to Privacy in the Digital Age* shed some light on these questions, drawing upon a number of international instruments and firmly asserting that any interference with the right to privacy must comply with the principles of legality, proportionality and necessity, regardless of the nationality or location of the individual.³⁰ Tensions around mass surveillance of foreign citizens and political leaders, and a lack of legal constructs domestically and internationally to address these tensions, have led to questions of direction and the future of internet governance – discussed at forums like NETmundial, where principles relating to surveillance and intermediary liability were raised.³¹ Similarly, in March 2014, the US announced plans to relinquish the responsibility of overseeing the body tasked with regulating internet codes and numbering systems. This move has raised concerns about a backlash that could result in the division and separation of the internet, facilitating mass surveillance and content control.³²

State surveillance and intermediary liability: The impact on the user and the role of the company

Government-initiated content restrictions and surveillance of individuals’ online communications, transactions and interactions have widely been recognised as having a negative impact on users’ right to privacy and a chilling effect on freedom of speech. Depending on the target and reasons, such actions by governments can have deeper human rights implications – if, for example, dissenting voices, activists and journalists are targeted. The gravity and clear human rights implications of actions related to intermediary liability and surveillance highlight the complexity of these issues. Numerous cases exist of individuals being identified and persecuted for speech shared or communicated online, and the identification of these individuals being facilitated by internet companies. For example, Yahoo! has been heavily criticised in the international media for providing the Chinese government in 2006 with user account details and the content of communications of political dissident and journalist Shi Tao – allowing police to identify and locate Shi and subsequently imprison him for ten years.³³ Instances such as the Shi Tao case demonstrate the complexity of issues related to intermediary liability and surveillance and raise questions about reasonable expectations regarding internet company practices and responses (particularly multinational companies), adequate national legislation, international guidelines, and appropriate public response. As noted in *The Right to Privacy in the Digital Age*, “the Guiding Principles on Business and Human Rights, endorsed by the Human Rights Council in 2011, provide a global standard for preventing and addressing adverse effects on human rights linked to business activity. The responsibility to respect human rights applies throughout a company’s global operations regardless of where its users are located, and exists independently of whether the State meets its own human rights obligations.” This is a high standard that intermediaries must adhere to. Some companies such as Google,³⁴ Facebook,³⁵

20 Licence Agreement for Provision of Unified Access Services After Migration from CMTS, Section 40.3. www.auspi.in/policies/UASL.pdf

21 Call record details consist of information about a subscriber’s use of mobile and broadband networks and can include: called numbers, subscriber name and address, date and time of the start and end of a communication, type of service used (SMS, etc.), international mobile subscriber identity, international mobile equipment identity, location details. For more information see: Afentis Forensics, “Telephone Evidence: Mobile telephone forensic examinations, Billing Records, Cell Site Analysis”. afentis.com/telephone-evidence

22 Licence Agreement for Provision of Unified Access Services After Migration from CMTS, Section 41.10. www.auspi.in/policies/UASL.pdf

23 Mozur, P. (2014, June 4). LinkedIn Said it Would Censor in China. Now That It Is, Some Users are Unhappy. *The Wall Street Journal*. blogs.wsj.com/chinarealtime/2014/06/04/linkedin-said-it-would-censor-in-china-now-it-is-and-some-users-are-unhappy

24 Galperin, E., & York, J. (2014, June 23). Twitter Reverses Decision to Censor Content in Pakistan. *Electronic Frontier Foundation*. <https://www.eff.org/deeplinks/2014/06/twitter-reverses-decision-censor-content-pakistan>

25 Open source intelligence has been widely recognised as an essential tool for law enforcement and security agencies. Open source intelligence is derived from information that is publicly available from sources such as the internet, traditional media, journals, photos, and geospatial information. For more information see: Central Intelligence Agency. (2010, July 23). *INTelligence: Open Source Intelligence*. *Central Intelligence Agency*. <https://www.cia.gov/news-information/featured-story-archive/2010-featured-story-archive/open-source-intelligence.html>

26 Bloxx. (n/d). *Whitepaper: Understanding Web Filtering Technologies*. www.bloxx.com/downloads/US/bloxx_whitepaper_webfilter_us.pdf

27 Frank La Rue, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, United Nations General Assembly, 17 April 2013. www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf

28 YouTube, “How Content ID Works”. <https://support.google.com/youtube/answer/2797370?hl=en>

29 www.vodafone.com/content/sustainabilityreport/2014/index/operating_responsibly/privacy_and_security/law_enforcement.html

30 Report of the Office of the United Nations High Commissioner for Human Rights: *The Right to Privacy in the Digital Age*, 30 June 2014. www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf

31 Powles, J. (2014, April 28). Big Business was the winner at NETmundial. [wired.co.uk](http://www.wired.co.uk/news/archive/2014-04/28/internet-diplomacy-netmundial). www.wired.co.uk/news/archive/2014-04/28/internet-diplomacy-netmundial

32 Kelion, L. (2014, April 23). Future of the Internet Debated at NetMundial in Brazil. *BBC*. www.bbc.com/news/technology-27108869

33 MacKinnon, R. (2007). *Shi Tao, Yahoo!, and the lessons for corporate social responsibility*. rconversation.blogs.com/YahooShiTaoLessons.pdf

34 Google Transparency Report. www.google.com/transparencyreport

35 Facebook Global Government Requests Report. https://www.facebook.com/about/government_requests

Twitter,³⁶ Vodafone,³⁷ Microsoft,³⁸ Yahoo³⁹ and Verizon⁴⁰ have begun to shed light on the amount of surveillance and content requests that they are subject to through transparency reports. Companies like Vodafone,⁴¹ Facebook⁴² and Twitter⁴³ also have policies in place for addressing requests from law enforcement.

Conclusions

As demonstrated above, there is significant overlap between intermediary liability, privacy and surveillance. Yet jurisdictions have addressed these issues separately – often having independent legislation for data protection/privacy, intermediary liability and surveillance. The result is that the present legal frameworks for intermediary liability, privacy and surveillance are governed by models that do not necessarily “speak to each other”. When

requirements that facilitate surveillance are embedded in provisions and practices pertaining to intermediary liability, there is a risk that these requirements can omit key safeguards to surveillance that have been recognised as critical at the international level, including necessity, proportionality, legality and legitimate aim. As La Rue stressed, and as emphasised in other international reports and forums, there is a need for governments to review, update and strengthen laws and legal standards addressing state surveillance. Ideally such a review would also include legal standards for intermediary liability.

Where multi-stakeholder⁴⁴ and multilateral⁴⁵ dialogues are resulting in incremental and slow progress, some decisions by the Court of Justice of the European Union and European Parliament are calling attention and efforts to the issue.⁴⁶

Unmasking the Five Eyes’ global surveillance practices¹

Carly Nyst and Anna Crowe
Privacy International
carly@privacy.org, annac@privacyinternational.org

The revelations of the last year – made possible by NSA-whistleblower Edward Snowden – on the reach and scope of global surveillance practices have prompted a fundamental re-examination of the role of intelligence services in conducting coordinated cross-border surveillance. The Five Eyes alliance – comprised of the United States National Security Agency (NSA), the United Kingdom’s Government Communications Headquarters (GCHQ), Canada’s Communications Security Establishment Canada (CSEC), the Australian Signals Directorate (ASD), and New Zealand’s Government Communications Security Bureau (GCSB) – is the continuation of an intelligence partnership formed in the aftermath of the Second World War. The patchwork of secret spying programmes and intelligence-sharing agreements implemented by parties to the Five Eyes arrangement constitutes an integrated global surveillance arrangement that now covers the majority of the world’s communications. Operating in the shadows and misleading the public, the Five Eyes agencies boast in secret how they “have adapted in innovative and creative ways that have led some to describe the current day as ‘the golden age of SIGINT [signals intelligence]’.”²

This report summarises the state of understanding about the Five Eyes global domination of communications networks, and explains the most concerning surveillance capabilities developed by the intelligence agencies. It also explores the implications of expanded surveillance powers for the rights to privacy and free expression, and the free flow of information and ideas throughout global communications networks. Finally, it canvasses some of the ways that Privacy International is seek-

ing to unpick the Five Eyes alliance and argues for the restoration of privacy and security in digital communications.

The Five Eyes

Beginning in 1946, an alliance of five countries (the US, the UK, Australia, Canada and New Zealand) developed a series of bilateral agreements over more than a decade that became known as the UKUSA (pronounced yew-kew-zah) agreement. This established the “Five Eyes” alliance for the purpose of sharing intelligence, but primarily signals intelligence (hereafter “SIGINT”). The close relationship between the five states is evidenced by documents recently released by Snowden. Almost all of the documents include the classification “TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL” or “TOP SECRET//COMINT//REL TO USA, FVEY”. These classification markings indicate the material is top-secret communications intelligence (aka SIGINT) material that can be released to the US, Australia, Canada, UK and New Zealand. Notably while other alliances and coalitions exist, such as the North Atlantic Treaty Organization, none of the documents that have thus far been made public refer to any of these arrangements, suggesting the Five Eyes alliance is the preeminent SIGINT collection alliance.

The Five Eyes agencies are playing a dirty game. They have found ways to infiltrate all aspects of modern communications networks: forcing companies to hand over their customers’ data under secret orders, and secretly tapping fibre optic cables between the same companies’ data centres anyway; accessing sensitive financial data through SWIFT, the world’s financial messaging system; spending years negotiating an international agreement to regulate access to the data through a democratic and accountable process, and then hacking the networks to get direct access; threatening politicians with trumped-up threats of impending cyber war while conducting intrusion operations that weaken the security of networks globally; and sabotaging encryption standards and standards bodies, thereby undermining the ability of internet users to secure information.

36 Twitter Transparency Report. <https://transparency.twitter.com>
37 Vodafone Disclosure to Law Enforcement Report. www.vodafone.com/content/sustainabilityreport/2014/index/operating_responsibly/privacy_and_security/law_enforcement.html
38 Microsoft’s Law Enforcement Request Report. www.microsoft.com/about/corporatecitizenship/en-us/reporting/transparency
39 Yahoo Transparency Report. <https://transparency.yahoo.com>
40 Verizon’s Transparency Report for the first half of 2014. transparency.verizon.com
41 Vodafone, Human Rights and Law Enforcement: An Overview of Vodafone’s policy on privacy, human rights, and law enforcement assistance. www.vodafone.com/content/index/about/about-us/privacy/human_rights.html
42 Facebook, Information for Law Enforcement. <https://www.facebook.com/safety/groups/law/guidelines/>
43 Twitter Guidelines for Law Enforcement. <https://support.twitter.com/articles/41949-guidelines-for-law-enforcement>

44 Powles, J. (2014, April 28). Op. cit.
45 RT. (2013, October 26). Germany, Brazil enlist 19 more countries for anti-NSA UN resolution. RT. rt.com/news/nsa-un-resolution-talks-788
46 Powles, J. (2014, April 28). Op. cit.

1 This paper is based substantially on “Eyes Wide Open”, a report published by Privacy International in November 2013, available at: <https://www.privacyinternational.org/reports/eyes-wide-open>
2 NSA SIGINT Strategy, 23 February 2012, available at: www.nytimes.com/interactive/2013/11/23/us/politics/23nsa-sigint-strategy-document.html?ref=politics&gwh=5E154810A5FB56B3E9AF98DF667AE3C8

The Five Eyes is a close-knit group. The level of cooperation under the UKUSA agreement is so complete that “the national product is often indistinguishable.”³ This has resulted in former intelligence officials explaining that the close-knit cooperation that exists under the UKUSA agreement means “that SIGINT customers in both capitals seldom know which country generated either the access or the product itself.”⁴ In addition to fluidly sharing collected SIGINT, it is understood that many intelligence facilities run by the respective Five Eyes countries are jointly operated, even jointly staffed, by members of the intelligence agencies of Five Eyes countries. Each facility collects SIGINT, which can then be shared with the other Five Eyes states.

Code-named programmes that have been revealed to the public over the last decade go some way to illustrating how the Five Eyes alliance collaborates on specific programmes of activity and how information is shared. One important example is the TEMPORA programme, revealed by Snowden. By placing taps at key undersea fibre-optic cable landing stations, the programme is able to intercept a significant portion of the communications that traverse the UK. The *Guardian* has reported that 300 analysts from GCHQ and 250 from the NSA were directly assigned to examine material collected.⁵ TEMPORA stores content for three days and metadata for 30 days.

Once content and data are collected, they can be filtered. The precise nature of GCHQ’s filters remains secret. Filters could be applied based on type of traffic (e.g. Skype, Facebook, email), origin/destination of traffic, or to conduct basic keyword searches, among many other purposes. Reportedly, approximately 40,000 search terms have been chosen and applied by GCHQ, and another 31,000 by the NSA to information collected via TEMPORA. GCHQ have had staff examining collected material since the project’s inception in 2008, with NSA analysts brought to trial runs of the technology in summer 2011. Full access was provided to NSA by autumn 2011. An additional 850,000 NSA employees and US private contractors with top-secret clearance

reportedly also have access to GCHQ databases. GCHQ received £100 million (USD 160 million) in secret NSA funding over the last three years to assist in the running of this project.⁶

A core programme that provides filtering capability is known as XKEYSCORE. It has been described by internal NSA presentations as an “analytic framework” which enables a single search to query a “3-day rolling buffer” of “all unfiltered data” stored at 150 global sites on 700 database servers.⁷ The NSA XKEYSCORE system has sites that appear in Five Eyes countries.⁸ The system indexes email addresses, file names, IP addresses and port numbers, cookies, webmail and chat usernames and buddylists, phone numbers, and metadata from web browsing sessions including searches queried, among many other types of data that flow through their collection points.

While UKUSA is often reported as having created a “no spy pact” between Five Eyes states, there is little in the original declassified documents from the 1940s and 1950s to support such a notion. Crucially, first and foremost, no clause exists that attempts in any form to create such an obligation. As best as can be ascertained, it seems there is no prohibition on intelligence gathering by Five Eyes states with respect to the citizens or residents of other Five Eyes states. There is instead, it seems, a general understanding that citizens will not be directly targeted, and where communications are incidentally intercepted, there will be an effort to minimise the use and analysis thereof by the intercepting state. Outside the Five Eyes, everyone else is fair game, even if they have a separate intelligence-sharing agreement with one or several Five Eyes members.⁹

The rights implications

The world has changed dramatically since the 1940s; then, private documents were stored in filing cabinets under lock and key, and months could pass without one having the need or luxury of making an international phone call. Now, private documents are stored in unknown data centres around the

world, international communications are conducted daily, and our lives are lived – ideas exchanged, financial transactions conducted, intimate moments shared – online.

With the advent of the internet and new digital forms of communication, now most digital communications take the fastest and cheapest route to their destination, rather than the most direct. This infrastructure means that the sender has no ability to choose, nor immediate knowledge of, the route that their communication will take. This shift in communications infrastructure means that communications travel through many more countries, are stored in a variety of countries (particularly through the growing popularity of cloud computing) and are thus vulnerable to interception by multiple intelligence agencies. From their bases within the territory of each country, each Five Eyes intelligence agency collects and analyses communications that traverse their territory and beyond.

An analysis of the legal provisions in each of the Five Eyes countries reveals that they fall far short of describing the fluid and integrated intelligence-sharing activities that take place under the ambit of the Five Eyes arrangement with sufficient clarity and detail to ensure that individuals can foresee their application.¹⁰ None of the domestic legal regimes set out the circumstances in which intelligence authorities can obtain, store and transfer nationals’ or residents’ private communication and other information that are intercepted by another Five Eyes agency, nor the circumstances in which any of the Five Eyes states can request the interception of communications by another party to the alliance. The same applies to obtaining private information such as emails, web histories, etc., held by internet and other telecommunication companies. Carefully constructed legal frameworks provide differing levels of protections for internal versus external communications, or those relating to nationals versus non-nationals.

The Five Eyes agencies are seeking not only to defeat the spirit and purpose of international human rights instruments, they are in direct violation of their obligations under such instruments. The right to privacy is an internationally recognised right.¹¹ The way the global communications infrastructure is built requires that the right to privacy of commu-

nications be exercised globally, as communications can be monitored in a place far from the location of the individual to whom they belong. When an individual sends a letter, email or text message, or makes a phone call, that communication leaves their physical proximity, and travels to its destination. In the course of its transmission the communication may pass through multiple other states and, therefore, multiple jurisdictions. The right to privacy of the communication remains intact, subject only to the permissible limitations set out under human rights law. Accordingly, whenever Five Eyes countries interfere with the communication of an individual, thus infringing upon their privacy, they invoke jurisdiction over that individual, and have to comply with human rights obligations accordingly.

The practice of mass surveillance detailed in the Snowden documents is contrary to international law. The Special Rapporteur on the promotion and protection of the right to freedom of expression and opinion, for example, has described the invasiveness of mass interception of fibre-optic cables: “By placing taps on the fibre optic cables, through which the majority of digital communication information flows, and applying word, voice and speech recognition, States can achieve almost complete control of tele- and online communications.”¹²

The Special Rapporteur reasons that “[m]ass interception technology eradicates any considerations of proportionality, enabling indiscriminate surveillance. It enables the State to copy and monitor every single act of communication in a particular country or area, without gaining authorization for each individual case of interception.”¹³

Taking action

The intelligence agencies of the Five Eyes countries conduct some of the most important, complex and far-reaching activities of any state agency, and they do so behind the justification of a thicket of convoluted and obfuscated legal and regulatory frameworks. The laws and agreements that make up the Five Eyes arrangement and apply it to domestic contexts lack any semblance of the clarity or accessibility necessary to ensure that the individuals whose rights and interests are affected by them are able to understand their application. Their actions have been justified in secret, on the basis of secret interpretations of international law and classified

3 Aldrich, R. (2004). Transatlantic intelligence and security cooperation. *International Affairs*, 80(4), 731-753. www2.warwick.ac.uk/fac/soc/pais/people/aldrich/publications/inta80_4_08_aldrich.pdf

4 Lander, S. (2007). International intelligence cooperation: An inside perspective. *Cambridge Review of International Affairs*, 17(3), p. 487.

5 The Guardian quotes an internal GCHQ report that claims “GCHQ and NSA avoid processing the same data twice and proactively seek to converge technical solutions and processing architectures.” It was additionally reported that the NSA provided GCHQ with the technology necessary to sift through the material collected.

6 MacAskill, E. (2013, November 2). Portrait of the NSA: no detail too small in quest for total surveillance. *The Guardian*. www.theguardian.com/world/2013/nov/02/nsa-portrait-total-surveillance

7 The Guardian (2013, July 31). XKeyscore presentation from 2008. www.theguardian.com/world/interactive/2013/jul/31/nsa-xkeyscore-program-full-presentation

8 Ibid., p. 5.

9 Poitras, L. et al. (2013, July 1). How the NSA targets German and Europe. *Spiegel Online*. www.spiegel.de/international/world/secret-documents-nsa-targeted-germany-and-eu-buildings-a-908609.html

10 Privacy International. (2013). *Eyes Wide Open*. <https://www.privacyinternational.org/reports/eyes-wide-open>

11 Article 17 (1) of the International Covenant on Civil and Political Rights provides: “No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.”

12 Report of the Special Rapporteur on the promotion and protection of the right to freedom of expression and opinion, Frank La Rue, 17 April 2013, A/HRC/23/40, para. 38. www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf

13 Ibid., para. 62.

agreements. By remaining in the shadows, our intelligence agencies – and the governments who control them – have removed our ability to challenge their actions and their impact upon our human rights. We cannot hold our governments accountable when their actions are obfuscated through secret deals and covert legal frameworks. Secret, convoluted or obfuscated law can never be considered law within a democratic society governed by the rule of law.

We must move towards an understanding of global surveillance practices as fundamentally opposed to the rule of law and to the well-established international human right to privacy. In doing so, we must break down legal frameworks that obscure the activities of the intelligence agencies or that preference the citizens or residents of Five Eyes countries over the global internet population. Trust must be restored, and our intelligence agencies must be brought under the rule of law. Transparency around and accountability for secret agreements is a crucial first step.

Privacy International has spent the last year trying to unpick the Five Eyes alliance. We have sent

freedom of information requests to intelligence agencies in each of the five countries, seeking access to the secret agreements that govern the Five Eyes. We have brought legal cases against Britain's GCHQ for mass surveillance and hacking activities, and have sought avenues to take similar complaints in other jurisdictions. We filed a complaint under the OECD Guidelines for Multinational Enterprises against the seven telecommunications companies facilitating UK interception of fibre-optic cables. We have written to the Australian Inspector-General of Intelligence and Security asking her to commence an investigation into the ASD, and to the US Treasury Department and to every data protection authority in Europe seeking an investigation into the SWIFT hacking.

Now we are calling for the UN to appoint a Special Rapporteur on the right to privacy, to ensure that privacy and surveillance issues stay high on the agenda in the Human Rights Council. Support our work here: www.privacyinternational.org.

Country reports

Slaying the monster

The country reports gathered here have been written at a critical time: new threats of terrorism in countries such as Kenya, the intensification of regional conflicts and wars, the economic isolation of Russia, and a drift towards authoritarianism in many states. Alarming parallels in Japan are made between the rise of totalitarianism ahead of World War II and what is happening now in that country; and there is a sense many have that regional conflicts might spin even more out of control.

At the centre of this is the need for governments to control their futures, and to maintain power over situations that threaten to become ungovernable. One way they do this is through surveillance. This makes these country reports – and the thematic reports that you have just read – highly political. They come in the wake of WikiLeaks revelations, and Edward Snowden’s public exposure of United States (US) spying and the so-called “Five Eyes network”, linking some of the most powerful countries in a global surveillance programme. They reinforce the idea that human rights are under threat globally.

Common to most of the country reports published here is that states – frequently with the cooperation of business – are acting illegally: their actions are neither in line with national constitutional requirements, nor with a progressive interpretation of global human rights standards. While many profess to be standard bearers of democracy, they are in fact acting illegitimately – they no longer carry the mantle of public good or operate in the best interests of their citizens that have voted them into power. For instance, in South Korea, “Communications surveillance, in particular, which has insufficient legal control given the rapid development of the internet and mobile technologies, has largely extended the power of the police and the intelligence agency beyond the law.”

Despite the media attention that Snowden’s revelations received, the public at large remains numb to the problems of surveillance, through ignorance, or, in some instances, complicity. In Turkey, “If you do nothing wrong, if you have no illegal business, don’t be afraid of wiretapping,” a government minister said there.

This attitude of “only bad people should worry” completely misses the point of mass surveillance: it is ubiquitous, widespread, and involves everyone, whether or not you are a “threat to the state”, or engaged in criminal activities. This includes legislation allowing authorities to bug an entire room, and capture the conversations of innocent bystanders, or to monitor the public en masse if there is a potential that a suspect happens to be amongst that public.

Moreover, as numerous reports point out, defining who is or is not a “threat to the state” is obviously a slippery concept, and depends on the regime in power, democratically elected or not. Today’s friend is tomorrow’s enemy. In Pakistan, in the words of the chairperson of Aware Girls:

I was shocked when I was told that I and my social media communications had been under surveillance for last three years... In my communication with the agencies it was clear that my work for peace and human rights was seen as “anti-state”, and I was seen as an enemy rather than an activist.

And for those who imagine a benign government only interested in their welfare, Syria shows how, during a national strike, even the children and families of striking union members were surveilled:

Firstly, the police acquired all the mobile communication records of union members and their families, including schoolchildren, and tracked the real-time location of their mobile phones – the mobile service providers had offered to provide this at ten-minute intervals for several months.

In fact surveillance can put the security of the average citizen constantly under threat – and can often have even more dire implications for the vulnerable. Without public awareness of this, and transparency in surveillance programmes, a real erosion of human rights occurs.

Sometimes surveillance legislation is rushed through without proper parliamentary discussion, process or media attention. Legislation shifts and

changes, frequently to suit the new needs of the surveillance regime, and only sometimes are there victories for privacy rights, and for transparency – perhaps the most notable being the European Union (EU) cancelling its data retention directive, with a mixed knock-down effect on national legislation amongst EU members.

Argentina shows that even if governments are open about their new programmes to capture and centralise data – in this case biometric data – and emphasise the positive aspects of these programmes, the potential for this to be used in the future in ways that violate the rights of ordinary citizens is extraordinary. Without citizen-driven legislation, and public oversight, democracies are under threat (the story of Frankenstein's monster comes to mind here).

Syria points out that less-democratic states have little impetus to not surveil their citizens. If so-called democracies like the US and the United Kingdom with all their rights and privileges and sturdy legal systems can get away with it, how can we expect struggling democracies not to do the same? Those in totalitarian regimes, the country report argues, suffer a kind of double surveillance, and are subject to the spying by world powers and their own governments: “It is not unrealistic to imagine this to turn into a global overlapping ‘spaghetti’ of surveillance programmes where everyone is spying on everyone else.”

The complicity of business in all of this needs to be directly addressed by civil society. While some service providers seem to be making attempts at transparency by releasing statistics of government requests for information, many – or most – are not. Ostensibly, they feel no obligation to, with human rights not a primary concern. For instance, MTN's involvement in Cameroon requires attention. Beyond service providers and intermediaries – who appear to prefer “business as usual” rather than to rock the boat – the technology companies that make surveillance tools in the first place are a big part of the problem. Obscenely, in Nigeria, there is the allegation that the systems employed there were “tested” on Palestinians.

Marketing data – tracked and acquired without permission from the public – is also a form of surveillance, and one that now involves our children. That this is often done with a smile and a wink by companies who, if they wish, can on-sell data about our daily habits and behaviours as cheaply as mobile phone numbers to whomever – including states, and other business – shows how far business has slipped from anything resembling an interest in

consumer rights. Stronger advocacy is needed in this regard, both from consumer rights and human rights groups.

As Senegal points out, it is not only states that do the surveillance. There are numerous cases of companies illegally spying on their employees, whether through monitoring correspondence or even telephonic communications. Surveillance happens in restaurants, nightclubs, outside shops, in cameras mounted on the neighbour's wall – little attention is given to the right to privacy in these instances, or the need to alert the public to the fact that they are being watched.

Secrecy is at the core of surveillance – whether by states or businesses. It is why it works, and why it is a direct threat to our fundamental rights. It is no use to states or to businesses if those being surveilled know about it. To achieve this, new technology needs to be continually developed and sold to governments (and others). Australia argues that Snowden's revelations have resulted in an increased drive towards surveillance, not less: “Since the Snowden leaks, public reporting suggests the level of encryption on the internet has increased substantially. In direct response to these leaks, the technology industry is driving the development of new internet standards.”

So how do we slay Frankenstein's monster?

The country reports make several suggestions in this regard. A citizen-driven, balanced approach to legislating surveillance is necessary, with the recognition that some measure of surveillance is in the interests of public safety (against violence and crime, including the protection of children against pornography and child trafficking). Lebanon puts this clearly: “Many argue that online privacy is a human right, while others insist that it is a negotiated contract between the state and its citizens – a contract in which citizens exchange some of their data in return for national security.” (Secrecy is, in other words, different to the need for state secrets). Costa Rica argues that citizen oversight in the implementation of national databases and of surveillance programmes is also necessary. Users of the internet can practice safer communications using encryption technology, and other behaviour changes when going online – such as paying more attention to the kind of information they share with businesses or individuals.

The idea of the internet as a free, open space that promotes democracy needs to be revisited. “In mainland China the internet and everything in it can reasonably be viewed as public space – that is, ultimately belonging to the state,” the author

contends. In the UK, the Government Communications Headquarters (GCHQ) – the counterpart of the National Security Agency (NSA) in the US – has said: “[W]e are starting to ‘master’ the Internet... And our current capability is quite impressive... We are in a Golden Age.” In this context, as in Switzerland, privacy becomes a “privilege”, not a right.

Elsewhere, activists are going “offline” out of necessity and safety. In Indonesia, Papuan activists

say: “Now I only trust face-to-face communication. I rarely use the telephone to talk about sensitive issues.”

Privacy, transparency and accountability are key words. They are also old struggles. In this sense the terrain has not changed. But these country reports suggest the terrain might just have got rockier, and the path much more perilous.

ARGENTINA

“Your software is my biology”:¹ The mass surveillance system in Argentina



Nodo TAU

Flavia Fascendini and María Florencia Roveri
www.tau.org.ar

Introduction

In 2011 Argentine President Cristina Fernández de Kirchner created, through an executive decree,² a federal biometric system for the identification of citizens, named SIBIOS (*Sistema Federal de Identificación Biométrica para la Seguridad*). It was developed, according to the decree, to provide a centralised system of information regarding individual biometrics registers. This would be used for appropriate testing when identifying people and faces, optimising the investigation of crimes and supporting national security.

The adoption of this measure involved very little – almost no – public discussion, except for a few civil society organisations that warned the government about the risks involved in these kinds of surveillance methods, and their implications for people’s right to privacy.

Two strong arguments emerged:

- There is a risk involved in this information being in the hands of a government in a democratic regime. In Argentina this argument is made within the context of the dictatorial governments the country experienced following military coups, the last of them extending from 1976 until 1983.
- The low level of public awareness regarding the possible violation of human rights related to the implementation of the system revealed the absence of social debate around the violation of human rights related to information and communications technologies (ICTs).

Policy and political background

Argentina is recognised worldwide for being one of the first countries to adopt biometric technologies as a form of recognition of individuals’ legal

identity. In the late 1800s, an Argentine police officer named Juan Vucetich established the first system of fingerprint identification³ and started the use of fingerprint evidence in police investigations.⁴

In Argentina, the national identification document (DNI is its acronym in Spanish) is the only personal identification document individuals are obliged to have. Its format and use have been regulated since 1968 by Law No. 17671⁵ for the Identification, Registration and Classification of National Human Potential, which also created the National Registry of Persons. It is issued to all people born in the country, and to foreigners who apply for a residence permit, once the National Directorate of Immigration considers that the applicant meets the necessary requirements to that end. Since November 2009, and as part of the digitalisation of national documents, a new national identification document was issued as a plastic card.

In Argentina, data protection has both constitutional and legislative protection. The constitution states in Article 43 that any person can file an action of *habeas data* “to obtain information on the data about himself, and its purpose, registered in public records or databases, or in private records or databases intended to supply information; and in case of false data or discrimination, this action may be filed to request the suppression, rectification, confidentiality or updating of said data. The secret nature of the sources of journalistic information shall not be impaired.”⁶

At the same time, Law 25.326⁷ on the Protection of Personal Data (2000) deals with the administration of public and private databases that include personal information. The legislation prevents any entity from handing over personal data unless it is justified by legitimate public interest. The

law created the National Directorate for Personal Data Protection. Legal experts consider this law an advanced one, because its regulation was prior even to some technologies being used in practice. The Argentine version of *habeas data* is considered one of the most complete to date.

However, as mentioned by the Association for Civil Rights, Argentina “also suffers from a chronic lack of control over its intelligence agencies. Every now and then, the accounts of public officials, politicians and journalists are hacked and scandal erupts. These abuses are the result of an Intelligence Law for which parliamentary oversight mechanisms simply don’t work.”⁸

Also relevant to the analysis is the Anti-Terrorist Act No. 26.268,⁹ driven through in 2007 without parliamentary debate, which aims to punish crimes of terrorism. The Act defined a duplication of penalties for any offence contained in the Criminal Code if committed by an organisation or individual who seeks to create terror among the population or “compel a government to take action or refrain from taking it.” This definition could be applied to certain labour or social-related demands. That is why human rights organisations fear that the Act serves to criminalise social protest. In addition to this legal framework that could allow the criminalisation of social protest, the biometric system could offer a tool that aggravates the risk. After the pressure and debate generated around the treatment of the Act, the executive agreed to include a point that establishes that “the aggravating circumstances provided do not apply where the act or acts in question take place in the performance of human and/or social rights or any other constitutional right.”¹⁰

A biometric system for the identification of citizens

SIBIOS, which was developed with the technological cooperation of the government of Cuba,¹¹ is a centralised database that is fed by information collected by the National Registry of Persons (RENAPER - *Registro Nacional de las Personas*). RENAPER is responsible for issuing national identity documents and passports, a task which used to be the responsibility of the Federal Police. It collects the fingerprints, a photograph and the signature of

every citizen who is obtaining an identity document or passport.

After that, RENAPER provides the biometric information necessary for the Automated Fingerprint Identification System (AFIS) as well as the faces used by the Federal Police to satisfy the requirement of identification made by users of SIBIOS. The AFIS started with a database of eight million biometric records collected when the police used to issue identity cards and passports.

The Ministry of Security has the authority over the application of the system, which can be used by these organs of the state: the Federal Police, the Argentine National Gendarmerie, the National Coast Guard, the Airport Security Police, the National Directorate of Immigration and the National Registry of Persons. The national government also encourages provincial entities to use the system, through the Federal Programme of Partnership and Assistance for Security.¹²

The National Office of Information Technology (ONTI), under the direction of the Chief of the Cabinet of Ministers, provides advice related to required standards, equipment compatibility and software and hardware platforms. Since 2011, the team implementing the SIBIOS system has been working closely with the National Institute of Standards and Technology (NIST) in the United States, in order to keep the Argentine software in line with NIST’s standards.

The main governmental argument to justify the use of this system is that it is supposed to provide “a major qualitative leap in security in the fight against crime,”¹³ a very sensitive issue for citizens these days and clearly the main issue on the public agenda.

A promotional video¹⁴ of SIBIOS – launched by the government – highlights the importance of identity databases in a positive way. “If we know more about who we are, we can take better care of ourselves,” states the introduction to the video. It argues that faces, fingerprints and signatures are three essential elements of identity and they should be managed by a very efficient system. It also mentions that in the future the system could integrate other data such as voice, iris scans and DNA.

The video describes the AFIS as a technology used to identify physical characteristics and human behaviour. It also mentions the importance of SIBIOS for the identification of people without identity

1 Cippolini, R. (2010, November 29). Tu software es mi biología. *Cippodromo*. <http://cippodromo.blogspot.com/2010/11/tu-software-es-mi-biologia.html>

2 Decreto 1766/2011. www.infoleg.gob.ar/infolegInternet/anexos/185000-189999/189382/norma.htm

3 Biography of Juan Vucetich, Visible Proofs. www.nlm.nih.gov/visibleproofs/galleries/biographies/vucetich.html

4 Pirlot, A. (2013, December 10). Ignoring repeated warnings, Argentina biometrics database leaks personal data. *Privacy International*. www.privacyinternational.org/blog/ignoring-repeated-warnings-argentina-biometrics-database-leaks-personal-data

5 Act Nº 17.671. infoleg.mecon.gov.ar/infolegInternet/anexos/25000-29999/28130/texact.htm

6 en.wikipedia.org/wiki/Habeas_data

7 www.infoleg.gov.ar/infolegInternet/anexos/60000-64999/64790/texact.htm

8 Álvarez Ugarte, R. (2013, October 30). Argentina’s new biometric ID system ignores right to privacy. *IFEX*. www.ifex.org/argentina/2013/10/30/new_surveillance

9 infoleg.mecon.gov.ar/infolegInternet/anexos/125000-129999/129803/norma.htm

10 Act 26.734. infoleg.mecon.gov.ar/infolegInternet/anexos/190000-194999/192137/norma.htm

11 vimeo.com/77142306

12 infoleg.mecon.gov.ar/infolegInternet/anexos/215000-219999/218789/norma.htm

13 Official presentation of SIBIOS. <https://www.youtube.com/watch?v=9goN2MR1TR4>

14 vimeo.com/77142306

documents in accidents, economic crimes including phishing, or human and – specifically – child trafficking. It also mentions that the physiognomic recognition of individual's faces that this system uses allows for the projection of how people's faces will change over time.

The government maintains that the implementation of this system also strengthens migratory controls in order to ensure that every person that enters the country is the same person that leaves it. Besides this, the system increases the chances of clarification of solving crimes, providing greater scientific support in the resolution of criminal cases.

Even though the system is considered a step forward as a government resolution to act on these sensitive matters, implementing it could entail some dangers, depending on how it is used in the future:

- SIBIOS collects information from all Argentine natural citizens, as well as foreign residents in the country, by means of the first article of Decree 1501/09.¹⁵ Some of the data collection standards also apply to *foreign individuals who do not have a national ID* such as tourists or travellers in transit who arrive in the country. This actually means that the scope of the data collection exceeds even the 41.09 million inhabitants of Argentina.
- SIBIOS will be *fully “integrated”* with existing ID card databases, which aside from biometric identifiers include the digital image, civil status, blood type and key background information collected since the person's birth. Apparently there is an intention to increase the amount of data collected. Recently a legislator presented a bill that proposes including palm prints among the registries for the system.¹⁶
- The main criticism of the system is that it contradicts privacy norms and also has implications in terms of the citizens' security, since there are no clearly established mechanisms of control for the system. In this sense, the local organisation *Fundación Via Libre*, with the support of the Electronic Frontier Foundation (EFF), raised the alarm about the implementation of SIBIOS and the risk it implies for people's privacy. The EFF has been warning for a long time about how damaging it is for a free and democratic society to aspire to having “perfect surveillance”. Along the same lines, the founder of WikiLeaks, Julian

Assange, said that Argentina – although not on the scale of China and the United States – has “the most aggressive surveillance regime in all of Latin America.”¹⁷

As mentioned before, the concerns in terms of SIBIOS relate not only to the power created through data centralisation, but also to different issues regarding its implementation and use. The decree that allows the implementation of SIBIOS does not include adequate mechanisms of control and protection of sensitive personal data. The functions assigned to the coordination unit created to manage the system are not clear and it is not an autonomous body.

There has also been no public discussion about the conditions under which public officials will have access to the data. Yet this type of mass surveillance can have serious repercussions for those who are willing to voice political dissent. The risk is even worse considering other public policies and private initiatives related to monitoring public spaces – such as monitoring streets using video cameras¹⁸ in the most important cities of the country¹⁹ or implementing a biometric system for the identification of people at football games when there is violence.²⁰

According to Eduardo Bertoni, an Argentine lawyer specialised in freedom of expression and ICT issues, the deficiencies in the institutional design when it comes to implementing SIBIOS could increase the dangers already predicted by the critics of the system's implementation.²¹ Another aspect highlighted by Bertoni²² is the so-called “right to anonymity”, considered as one of the basic guarantees of democracy, because it allows the expression of opinion without fear of reprisal. Consequently, this right also enables freedom of expression.

Conclusions

If we consider SIBIOS a tool implemented for the investigation of crimes, the system is a good resource. However, the issue of the sensitivity of the

data, and the ways it is used in the investigation of crimes, should be decided in a participatory way in a democratic society. The lack of legislative debate due to the fact that the creation of SIBIOS was decided by a presidential decree leaves the issue out of the reach of public opinion.

There was little consultation before the implementation of SIBIOS with non-governmental and independent entities – which is usually a positive feature of the current government when it comes to shaping policies and legislation that impact on basic human rights. Because of this, there are extremely low levels of awareness of the risks entailed in the collection of such an amount of private data that remains in the hands of the state and within the reach of public security bodies.

Even though the rights to privacy and data protection are enshrined in international law and in the Argentine constitution, national IDs and similar methods of data centralisation increase state capacity for intrusive surveillance. In this sense, the rationalisation for the collection of biometric data in a nationwide ID scheme should be examined to avoid the *unnecessary* collection, processing, retention and sharing of this very sensitive data.

Regarding transparency in the implementation of the system in Argentina, the measure was officially announced in the media at the time it

was launched, described as being a technological improvement to help fight crime and as an action framed within the overall modernisation of the state. Since both arguments strike the general public as advancements, this might have negatively affected open, intensive and thought-provoking debate around the real implications of the measure.

Action steps

- In this context, the following action steps can be recommended in Argentina:
- Demand more transparency and accountability from the government in terms of the use of the biometric information, including who has access to it.
- Develop campaigns targeting legislators in order to inform them of the controversial aspects the issue raises in relation to human rights.
- Create awareness campaigns for citizens so they are informed of the risks this initiative poses when it comes to personal data, privacy and surveillance.
- Conduct comparative research on the success and failures of similar systems in other countries where they have been implemented.

¹⁵ infoleg.mecon.gov.ar/infolegInternet/anexos/155000-159999/159070/norma.htm

¹⁶ www.diputados.gov.ar/proyectos/proyecto.jsp?id=159974

¹⁷ Interview with Julian Assange by Infobae. www.youtube.com/watch?v=If7MbOvuEbg

¹⁸ Ramallo, F. (2013, August 29). Porteños bajo el foco de las cámaras de vigilancia. *Infotechnology.com*. www.infotechnology.com/comunidad/Porteos-bajo-el-foco-de-las-camaras-de-vigilancia-como-funciona-el-sistema-de-monitoreo-20130826-0004.html

¹⁹ CEMAC (Centro de Monitoreo y Atención Ciudadana) www.rosario.gov.ar/sitio/lugaresVisual/verOpcionMenuHoriz.do?id=8726&idLugar=3988

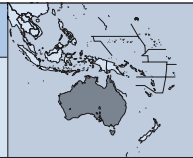
²⁰ AFA Plus. www.afaplus.com.ar/afaplus

²¹ Bertoni, E. (2013, December 15). Una herramienta peligrosa. *La Nación*. www.lanacion.com.ar/1647828-una-herramienta-peligrosa

²² Interview with Eduardo Bertoni by Infobae, 24 April 2014. www.palermo.edu/derecho/up-en-los-medios/gobernanza-global-de-internet.html

AUSTRALIA

Internet the panopticon: Exhibition and surveillance



Andrew Garton
www.agarton.org

Introduction

The story of the internet is imbued with our desire to tell each other stories – *the campfire of our times* as artist/musician Laurie Anderson¹ harvested from her iconic imagination. It is from such like minds – exploratory, free-thinking and socially conscious – that the earliest of computer networks rebuilt themselves upon and throughout the emergent internet, an internet of like minds that would inform, inspire and challenge the power structures that threatened the well-being of people, their culture and the flora and fauna on the precipice of extinction. That is the ideal many of us held onto as we travelled the world bringing modems to where they were needed, to where they were wanted. Things did not work out as we had envisaged, but we held our ground.

This report discusses the privacy and online security concerns of 13 Australians, two Malaysians and an ex-pat living in the United States (US), all of whom have journeyed the internet in unique ways, some since its inception and others in more recent times. They are all colleagues of mine, most of whom I have worked with or met through online media projects over the past 25 years. I wanted to know how we were doing as an online community, given both our aspirations at the outset and the revelations that continue to haunt our presence online, and that of the global internet community.

As early as 1986 a panel at the annual conference for computer graphics, SIGGRAPH,² predicted that creative and social uses of computing would overtake scientific and technological uses within ten years. Not a bad piece of crystal-ball gazing. We thought, or at least I thought, this would be a

good thing. In 1989 Ian Peter, co-founder of Australia's Pegasus Networks, sought affordable global communications for everyone. I liked the sound of that and hopped on board. Online activist Mysta Squiggle was keen to connect "activists and people with odd interests, including whistleblowing." Seemed to fit with our work at Pegasus Networks. We sought to make this happen.

Dr. June Lennie, convenor of a Queensland rural women's network, "saw the internet and email as potential means of supporting and empowering women and reducing the isolation of women in rural and remote Queensland." Her critique of networks, "that computers were linked to masculine discourses of technology which tended to exclude women and created barriers to the effective use of computers by women," was taken up with vigour through the Association for Progressive Communications' Women's Networking Support Programme (APC WNSP), which in the early 1990s Pegasus Networks had also contributed to.

NGO worker Sandra Davey saw the early internet informing, empowering and connecting us, while others, such as musician Andrew Sargeant, aspired to "play Doom online with four players via BBS³ on 28.8k dial-up connection." Andrew's BBS networks would often dovetail with ours. Those kids playing Doom, some of whom I would meet, would aspire to be informed and empowered and stimulate connected communities, just as Sandra foresaw.

It was sounding pretty good. However, whether it be game play, whistleblowing or affordable communications for everyone, the promise was no match for the threat that lay ahead. I myself humbly predicted that repression – or power structures for that matter – would be no match for an informed citizenry.⁴ In fact, the backlash to our efforts has been so all consuming, so pervasive, that 25 years later Squiggle considers the only remaining level playing field is an internet with no privacy whatsoever!

Who cares about online privacy?

Apart from Squiggle, who proposes an internet bereft of privacy, my colleagues care deeply about their privacy. Closer to home, do Australians care about theirs?

A survey conducted by the Office of the Australian Information Commissioner (OAIC), with results published in October 2013, unreservedly clarified that Australians of all ages do care about their privacy, specifically around improper information sharing, collection and processing by businesses and government agencies.⁵

Bruce Baer Arnold, assistant professor at the School of Law at the University of Canberra, summarised these findings by describing that some Australians "aren't engaging with businesses they consider untrustworthy. Some are complaining about privacy abuses... some young people claim their privacy is important but still engage in 'too much sharing' on social networks such as Facebook." In general, consumers "have a perception that governments actually don't care much about the privacy of ordinary people."⁶ So what does the government care about?

What does the government care about?

Well, surprise surprise. The Australian government wants to know what its citizens are doing. All of its law enforcement bodies are keen to support a mandatory data-retention scheme. And they are using Edward Snowden's revelatory leaks as an excuse to increase privacy encroachments in Australia. An extract from the Australian Security Intelligence Organisation's (ASIO) response to the Senate Inquiry into the Telecommunications (Interception and Access) Act 1979 reads:

These changes are becoming far more significant in the security environment following the leaks of former NSA contractor Edward Snowden. Since the Snowden leaks, public reporting suggests the level of encryption on the internet has increased substantially. In direct response to these leaks, the technology industry is driving the development of new internet standards with the goal of having all Web activity encrypted, which will make the challenges of traditional telecommunications interception for

necessary national security purposes far more complex.⁷

This is the first time in Australia that the alleged uptake of encryption software as a consequence of a whistleblower's leaks is used as an argument to push for legislation that would effectively see ASIO spy on most, if not all Australian citizens. Chris Berg, director of policy at the Institute of Public Affairs, says "the Snowden angle is a new one, demonstrating the rhetorical leaps that agencies such as ASIO are willing to make to grab new powers."⁸

The internet, and offspring technologies, have become the one-stop-shop for knowing all things about everyone. It forgets little to nothing. There was a time when the Australian government could not care less about the internet. In the early 1990s the government and many NGOs were still coming to grips with fax machines. Faxes presented their own challenges at a time when many of us were encouraging Australian progressives and community organisations online, as well as critical human rights observers and indigenous community support advocates across Southeast Asia and the Pacific Islands. We were seen as odd and idiosyncratic. At that time the early internet was about as complex to most people as a VHS⁹ remote control.

However, in spite of the internet, the Australian government has kept a close watch on its citizens for some years. In fact, a "multilateral agreement for cooperation in signals intelligence between the United Kingdom, the United States, Canada, Australia, and New Zealand", otherwise known as the Five Eyes, originated in 1941. Originally referred to as the UKUSA Agreement, it was allegedly a secret treaty hidden from parliamentarians until 1973, when it became known to the prime minister of the day, Gough Whitlam. Whitlam went on to discover that a secret surveillance station known as Pine Gap, located in the Northern Territory, was allegedly operated by the US Central Intelligence Agency (CIA). Strongly opposing the use of Pine Gap by the CIA, Whitlam fired the then head of ASIO before he himself was controversially dismissed as prime minister by order of the Governor-General Sir John Kerr in 1975.

¹ McCorduck, P. (1994). America's Multi-Mediatrix. *Wired*, March. archive.wired.com/wired/archive/2.03/anderson.html

² SIGGRAPH, founded in 1974, is an international community of researchers, artists, developers, filmmakers, scientists and business professionals who share an interest in computer graphics and interactive techniques. www.siggraph.org/about/about-acm-siggraph

³ Bulletin Board Services (BBS) were computers reachable by way of a direct phone call via a modem. BBS software provided the user, once a call was successfully made, with access to publicly accessible files and real-time text-based chat.

⁴ Garton, A. (1993) The Net: Promise or Threat? 21-C, 12, Autumn 1994.

⁵ OAIC. (2013). *Community Attitudes to Privacy survey Research Report 2013*. www.oaic.gov.au/privacy/privacy-resources/privacy-reports/oaic-community-attitudes-to-privacy-survey-research-report-2013

⁶ Baer Arnold, B. (2013, October 9). The Australian public cares about privacy: do politicians? *The Conversation*. theconversation.com/the-australian-public-cares-about-privacy-do-politicians-19033

⁷ ASIO submission to the Senate inquiry into a comprehensive revision of the Telecommunications (Interception and Access) Act 1979, February 2014. goo.gl/6wbcqh

⁸ Berg, C. (2014, March 18). ASIO: Fixing one massive privacy breach with a second massive privacy breach. *Freedom Watch*. freedomwatch.ipa.org.au/asio-massive-privacy-breach-second-massive-privacy-breach

⁹ The video home system (VHS) is a consumer-level analogue recording videotape-based cassette standard developed by Victor Company of Japan. en.wikipedia.org/wiki/VHS

In subsequent years both funding to and the powers of ASIO have increased at an unprecedented pace,¹⁰ including amendments to the ASIO act, giving it the wherewithal to spy on anyone involved in WikiLeaks.¹¹ Moves to impose judicial oversight on ASIO, based on the recommendations of two reports – one by the Council of Australian Governments – were presented to the government in December 2013. This has all but been shelved by the present government, which has substantially increased resources to both ASIO and the Australian Secret Intelligence Service (ASIS).¹² Additionally, ASIO's relationship with US agencies has deepened. Documents from the US National Security Agency (NSA),¹³ dated February 2011, describe the ever-widening scope of the relationship Australia has with them, in particular assistance with the increased surveillance of Australian citizens.¹⁴ It has also been revealed that a secret 2008 document states Australia's Defence Signals Directorate offered to share with its major intelligence partners, namely those that make up the Five Eyes, information collected about ordinary Australians.¹⁵

Did we get the internet we wanted?

Many of us sought a means to inform the largest number of people about local and international events that were overlooked by mainstream media. Self-professed “geek” and businesswoman Juliette Edwards put her efforts into a vision of a “more open-minded global community with less fear and more tolerance of others’ differences.” Sandra Davey experienced an internet that did connect “like-minded peeps throughout the world and it was all about action. The internet informed

us, empowered us, connected us,” while founder of the Australian Centre for the Moving Image and now painter John Smithies foresaw the opportunities that “graphics and audio standards” afforded the imminent development of technologies that would see an internet populated by video.

Like many who sought to change the way we govern, feed and sustain ourselves, through equitable means that would feed a population more tolerant of each other, more conscious of the world we inhabit and eat from, we seem to have created the ultimate in panopticons.

John's vision of video everywhere is one of the miracles of the internet, while the altruistic expectations are being fought over day in day out. In some respects we seem to have also found a world increasingly less tolerant of each other.

With everyone online serving up individual opinions, the notion of an informed public making informed decisions is increasingly questionable. But as tragedies, such as the 2009 Black Saturday Bush Fires in Australia, bring people of all persuasions together to find a common bond and common ground, international events are no doubt driving the like-minded together in ways we have yet to truly know.

We are the exhibitors in a surveillance society, a virtual panopticon that documents our movements from street corner cameras to MAC¹⁶ address readers, from ATMs¹⁷ to border controls, modulating our personality profiles with billions of “likes” and “tweets” and the content that billions more share willingly on cloud servers that may as well be as porous as polymeric foams! The internet is young and naïve. Perhaps so are we... and many are suffering for it. May it not be so for much longer.

Do we need to be watched?

We all want to reach in and across the net to inform ourselves, to share in confidence intimate moments between friends and family, whether it be in an email or photos and videos within social networks. Some of us would like to find new audiences for our personal endeavours, whether it be research, poetry, knitting or stamp collecting... and we find inspiration in others we might meet in those spaces and the ones we find in between. This is the kind of internet I had sought to contribute to; not one that

finds one self-censoring within known commons, whether it be public or privately owned.

Self-censorship can be a great tool when wanting to find common cause with people of wide-ranging interests. However, within the context of mass surveillance, self-censorship is, as Ian Peter describes, “an affront to human dignity.” Ian goes on to suggest that “humans have worked together before to limit excesses in the common good. Clearly we have excesses here and we need necessary and proportionate principles to be applied to surveillance.”

Only those who are committing serious internationally recognised crimes ought to be fearful of surveillance. The rights of the rest of us need to be respected. Confidentiality, as Peter puts it, is “important to social discourse and as a part of freedom of expression.” Anonymity protects the outspoken in politically volatile countries; however, June Lenie agrees with the idea that “not allowing people to post messages anonymously could reduce the amount of abuse that happens online these days.”

Whether we continue to abuse each other or find common cause to rail against those who would stifle free expression and inquiry remains to be seen. As I write, the present Liberal/National coalition government in Australia has cancelled the contract of the Australia Network, the public broadcast unit that served the Asia-Pacific region, resulting in 80 job losses in both the Asia Pacific News Centre and Australian Broadcasting Corporation (ABC) International.¹⁸ Constraints to independent media in Australia are being gruffly imposed, with the Australia Network being the first to be axed, and further cuts to the national broadcaster, the ABC,¹⁹ expected. It is no secret that Rupert Murdoch has had a hand in these changes,²⁰ furthering the notion that Australia is following the US in whatever means necessary to undermine the egalitarian principles of democracy, replacing it with an oligarchy.

Turning the panopticon back in on itself

Vested interests in the internet and its ever-increasing outreach through devices that we use every day are no doubt watching and recording our

every movement. Photographer Werner Hammerstingl describes the internet as “a place where it's not always easy to escape the data harvesting and profiling that's now omnipresent.” Sandra Davey “can't stand the idea of bots and humans compiling data” about her – behind-the-scenes features that she has not given any permission for. “It irks me, it upsets me,” she says. “I do the best I can to prevent that, but I fear for how much is already known about me out there somewhere.”

Turning the panopticon in on itself

Can we turn the panopticon in on itself? Does the internet still give us the means to create the world we would like to live in? Can we do so in a world where, as Sandra describes, the next generation that hops online after us “has little understanding of what they've given away, barely without a thought”? As a woman, Davey is “deeply fearful and concerned about what has happened to thousands of young girls who have traded their utmost privacy for instantaneous gratitude, fun, play or recognition.”

Broadcaster and writer Nyck Jeans suggests that we can turn the panopticon back in on itself. There is always “the potential that those who challenge the system CAN gain access, educate us, subvert and shift world opinions through the very same methods the ‘powers’ use to peek into lives and seek control via knowledge of private habits and political affiliations.”

Governments are behaving badly, but we need governance structures to deal with the inequities, to tackle the oligarchs and hold security services accountable. The internet has proved to be so powerful a means to make such a thing possible that it has been turned against us. But for those of us who helped to create it, we know that we have the means, and those in the coming generations who have the technical means and political willpower can and will use the promise of an internet commons.

“Governments,” Matt Abud says, “often can, and will, use their tools for anti-democratic state agendas, and they'll manipulate the crime rhetoric to advance towards other, unconnected goals.”

Even so, Matt continues, we still need governments to tackle organised crime. “It needs transparent oversight of accountable regimes, rather than only taking power away from regimes. That's the conundrum.”

Our voices, our intentions, our loves and passions may be heard and recorded, but do we remain silent, do we contest the commons the internet promised?

10 Keane, B. (2011, July 5). ASIO gets its new powers – and no one will tell us why. *Crikey*. www.crikey.com.au/2011/07/05/asio-gets-its-new-powers-and-no-one-will-tell-us-why

11 Intelligence Services Amendment - “Wikileaks Amendment”, speech by Senator Scott Ludlam, 4 July 2011. greensmps.org.au/content/speeches/intelligence-services-amendment-wikileaks-amendment

12 Garnaut, J. (2014, July 10). ASIS and ASIO to get injection of funds to fight threat from Middle East. *The Sydney Morning Herald* www.smh.com.au/federal-politics/political-news/asis-and-asio-to-get-injection-of-funds-to-fight-threat-from-middle-east-20140710-zt3dm.html

13 Greenwald, G. (2014). *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*. New York, Metropolitan Books.

14 Farrell, P. (2014, May 13). Australia asked Americans for more help to spy on Australian citizens. *The Guardian*. www.theguardian.com/world/2014/may/13/australia-americans-help-spy-terror-suspects

15 MacAskill, E., Ball, J., & Murphy, K. (2013, December 2). Revealed: Australian spy agency offered to share data about ordinary citizens. *The Guardian*. www.theguardian.com/world/2013/dec/02/revealed-australian-spy-agency-offered-to-share-data-about-ordinary-citizens

16 A media access control address (MAC address) is a unique identifier assigned to network interfaces, such as the networking components of a smartphone, by the manufacturer of a network interface controller (NIC), and is stored in its hardware. en.wikipedia.org/wiki/MAC_address

17 An automatic or automated teller machine (ATM) is an electronic interface common to banking services.

18 Australian Associated Press. (2014, July 14). ABC to lose 80 staff in Melbourne due to budget cuts, union confirms. *The Guardian*. www.theguardian.com/media/2014/jul/14/abc-to-lose-80-staff-in-melbourne-due-to-budget-cuts-union-confirms

19 Dempster, Q. (2014, June 4). What we will lose if we destroy the public broadcaster. *Crikey*. www.crikey.com.au/2014/06/04/what-we-will-lose-if-we-destroy-the-public-broadcaster

20 Dyer, G., & Keane, B. (2013, December 3). The ABC v the Murdochs: your guide to the battlefields. *Crikey*. www.crikey.com.au/2013/12/03/the-abc-v-the-murdochs-your-guide-to-the-battlefields

Media theorist and writer Paul Brown reminded me of this poem by Martin Niemöller:²¹

First they came for the Socialists, and I did not speak out –

Because I was not a Socialist.

Then they came for the Trade Unionists, and I did not speak out –

Because I was not a Trade Unionist.

Then they came for the Jews, and I did not speak out –

Because I was not a Jew.

Then they came for me – and there was no one left to speak for me.

It is not uncommon....

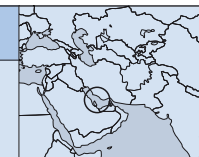
It is not uncommon that I hear the sound of children crying in my sleep. The world has become, Juliette Edwards says, our prison. We are reading daily of the poor behaviour of governments and their security services the world over, in particular the Orwellian NSA and their contempt for any public oversight or scrutiny.

Every day we are seeing footage from war zones and outright, brazen atrocities perpetrated by powerful governments and their elites on civilian populations increasingly marginalised by inept international response; and the castration of independent media and the victimisation of journalists. A year since Snowden's infamous revelations, one wonders if anything has changed. The screws are tightening and I still hear the sound of children crying as I sleep.

"If there is anything important in all the masses of noise," suggests Andrew Sargeant, "it would be like finding a haystack, inside a needle, inside a haystack."

BAHRAIN

The struggle of online activists against surveillance technology



Ali Abdulleamam

Introduction

Bahrain is a tiny island in the Persian Gulf, ruled by the Al-Khalifa family since 1783. The population of Bahrain stands at 1,314,089:¹ 46% are Bahraini and the rest are foreigners, mainly workers.

The illiteracy rate stands at 1.13% of the population (2013).² At 87%, Bahrain has the highest internet penetration rate amongst Arab countries³ and also has the highest Twitter usage.⁴ Information and communications technologies (ICTs) are very important both to foreigners and the Bahrain economy, which is dependent on financial services and offshore banks. The internet became available in the country in 1994, making Bahrain one of the earliest Arab countries in the region to have internet.

Since the start, civil society activists have used the internet for their activities and communications – leading to the first arrest of an online activist in 1998, the censoring of sites and, recently, spying on activists through advanced surveillance technology.

Civil society organisations depend on the internet for advocacy, as the traditional media is either owned by the regime, or is controlled through publishing law.⁵ Publishing stories or media releases on the internet is a way for activists to go viral in Bahrain.

Policy and political background

BahrainOnline.org⁶ (BOL) was the first site to be created and funded by online activists. It was started in 1998 during the implementation of the State Security Law⁷ (from 1975 to 2001), which allowed the government to arrest anyone for three years without proper investigation or trial. This was also during the Dignity Uprising in Bahrain⁸ (1994-2000),

which led to dozens of deaths and thousands of political prisoners. For more than 100 years Bahrain has been known to experience uprisings every 10 years. The regime is also widely known for its human rights violations, torture, discrimination and totalitarianism.

BOL was the main source for opposition opinions and in 2001 during the National Action Charter⁹ (NAC), a reform project launched by the new emir, BOL hosted an online debate to discuss it – and similar online discussions have continued since its launch. This has caused a shift from BOL just reporting on stories, to acting as a public opinion maker, often critical of the government.

Campaigns have been launched on the website, and videos and photos of protest activities or human rights violations posted online. The fact that the regime could no longer control the flow of information and news led to the arrest of activists who ran the site in February 2005.¹⁰ The site was blocked in 2002, although massive public interest in the site remained.

Online resistance

In March 1999 the previous emir of Bahrain died suddenly and his son succeeded him to the throne. At that time the Dignity Uprising was struggling, after most of its activists on the ground had been arrested. There was also no political will to move forward with reform, the state security law and its men were controlling the island, and the economy was in difficulties.

At that time BOL started to become popular and received more attention from people trying to find news from different, credible sources.

When the new emir came to power, he promised real reform, allowing people to have their full rights, including freedom of expression, and shifting the power to the people. Basically, he promised to modernise the country. People believed him, and started to debate the NAC. Many started to share their opinions on BOL, using anonymous names which gave them some privacy and security.

21 en.wikipedia.org/wiki/First_they_came_

1 <https://www.cia.gov/library/publications/the-world-factbook/geos/ba.html>

2 www.alwasatnews.com/3654/news/read/699870/1.html

3 www.alwasatnews.com/4070/news/read/823318/1.html

4 www.alwasatnews.com/3825/news/read/742134/1.html

5 iaa.bh/ar/arpolicyRules.aspx

6 en.wikipedia.org/wiki/Bahrain_Online

7 www.legalaffairs.gov.bh/LegislationSearchDetails.aspx?id=5682#.U9EIU4BdUZE

8 en.wikipedia.org/wiki/1990s_uprising_in_Bahrain

9 en.wikipedia.org/wiki/National_Action_Charter_of_Bahrain

10 Committee to Protect Journalists. (2005, March 14). Attacks on the Press 2014: Bahrain. *Committee to Protect Journalists*. www.cpj.org/2005/03/attacks-on-the-press-2004-bahrain.php#more

BOL's credibility grew, even though it was run by an unknown group. The government started to pay attention to it in order to get a sense of how citizens felt about the reform project. However, when differences arose between the government and the opposition regarding the new constitution that had been issued by the king without reference to the opposition, BOL played a huge role in revealing the difference between a constitutional monarchy and what the king was offering with his new constitution. Articles were printed from the site and distributed. This again helped BOL to become a credible resource, especially when the opposition depended on it to post messages.

In 2002, during the first election and the opposition's call for a boycott, BOL was the only media outlet supporting the boycott. This led to the arrest of three activists who used to run the site. They were imprisoned for a period of two weeks on the charge of insulting the king, broadcasting hate speech and posting false news.

During this time BOL moved from being an online platform to playing a role "on the ground", arranging protests, visiting hospitals and even issuing media releases when important things were happening. BOL was covering the protests live, and posting pictures of events that may not have appeared in the traditional media. At times it wrote investigative stories about corruption. This led to the site being blocked in 2002.

Blocking BOL showed how loyal people in Bahrain were to the site. They shared proxies between them and members wrote a script to open the site. They used Dynamic DNS to create redirected links. When the links were censored, members shared a document on how to create your own link with readers. This kept BOL up and running, and, with 80,000 hits a day, it became the most read site in Bahrain.

This was the first hint of how people could train themselves to use new technology to avoid censorship in Bahrain. During the arrest of the administrators of BOL, the members organised several protests themselves, asking for the release of the administrators, and the dropping of charges against them. This led to widespread coverage in the media, and the release of the administrators without trial.¹¹

During the arrest of the BOL administrators, the government discovered that they lagged behind in technical knowledge, and that they had failed to understand the nature of the internet. They started to use new tools to censor the opposition websites. But, again, people learned how to bypass the new censorship technology.

In February 2009, a member of BOL using the nickname "äÇÖß ÇäääÇÆßÉ"¹² posted the full list of the names of the employees of the National Security Apparatus (NSA). Two months later,¹³ on 14 May, Hasan Salman was arrested and charged with "publishing secret information over the internet".¹⁴ In September 2009 Hasan was sentenced to three years by the High Criminal Court.¹⁵ He was recently released.

After this incident, and the same year, the Telecommunications Regulatory Authority (TRA) issued new regulations for internet service providers (ISPs)¹⁶ saying that all ISPs should retain their communications logs for three years, as well as providing technical access for the NSA to monitor or block online communications in Bahrain. This regulation was greeted with huge opposition from the media, NGOs and members of parliament. However, it seems it will be implemented soon.¹⁷

In 2010, when the government arrested human rights activists, public figures and bloggers (including a BOL administrator for the second time), the NSA confronted them with printouts of SMS text messages and emails, even though their devices had not been confiscated by the authorities.¹⁸

The only explanation for this is that the government had bought new surveillance technology, and installed it at all the ISPs. This includes the Bahrain Internet Exchange (BIE), as stated by Mai Al Khalifa¹⁹ in her first resolution in 2009 as minister of culture and media. This forced all ISPs to provide access to the government to block websites by installing the necessary equipment. This resolution was received negatively by NGOs and online activists.

When the Arab Spring started, the youth tried to organise themselves in a movement to push forward with reform. BOL was the platform used to talk about the idea,²⁰ plan it,²¹ organise it, and cover it, second by second. They called this push the Day of Rage and issued media releases stating their demands.²² Because people started to learn online

security tactics the government could not recognise or arrest the people behind the uprising.

When the crackdown started in Bahrain, the international media turned its back on what was going on in the country. Only the internet and the youth who believed they could bring about change kept the uprising alive, and now after three and a half years the movement in Bahrain is still alive because of them.

In 2012, Alaa Alshehabi,²³ among other activists, received suspicious emails from someone claiming to be from Al Jazeera. The attachment was infected with the FinFisher virus, sold by a UK-based company. An investigation by BahrainWatch.org led to the discovery of others infected by the same spy tool and raised awareness in Bahrain about the new technology that the government was using to attack activists.

BahrainWatch.org found that after the release of their IP Spy²⁴ report, no new activists were targeted. The investigation also found that the awareness of online security by activists is high, and that even non-activists have started to download encryption tools and more secure instant messaging.

Conclusions

In February 2014, the king ratified a law that severely punished those who insulted him, with from three to seven years imprisonment and a fine of up to USD 1,000. The problem is not with insulting the king as much as with the way the government is using the laws to take revenge on the opposition. Recently more than 15 people are either in prison or awaiting trial for using the internet. Some of them are accused of insulting religious symbols or figures, and some of them for insulting the king or the prime minister.

We also came across stories that people had been fired from their work because they had "liked" an article on Facebook, while others had their telephones stolen because pictures or a chat had been found on them.

Freedom of expression is defined as a universal human right which is needed by all human beings, and it should be protected by governments. Bahrain has ratified laws which should protect freedom of expression, but in reality the opposite happens: those laws are used as "political revenge", as the UN spokesperson said at the Human Rights Council in Geneva. Bahrain failed to obey 176 recommendations by the Human Rights Council in May 2012.

Internationally respected NGOs are keeping pressure on the Bahraini government to free bloggers, photographers, and human rights and political prisoners, as well as to stop human rights violations, but nothing is changing. Bahraini activists are simultaneously receiving international awards even though they are still in jail under fake charges, like Ahmed Humaidan, who has been imprisoned for 10 years.

If the international community cannot put pressure on the regime to start reform to meet the demands of the people in Bahrain, at least we should put pressure on companies to stop selling surveillance technology to Bahrain that is used to violate human rights. When spy tools are sold to the government, human rights defenders will have to work harder, they will not be able to move freely, they will not be able to communicate and document stories, and they will always feel as if their ICT devices are a weapon being used against them.

We should not accept the argument that companies are not responsible for the way their products are used; they know that some countries have a bad human rights record and a long history of attacking activists. This technology will definitely be used to violate human rights.

Action steps

The state of Bahrain is using laws to repress remaining freedoms as a method of "political revenge". Selling it technology that allows it to do this is not making the world a better place. With more than 20 online activists and photographers in jail right now, and more than 15 journalists and bloggers living in exile, we should launch a global campaign against selling surveillance technology to Bahrain. We should also argue that the companies that sell this technology to governments should uninstall it remotely. By sharing information with the public on the kind of technology used, and through offering training, citizens can learn how to protect themselves online.

Over the past 16 years the people of Bahrain have managed to teach themselves how to avoid censorship or use secure routes for their online activities. But we should not rely on them continuing to understand the new surveillance technology entering the market, and being able to fight it.

¹² bahrainonline.org/showthread.php?t=229316

¹³ freehasan.wordpress.com/2009/05/15/arrest

¹⁴ freehasan.wordpress.com/calendar

¹⁵ freehasan.com/?p=310

¹⁶ www.tra.org.bh/media/document/PublishedLawfulAccessRegulation-1.pdf

¹⁷ www.alwasatnews.com/2393/news/read/44106/1.html

¹⁸ Silver, V., & Elgin, B. (2011, August 22). Torture in Bahrain becomes routine with help from Nokia Siemens. *Bloomberg*. www.bloomberg.com/news/2011-08-22/torture-in-bahrain-becomes-routine-with-help-from-nokia-siemens-networking.html

¹⁹ www.alwasatnews.com/2323/news/read/33266/1.html

²⁰ bahrainonline.org/showthread.php?t=258985

²¹ bahrainonline.org/showthread.php?t=259468

²² bahrainonline.org/showthread.php?t=259370

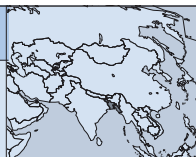
²³ Doward, J. (2013, May 12). UK company's spyware 'used against Bahrain activist', court papers claim. *The Guardian*.

²⁴ <https://bahrainwatch.org/ipspy>

¹¹ <https://www.youtube.com/watch?v=-GrIFni74hw>

BANGLADESH

Online spaces, privacy and surveillance in Bangladesh



Bytes for All Bangladesh

Partha Sarker and Munir Hasan
www.bytesforall.org

Introduction

“In enabling the creation of various opportunities for communication and information-sharing, the Internet has also facilitated the development of large amounts of transactional data by and about individuals. This information, known as communications data or metadata, includes personal information on individuals, their location and online activities, and logs and related information about the e-mails and messages they send or receive.” This communications data is “storable, accessible and searchable,” and when it is combined and aggregated and used by the state, it can be “both highly revelatory and invasive.”¹

Ever since electronic media were opened to private sector involvement in the early 1990s, successive Bangladeshi governments have encouraged the development of an open internet access and communication regime in the country. Bangladesh currently has 33 million internet users, representing almost 20% of the total population, and ranks 138th out of 190 countries in the Household Download Index compiled by Net Index.² The World Economic Forum’s 2013 Global Information Technology Report³ ranked Bangladesh 114th out of 144 countries worldwide, with poor scores for its infrastructure and regulatory environment, even though an affordable and competitive communication service is generating exponential growth for users. In addition, localisation and the availability of phonetic Bangla software have contributed to the development of local blog and content hosting services.⁴

The current government in Bangladesh has a plan to establish what it calls a “Digital Bangladesh by 2021”, with the aim of integrating internet access with development efforts in various sectors.

But with widespread digital communication comes a greater threat to security and privacy, and uncertainty on how state and other institutions will address those issues while protecting the rights of individuals.

Globally there are two models available to protect citizens. One is the authoritarian model, where the problem is addressed through the development of a surveillance regime with filtering at the control points or on the backbone of the internet, and monitoring of the use of computers. A more liberal approach, on the other hand, is to make people aware of the risks, to develop their capacities and to set down punitive measures that require proper evidence and respect individual rights.⁵ Bangladesh is often swinging between these two models, and there is a sense in which it is addressing the situation on an *ad hoc* basis.

Policy and political background

Communication content can reveal a range of sensitive information about an individual, including a person’s identity, behaviour, associations, physical and medical data, race, colour, sexual orientation, national origins and viewpoints. Or it can show trends in a person’s location, movements, interaction or behaviour patterns over a period of time through metadata or other forms of data associated with the original content. Therefore, this requires significant protection in law.

Internationally, regulations concerning government surveillance of communications vary in approach and effectiveness, often with very weak or non-existent legal safeguards.⁶ The Constitution of Bangladesh touches on the issues of privacy and individual security in several places. Article 11

says that the republic shall be a democracy in which fundamental human rights and freedoms and respect for the dignity and worth of humans shall be guaranteed. Article 43 states that every citizen has the right to be secured in his or her home against entry, search and seizure, and the right to the privacy of his or her correspondence and other means of communication, unless there are any reasonable restrictions imposed by law in the interests of the security of the state.

In Bangladesh cyber crime is addressed with reference to several laws, including the Information and Communication Technology Act, 2006; the Penal Code, 1860; the Pornography Act, 2012; and the Bangladesh Telecommunication Act, 2001.

The Bangladesh Telecommunication (Amendment) Act, 2006, allows agencies to monitor the private communications of people with the permission of the chief executive of the Ministry of Home Affairs, under a special provision for the security of state and public order. This act was again amended in 2010, enabling officials to intercept the electronic communications of any individual or institution in order to ensure the security of the state or public order.⁷

The act was further amended in 2013 by granting law enforcers the right to arrest any person without warrant, and by making the crimes non-bailable. Section 57 of the ordinance states that if any electronically published material causes any deterioration of law and order, tarnishes the image of a person or the state, or hurts the religious sentiment of people, then the offender will be punished for a maximum of 14 years imprisonment.⁸

The Bangladesh Telecom Regulatory Commission (BTRC) also has the authority to tap and monitor phone calls if deemed necessary. The commission’s International Long Distance Telecommunications System Policy⁹ has enabled the country to set up three private international gateways, six interconnection exchanges and one international internet gateway. This policy says the operators of these will arrange the connection, equipment and software needed for online and offline monitoring, and will provide access for “lawful interception” by law enforcement agencies. All operators are also required to provide the records of call details (voice and

data) whenever necessary. The BTRC may also set up a monitoring centre at the country’s submarine cable landing station which connects Bangladesh’s internet backbone to the rest of the world.

In January 2012, the BTRC created an 11-member Bangladesh Computer Security Incident Response Team (BD-CSIRT) to look into the issues of cyber crime. This team was mandated to use wiretapping and internet surveillance if necessary. The government has also set up a “cyber tribunal” as per Section 68 of the ICT Act of 2006 to deal with cyber crime-related issues. The Right to Information Ordinance of 2008 was modified and gazetted in 2009. This ordinance has a provision for the proactive disclosure of information ensuring better transparency in the administration, but the amended ICT Act of 2013 may discourage the administration to disclose any information fearing the application of Section 57 of ICT Act.¹⁰

An insight into the chronological events: A saga of lone or dissenting voices

As discussed, the legal framework (such as the ICT Act and its 2006 and 2010 amendments) allows law enforcement agencies to monitor and intercept private communication. Therefore, communication surveillance probably happens at a level we are not aware of. There was a report¹¹ recently that Bangladesh is buying advanced communication surveillance equipment, which certainly validates this supposition. This came out more publicly in 2007 when, in a circular, the BTRC requested all internet service providers (ISPs) to submit the names, addresses, logins, location and other usage statistics of their users.¹² What they did with that information is still unknown. It has been reported that the BTRC often serves informal orders to different domestic service providers to provide information or block certain content – the ISPs are legally bound to do this through their licence and operations agreements with the BTRC.

However, there is the problem of cyber crime too. For example, a number of district web portals that were inaugurated by the prime minister in January 2010 were hacked immediately afterwards.

1 Frank La Rue, the United Nations Special Rapporteur on the promotion and protection of the right to freedom of expression and opinion, in his landmark report on state surveillance and freedom of expression during the 23rd session of the UN Human Rights Council in Geneva in April 2003. www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf

2 www.netindex.com/download/allcountries

3 www.weforum.org/reports/global-information-technology-report-2013

4 Freedom House. (2013). *Freedom on the Net 2013: Bangladesh*. www.freedomhouse.org/report/freedom-net/2013/bangladesh#.U4aWafldXsF

5 Hassan, M. (2012, June 30). Cybercrime: Implementation must to achieve Vision 2021. *The Daily Star*. archive.thedailystar.net/law/2012/06/05/analysis.htm

6 Rodriguez, K. (2013, February 13). Surveillance Camp IV: Disproportionate State Surveillance - A Violation of Privacy. *Electronic Frontier Foundation*. <https://www.eff.org/deeplinks/2013/02/disproportionate-state-surveillance-violation-privacy>

7 Privacy International. (2012). Bangladesh: Legal framework. <https://www.privacyinternational.org/reports/bangladesh/ii-legal-framework>

8 *Daily Star*. (2013, October 9). ICT (Amendment) Act, 2013: Right to Information and Freedom of Expression under Threat. ASK. www.askbd.org/ask/2013/10/09/ict-amendment-act-2013-information-freedom-expression-threat

9 www.btrc.gov.bd/sites/default/files/ildts_policy_2010_english_o.pdf

10 Siddiqui, M. S. (2013, September 29). ICT Act and freedom of expression. *Financial Express*. www.thefinancialexpress-bd.com/old/index.php?ref=MjBfMDI0fMjBfMTNfMV85Ml8xODUxMDM=

11 Privacy International. (2014, May 5). Who is selling surveillance equipment to a notorious Bangladeshi security agency? *IFEX*. www.ifex.org/bangladesh/2014/05/05/security_agency_surveillance

12 Rezwan. (2007, October 5). Internet user profiling and surveillance process initiated in Bangladesh. *Global Voices Advocacy*. advocacy.globalvoicesonline.org/2007/10/05/internet-user-profiling-and-surveillance-process-initiated-in-bangladesh

Different government and media websites, including those of leading newspapers, are attacked quite frequently.¹³

The use of social media is growing exponentially. Facebook, for example, is one of the most visited websites in the country, attracting more than 10% of the nation's total internet users. The platform – or different pages within the platform – has been blocked several times in Bangladesh. In 2013 a Facebook report showed that the Bangladeshi government requested the profile information of 12 users.¹⁴ A newspaper report suggests that the government asked Facebook on three occasions to remove content from its site.¹⁵ Popular video platform YouTube has been blocked repeatedly in recent times. First it was blocked in March 2009 after a recording of a meeting between the prime minister and army officers was published on the site. The block was lifted several days later. YouTube was blocked again in September 2012 following a controversial video clip on Islam – the block was later lifted in June 2013.

Although the reason given for the latter block was that the post hurt religious sentiment, many believe that the actual purpose was to exert more control over online content and behaviour. What was more worrying was the perspective of a Bangladeshi court which expressed the desire to find ways of facilitating future blocks of websites and pages.¹⁶ The court ordered the shutdown of five Facebook pages and a website for content deemed blasphemous towards Islam, while demanding that content hosts and creators be brought to justice for “uploading indecent material.”

Hurting religious sentiment is increasingly becoming a major issue when it comes to surveillance. Authorities seem to be ill prepared, both at the policy and implementation level, to define the issue properly. In October 2012, in the southeastern district of Ramu, temples in Buddhist neighbourhoods were attacked and vandalised following an allegation that the Facebook profile of a Buddhist showed an anti-Islamic image, inciting local Mus-

lims to retaliate.¹⁷ Similarly, in another incident in November 2013, vandals attacked Hindu houses and properties claiming that a local Hindu boy had uploaded something derogatory towards Islam on his Facebook profile, although this was later denied by the person in question.¹⁸

Social media played an important role in mobilising tens of thousands of people who gathered at Shahbagh Square in Dhaka in February 2013. This was in protest against a light court sentence given to Abdul Qader Mollah, an alleged war criminal of the 1971 liberation war. Social, cultural and pro-independence political forces later joined and strengthened the non-violent demonstration, causing some observers to compare it to the 2011 protests in Egypt's Tahrir Square. But, in response, Mollah's supporters rallied against what they called a conspiracy by “atheist bloggers”. On 15 February 2013 armed assailants followed, attacked and killed a blogger, one of the organisers of the Shahbagh demonstration, outside of his home.¹⁹ This shows how people see security threats as linked to online activism, and how surveillance and monitoring are also happening between citizens.

Many argue that the government uses security as an excuse to tame dissenting voices, and Section 57 of the ICT Amendment Act of 2013 gives enough power to the government to arrest and confine anyone without a warrant. Online activists are already finding themselves in an uncomfortable zone regarding the ICT Act amendment, and the ways in which it allows surveillance of communications. In one instance, a professor at a public university was sentenced to a six-month jail term by a court for failing to appear in court (due to the fact that he was in Australia at the time) to stand trial regarding his Facebook statement against the prime minister.²⁰ In another incident, a college student was arrested after posting some “derogatory comments” about the prime minister and her late father, Bangladesh's founding leader, Sheikh Mujibur Rahman. These incidents and the government response created heated debate, both online and offline.²¹

The government, on the other hand, senses a real threat. It cites the example of a failed coup conspiracy in 2012, where a group of ex-military officials used Facebook as the platform to prepare and plan to oust the government.²² No wonder the government's response was to create the BD-CSIPT to identify the websites and persons or institutions that engage in activities that can be seen as harmful to the state, society, political and religious beliefs – whether using mobile phones, a simple website, or social media.²³

Action steps: What's next?

Bangladesh still does not have any proper legal framework to protect privacy and to counteract surveillance. Communication surveillance happens both officially and unofficially without much

challenge. Civil society has a bigger role to play in this context. Civil society organisations can raise awareness among citizens and can push the government to educate and empower people on issues of privacy, cyber crimes, etc. This is preferable to the authoritarian approach of blocking or filtering content, or conducting surveillance. A comparative study on what other countries have done and what they have achieved could be a useful background resource to create this awareness and understanding. Activists can prepare guidelines on user rights and obligations and what can be done if someone feels violated by communication surveillance. Civil society also needs to speak up on the unconstitutional provisions in the ICT Act amendment and other legal provisions that allow surveillance.

13 Freedom House. (2013). Op. cit.

14 Reuters. (2013, August 28). Bangladesh sought data on 12 users: Facebook. *bdnews24.com*. bdnews24.com/bangladesh/2013/08/28/bangladesh-sought-data-on-12-users-facebook

15 *Daily Star*. (2014, April 13). Govt asks Facebook to remove 3 contents. www.thedailystar.net/govt-asks-facebook-to-remove-3-contents-19979

16 Rezwan. (2012, March 24). Bangladesh: Court Orders Shutting Down of Facebook Pages for Blasphemous Contents. *Global Voices*. globalvoicesonline.org/2012/03/24/bangladesh-court-orders-shutting-down-of-facebook-pages-for-blasphemous-contents

17 Freedom House. (2013). Op. cit.

18 Topu, A. H. K. (2013, November 3). Hindus attacked in Pabna. *The Daily Star*. archive.thedailystar.net/beta2/news/hindus-attacked-in-pabna

19 Freedom House. (2013). Op. cit.

20 Samad, S. (2012, January 4). Bangladesh teacher awarded imprisonment for Facebook status. *Bangladesh Watchdog*. bangladeshwatchdog.blogspot.in/2012/01/bangladesh-teacher-awarded-imprisonment.html

21 Ray, A. (2012, February 17). Bangladesh: Government observation of Facebook ignites debate. *Global Voices*. globalvoicesonline.org/2012/02/17/bangladesh-facebook-under-government-scanner-ignites-online-debate

22 BBC News. (2012, January 19). Bangladesh army 'foils coup' against Sheikh Hasina. *BBC News*. www.bbc.co.uk/news/world-asia-16627852

23 Times of India. (2012, January 26). Bangladesh unveils cyber watchdog. *The Times of India*. timesofindia.indiatimes.com/tech/it-services/Bangladesh-unveils-cyber-watchdog/articleshow/11640219.cms

BOLIVIA

Digital violence: Communications surveillance and the protection of privacy on the internet in Bolivia



Fundación REDES

J. Eduardo Rojas
www.fundacionredes.org

A national approach to digital violence

Digital violence¹ is defined here as the exercise of power that violates the human rights of a person or a group of people using new communications technologies. This new concept is harnessed to protect two types of “legal rights”: on the one hand *patrimonial property rights*, namely protection against cyber crime involving technological equipment, databases and the internet’s critical infrastructure; and on the other hand *personal property rights*, which are focused on protecting people’s rights when it comes to technology and databases.

Until now, Bolivia has no record of formal discussions dealing with the mass surveillance of communications and privacy protection. As in many countries, there was media coverage of the WikiLeaks case and Snowden’s whistleblowing against the National Security Agency’s (NSA) espionage. In June 2012,² a number of female members of parliament accused the executive of phone-tapping members of the opposition. However, there is no record that shows that any legal complaint has been filed, or is in process.

The most important initiative on communications surveillance and privacy protection in Bolivia, based on the multi-stakeholder approach, formally got under way during the first half of 2014. Three clearly identified groups of governmental actors promoted the enactment of laws in the Legislative Assembly. These laws touch upon privacy protection and communications surveillance on the internet in an indirect fashion.

a) *Initiatives led by the Ombudsman of Bolivia*, in collaboration with social organisations, promoted the following laws: a comprehensive law

guaranteeing women a life free of violence (Act No. 348; Article 7, paragraphs 4 and 5 refer to media violence); Act 243 against harassment and political violence towards women (Article 8, paragraph N, speaks about the disclosure of the personal information of women politicians).

b) *Initiatives led by the Ministry of Government* in collaboration with stakeholders, including the Ombudsman. Two laws were passed: a law on public security and a national system for a safer life. Act No. 264, Chapter IV, Articles 47 to 52, amongst other things, regulate the installation of surveillance cameras and set out agreements with internet service providers (ISPs) on the use of information technologies when it comes to public safety issues. Furthermore, Act 263, the law against human trafficking, in Article 323 deals with the production, consumption and possession of child pornography. Article 41 explicitly refers to telephone tapping, under a court order.

c) *Initiatives led by the Telecommunications Regulatory Authority*, which, since June 2014, organised a National Campaign to Prevent Digital Violence in Bolivia.³ The main expected outcome of the campaign is the enactment of a bill on prevention of digital violence in Bolivia, developed through a multi-stakeholder approach.

All three groups of stakeholders expressly requested advice from the REDES Foundation to understand and address digital violence. Firstly, between 2012 and 2014, the Ombudsman’s Office requested training for civil society actors, national police, government ministries, the Ministry of Justice and the Public Prosecutor. This involved capacity building to fight human trafficking and protect victims, using new technologies. They also requested the training of more than 16 actors who are part of the National Roundtable Against School Violence.

Secondly, between late 2013 and mid-2014, the Ministry of Interior, through the National Directorate Against Human Trafficking and the National Department of Public Safety (in charge of the installation

of surveillance cameras throughout the country) requested technical support. This was to ensure the fulfillment of people’s rights in the formulation of laws and regulations related to monitoring and the protection of privacy in police investigations, and the eradication of human trafficking networks.

Finally, the third group asked the REDES Foundation in May 2014 for technical assistance in order to develop a national campaign to prevent digital violence called *No caigas en la red* (“Don’t fall into the web”). This has been implemented at a national level since 12 August 2014. The main result of this campaign, apart from building awareness, will be the formulation of a bill on the prevention of digital violence in Bolivia, which will also address the needs of the two previous groups.

Raising awareness amongst national authorities

It is important to highlight that the actors involved in the current processes (regarding the rules that will allow monitoring of internet communications) are uninformed about the internet governance model.

The publication of specialised material on internet governance

Since 2010, the REDES Foundation has promoted awareness of the internet governance paradigm through the publication of the following material:

- *A Map of Internet Governance*, created by the DIPLO Foundation with the financial support of the vice-presidency and the REDES Foundation.
- *The Internet Ecosystem*, authored by the Internet Society with the financial support of the vice-presidency and the REDES Foundation.
- *Transition from IPV4 to IPV6*, authored by LAC-NIC with the financial support of the REDES Foundation.
- *Human Rights on the Internet*, authored by the Association for Progressive Communications (APC), with financial support from the National ICT Network and the REDES Foundation.

This material is currently being used to create awareness in the government, the private sector, international cooperation agencies and general users (including parents) interested in the eradication of internet violence.

High-level meetings on the principles of internet governance

We held workshops and conferences with the following high-level authorities:

- Representatives of the Ombudsman Special Affairs Department, following an agreement signed between this institution and the REDES Foundation in 2012.
- Members of the National Committee for Awareness of School Violence, in 2012.
- Members of the National Committee against Human Trafficking, in 2013 and 2014. This included holding conferences and workshops concerning the recruitment of victims and prosecution of internet crimes against children, using new technologies.
- The municipal governments of La Paz, Santa Cruz and Cochabamba, in 2014. This involved holding conferences and workshops on the prevention of digital violence against children and teenagers.
- The National Director of the Anti-Trafficking in Persons Unit, in May and July 2014. This involved holding meetings about the design of a bill to control internet content. These are considered historic meetings, due to the fact that authorities gained knowledge about net neutrality, internet governance, self-regulation, human rights on the internet, respect for privacy, and the sanctity of communications. Furthermore, they gained knowledge about the nature of international efforts on internet self-regulation and global progress regarding freedom of expression over the internet.
- The Telecommunications and Transportation Authority (ATT), to deal with cases of digital violence, between late 2013 and 2014. The meetings addressed cases of digital violence, with a focus on the importance of aligning the new telecommunications regulations with the self-regulation and internet governance approach.

Two approaches to build regulations related to communications surveillance in Bolivia

Since 2010, there has been a diversity of legal instruments regarding public violence and public security, which tackle communications monitoring. Two approaches can be clearly identified:

Legislation on national security, public safety and child protection: Initiatives on this matter are discussed above in this report. They deal with actions to penalise and punish different crimes involving public security and the criminalisation of violence against women and children. This involves taking into account the dissemination of content in traditional media and on the internet, but the approach is not directly related to the internet, and clearly lacks the inclusion of internet governance and human rights principles affecting the web.

¹ Since 2010, the REDES Foundation has published research on “Towards a transdisciplinary approach to information society violence” in order to categorise online violence using new technologies in Bolivia, including mass communications surveillance and the violation of privacy on the internet.

² www.la-razon.com/index.php?url=/suplementos/la_gaceta_juridica/Derecho-intimidad-privacidad-Constitucion_o_1627037350.html

³ The Telecommunications and Transport Authority (ATT) explicitly adopted the categorisation developed by the REDES Foundation in December 2013.

Legislation on the prevention of digital violence: This process, led by the Telecommunications Authority, formally began in 2014 with technical assistance from the REDES Foundation. Its approach is to bring the actors and initiatives mentioned above in this report together. It also raises the issue of digital violence in the internet governance context. The authority has instructed the REDES Foundation to develop the bill considering the new paradigm of internet self-regulation.

Action steps: A bill to prevent digital violence and address mass surveillance of internet communications

Between August and November 2014 we will design the Law for the Prevention of Digital Violence in Bolivia. It is important to highlight the preventive approach we are using, to open a new era of internet-related legislation we call “regulation ex-ante” (i.e. before unlawful acts occur). It also increases the responsibility of actors in the internet ecosystem regarding the prevention and eradication of different forms of internet violence, including mass surveillance and the violation of privacy.

Preventing digital violence involves three major categories of actors:

- *Cases of digital violence by the state:* These include cases of digital surveillance, spying and harassment within the state apparatus, by the state on companies, and by the state on citizens.
- *Cases of digital violence by companies:* These include cases of digital surveillance, spying and harassment within companies, actions by companies that affect the state, and actions by companies that affect citizens/users of digital communications services.
- *Cases of digital violence by people:* These include cases of digital surveillance, spying and harassment by organised criminal groups on ordinary people, and cases of violence between individuals (bullying, coercion, mail and wire fraud, child pornography, password theft, impersonation and identity theft, plagiarism, etc.).

Preventing digital violence requires multi-sectoral coordination between government actors, namely the Ministry of Interior, the Vice-Ministry of Telecommunications, the Telecommunications and Transportation Authority, the Vice-Presidency of the State, the Agency for the Development of the Information Society in Bolivia, the Ministry of Education, the Ministry of Communication, and municipal governments. They protect human rights on the internet and prevent all forms of violence online, including through respect for privacy and the requirement of

a court order for surveillance of communications, and through always respecting what is stated in the constitution.

When it comes to civil society, key actors are the Ombudsman of Bolivia, the National ICT Network of Bolivia, the REDES Foundation, parents’ associations, and the internet and mobile phone users’ associations. They all protect privacy, freedom of expression and the responsible use of the internet among users of value-added services. They promote the creation of a responsible digital culture and freedom of speech on the web.

Internet service providers (ISPs) and mobile services in Bolivia, including companies like ENTEL, Viva and Tigo, need to work in coordination with the regulator and receive technical support from the REDES Foundation. This area of work involves ensuring network neutrality, communications privacy, and the impartiality of ISPs and mobile communications companies. It also involves consumer protection and the preservation of the multi-stakeholder business model.

Addressing the monitoring of communications and the protection of privacy is currently moving forward in Bolivia under the larger umbrella of digital violence. This approach allows us to unite scattered initiatives, and to promote communications monitoring on the grounds of public security, state security and child protection.

The categorisation of digital violence committed by states, companies and individuals allows us to organise and coordinate the national regulatory framework in line with the constitution, which protects privacy and freedom of expression. It also allows us to contextualise this debate within the paradigm of internet governance and the need to develop a new preventive law drawing on the multi-stakeholder model.

Developing a digital violence prevention bill allows delegating new functions and responsibilities to all actors that are part of the internet ecosystem, including government actors, private users, civil society, international cooperation agencies and the technical community.

Bolivia is facing a new opportunity to develop bills under the paradigm of “ex-ante regulation” and to develop co-responsibility between all actors under the model of self-regulation. The challenge is out there, and it is a civil society actor that is providing technical assistance to guarantee an approach that ensures that no arbitrary action is taken against internet or mobile phone users in Bolivia.

BOSNIA AND HERZEGOVINA

The continuum of surveillance in Bosnia and Herzegovina



OneWorld Platform for Southeast Europe (OWPSEE) Foundation

Valentina Pellizzer and Aida Mahmutovic
www.oneworldsee.org

Introduction

Dissent has its grounding in the understanding of individuals, groups or communities about their entitlement to rights. When it comes to privacy, security, and the internet in general, citizens in Bosnia and Herzegovina are still far from considering themselves entitled to rights. Yet like anyone else in the world they actively use technology and social media to get informed and communicate with friends.

Activists use the internet and in particular social networks such as Facebook to engage the general public and to organise protests against the political establishment. For many who do not know much about Bosnia and Herzegovina, the immediate association is with the Balkans War of the 1990s and the fall of Yugoslavia. For human rights activists, Bosnia and Herzegovina holds the title of the most corrupt country in the western Balkans. It is also the only country in the region which still has to sign the pre-accession agreement to the European Union due to a stalemate on constitutional reform and the unwillingness of its politicians to negotiate necessary cross-party agreements and to go beyond rigid ethnic quotas. A good example of this situation is the country’s failure to comply with the anti-discrimination decision of the European Court of Human Rights in the case of Sejdic-Finci¹ regarding his eligibility for official posts. This meant five years of deadlock on constitutional reforms, and left citizens of Bosnia and Herzegovina trapped in the narrow and discriminatory framework of the Dayton Peace Agreement.²

Policy and political background

The primary purpose of the Bosnia and Herzegovina legislative and administrative system is to enforce

the rigid ethnic divisions in the country set up by the Dayton Peace Agreement, rather than developing policies and laws which respond to the needs of the country and its people. This ethnic structure constantly traps any new policy, law or decision that needs to be taken or developed in futile disputes about jurisdiction among the existing 14 governmental or legislative levels: the state, two entities, one district and ten cantons.

The agency for the information society was supposed to be the state’s concrete mechanism for developing, coordinating and overseeing the information and communications technology (ICT) sector, as described in policy and strategy documents signed by the Council of Ministries in 2004. But this never happened, with the effect that the sector lacks a serious and consistent development strategy.

Dependent on a plethora of bodies and authorities whose mandates are often not understood, citizens struggle to believe in or even follow the work they do, and very often remain passive spectators of violations.

The bodies with competences on security, privacy and surveillance at state level are the Personal Data Protection Agency (AZLP, *Agencija za zaštitu ličnih podataka u Bosni i Hercegovini*);³ the Agency for Identification Documents, Registers and Data Exchange (IDDEEA, *Agencija za identifikacione dokumente, evidenciju i razmjenu podataka*); the Ministry of Security; the sector for combating terrorism, organised crime, corruption, war crimes and misuse of narcotics; the sector for IT and telecommunication systems; the entity ministries of interior and the Brcko district; police apparatuses at entity and cantonal level; and the judiciary. In 2008 the Republic of Srpska created its own agency for the information society to act as a central body for policy and regulation on ICTs and the internet.

From wiretapping to the internet: Someone is listening to us...

When we started to research the right to privacy and surveillance in Bosnia and Herzegovina, we suddenly realised how short our memory sometimes

¹ Wakelin, E. (2012, October 31). The Sejdic and Finci Case: More Than Just a Human Rights Issue? *E-International Relations*. www.e-ir.info/2012/10/31/the-sejdic-and-finci-case-more-than-just-a-human-rights-issue-for-bosnia-and-herzegovina

² The General Framework Agreement for Peace in Bosnia and Herzegovina, 1995. www.ohr.int/dpa/default.asp?content_id=380

³ www.azlp.gov.ba/o_agenciji/nadleznosti/default.aspx

is. We immediately came across dozens of articles on wiretapping and illegal interception by various intelligence agencies, among others.

We suddenly realised that privacy in Bosnia and Herzegovina is more threatened than we thought, and that the internet simply serves as a new way in which information can be obtained, in violation of privacy rights. When talking to civil society representatives and participants in workshops on online safety for youth and women, their answers confirmed the assumption that there is almost a non-existent level of awareness on the right to privacy and information amongst the average citizen.

In 2011 *Nezavisne Novine*,⁴ a daily newspaper from Republic of Srpska published a list with more than 5,000 phone numbers under surveillance by the security intelligence agency OSA and the State Agency for Investigation and Protection (SIPA). Among people wiretapped from 2008 to 2010 were security experts, lawyers and representatives from the civil society sector. The newspaper at the time defined this as a cancer that started in Sarajevo, and spread to the rest of the country. It also accused the international community of being involved. Journalists were also reporting that Bosnia and Herzegovina intelligence was targeting international diplomats, and that in 2009 during his visit to the country, the director of the US Federal Bureau of Investigation (FBI) had asked that top officials from the Ministry of Security be dismissed.

In 2013 Zoran Čegar, chief of the police intelligence department in Bosnia and Herzegovina, admitted that the online communications of thousands of citizens, among them politicians, their wives and lovers, were intercepted with the purpose of blackmailing them. In both cases the public was not informed of any action taken, whether arrests or sanctions.

In March 2014 new leaks on the illegal interception of communications and wiretapping of journalists at the newspaper *Oslobodjenje* and the weekly paper *Bosni Hercegovina Dani* emerged. Excerpts from conversations between Zivko Budimir, president of the Federation of Bosnia and Herzegovina and Avdo Avdic, editor-in-chief of Federal Television, appeared on the internet. Vesna Budimir, the deputy state prosecutor and a candidate for appointment to the Supreme Court, also informed prosecutors that his communications had been illegally monitored and intercepted.

There is a pattern to all these scandals: the existence of parallel systems for intelligence structures that control legitimate security institutions – the result of former war intelligence agencies that never quite went away, and were not brought under the control of the new system.

Regardless how many reforms and new bodies are created, the constant practice of spying on people survives, and the authorities – as well as other interest groups – access the data held by public assets such as telecoms providers without court orders. Eavesdropping appears to be routine, which gives political leaders and their parties material for blackmailing and intimidating rival politicians, their partners and journalists. As Petar Kovacevic, director of the Agency for Personal Data Protection, said in an interview: “In 2007 the Council of Ministers formed a Joint Committee for the lawful interception of telecommunications, which has the authority to adopt procedures that govern the operation of telecoms operators.” In this way it annuls the power of the Agency. It is important to know that the current chairperson of this committee is the deputy minister of security. When, in 2013, the agency checked on the three telecoms operators (BH Telekom d.d. Sarajevo, Telekom Srpske a.d. Banja Luka, and JP Hrvatske Telekomunikacije d.d. Mostar), to verify the lawfulness of personal data processing, and to understand if interception was taking place using court orders, the operators simply did not allow access to documents, claiming that they were “confidential”. As a result the agency could not determine anything.

Personal data protection can easily be considered by many as irrelevant to public interest and reserved for police investigation. This was the case this year during riots and protests in Sarajevo (February 2014) where media footage and video footage from CCTV cameras was acquired by police authorities in order to identify people suspected of having caused damage to public property, and who were accused of “terrorism”. Yet personal data protection all of a sudden became an inviolable human right when citizens asked to access and use the same CCTV footage to identify a court police driver who hit a protestor. Privacy rights are also being used as a way to avoid answering requests based on the access to information act, and to not provide information to investigative journalists or citizens regarding the salaries of public officers, among other things. As confirmed by the Agency for Personal Data Protection’s report: “It is not rare that public administrative bodies use personal data protection or decisions by the Agency to hinder access

to information to which citizens have a right, or to cover up certain irregularities in their work.”⁵

Since existing legislation is not in line with European standards, authorities can easily find excuses to maintain the status quo.⁶ In particular, the Law on Communications does not follow European standards because parliament failed to approve the amendments proposed in 2010. Other relevant laws are the Law on Personal Data Protection, already mentioned; the Law on the Protection of Secret State Information; a set of related provisions in the four existing criminal codes; and laws on criminal procedure, which all define the crime of unlawfully processing personal data.

Since public statements on transparency remain on paper rather than in practice, the role and work of the Agency for Personal Data Protection becomes essential, not only to establish the rule of law, but also to provide citizens with an independent body that they can turn to.

Citizens who have asked the agency to intervene have won all five cases of video surveillance against the Federation Ministry of Veterans and People Disabled in the Defence and Liberation War, the Federation Ministry of Finance, an elementary music school in Ilidza, the Golden Grain Bakery in Bratunac, G-Petrol Ltd. in Sarajevo, and a residential building at 17 Armije Street in Tuzla. The rationale in all cases was almost the same: video surveillance was being used against its declared function of securing property, and used instead as a means of intimidation, blackmailing and controlling employees. In the case of the music school, the headmaster allowed footage of the teachers’ staff room to be uploaded to YouTube, and then used the ensuing scandal to dismiss a disobedient teacher who had been videotaped. The agency’s decision was that people clearly need to know when areas are under surveillance, and who to contact for information regarding video surveillance. Video surveillance installed without knowing to whom it belongs, who can see the recordings, or who can hand these recordings to third parties, is unacceptable.

⁵ Report by the Agency for Personal Data Protection, 2013.

⁶ The Report states: “The rules of the Council of Ministers about the participation of the Agency for Personal Data Protection in relevant legislative processes are not satisfactory. The principle of purposeful use and by-laws regulating the protection of personal data by the police have still not been fully implemented. The Law on Personal Data Protection does not apply to the Bosnia and Herzegovina Intelligence and Security Agency. Overall, preparations for personal data protection are still at an early stage. It is necessary to ensure the independence of the Agency for Personal Data Protection.” European Commission Progress Report in Bosnia and Herzegovina, 2012.

Conclusions

Over the years politicians have continued to use whatever a system allows to suit their own particular purposes. Ministries have changed, heads of security agencies and the police have been replaced, but the same scenario plays out with new people under surveillance, the same scandals but different names – and no solutions. The Agency for Personal Data Protection has introduced a new concept to authorities and even if it is fragile, it is trying to establish its reputation on new ground. In a closed system such as the one in Bosnia and Herzegovina, it is really important to refer substantially to legality, adequacy and proportionality, and introduce the concept of user notification.

Bosnia and Herzegovina, similar to all new democracies, has wonderful copy-and-paste laws in place, but they are mostly never implemented. The real power remains outside institutions, while rhetoric is used during official visits and good-sounding statements are produced easily. The participation of Bosnia and Herzegovina as a state in the global conversation around internet rights is non-existent, and security is understood in a very conservative way. The first action plan for children’s online safety is a perfect example, with a blacklist, measures for parental control, internet service provider (ISP) responsibility and other conservative measures.

Traditional actors seem not to grasp the urgency and the necessity of moving beyond the usual scheme of endangered human rights. Technology and the regulation of telecoms remain a distant world approached only in terms of the potential for corruption, and privatisation.

There is a world of non-traditional activism that is represented by internet users which can recognise the connection between technology, online platforms and tools, and the policy and legislation surrounding them. This is unique.

Action steps

Participatory awareness campaigns that use visual tools are key to helping citizens value their personal information and data and to pressurise institutions to fulfil their role when it comes to privacy rights. Since its inception, the Agency for Personal Data Protection has slowly been receiving more expert input and extended its controls over institutional decisions. There is still a need to build a bridge between the work of the agency and the average citizen and to translate the complexity of personal data processing into personal stories.

Public opinion in Bosnia and Herzegovina had become so disillusioned about its ability to bring

⁴ A. Ducic, Telekomski kriju podatke o prislusu353\61kivanju, Dnevni Avaz, 2014. www.avaz.ba/vijesti/teme/telekomski-kriju-podatke-o-prisluskivanju


about change. The silent majority is afraid to take risks, because it would be defending something it does not really understand, or is genuinely scared about the repercussions. In this as in other issues, it is important to leave behind the feeling of an overwhelming and invincible Big Brother that can see and control everything. To do this it is important to talk outside of the usual circles of activists, and also to produce and distribute information in a format that citizens can understand and use.

The internet has proved to be a space where people convene and take action in creative and

personal ways, and more than ever has become the place where actions start: content is easily distributed and memes are generated. With a mobile phone penetration rate of 90.8%, an internet penetration of 56.96%, and a total of 2,188,429 internet users in 2013, this is the place where ongoing awareness campaigns can generate *ad hoc* coalitions ready to take up the challenge of creating a positive sense of privacy. This can help build campaigns against the continuum of surveillance and its pervasive expansion under the paternalistic vest of protecting vulnerable communities.

BRAZIL

Marco Civil: A Brazilian reaction to surveillance on the internet



Brazilian Institute for Consumer Defense (Idec)
Veridiana Alimonti
www.idec.org.br

Bill No. 2126/2011 in Brazil, known as the Brazilian Civil Rights Framework for the Internet (in Portuguese: *Marco Civil da Internet*), was finally passed by the Brazilian Senate on 22 April 2014, and sanctioned the following day by President Dilma Rousseff at the opening ceremony of NETmundial.¹ With this, the bill became Federal Law No. 12965/2014, which is the result of widespread mobilisation by civil society searching for a guarantee on internet rights – a mobilisation which resulted in an innovative participatory movement in the Brazilian law-making process.

The three key pillars of the Marco Civil– net neutrality, intermediary liability aligned with freedom of expression, and data protection and privacy – encouraged people to link themselves to the mobilisation campaign and overcome great resistance in the National Congress of Brazil. The purpose of this report is to highlight the relevant points in the process of preparation and approval of the law, as well as to discuss the rules related to the three pillars, while emphasising data protection and privacy. A description of the main challenges to be faced after the approval of the law is also provided at the end of the report.

A bill of rights for the internet with civil society playing a leading role

The idea of a civil rights framework (“Marco Civil”) for the internet in Brazil gained momentum in the context of society’s reaction against regulation of the net focused on the persecution and punishment of its users. Bill No. 84/99, debated for almost 10 years in the National Congress, channelled much of this opposition when it was returned from the Senate to the Chamber of Deputies because it proposed very restrictive regulations.² Activists and civil so-

ciety organisations joined in a broad online and offline campaign³ that attacked the bill and its conception of net regulation, placing pressure on the president then in office, Luiz Inácio “Lula” da Silva, and changing the approach of the federal government on the subject.

In the absence of any other relevant legal framework, the Brazilian legal system considers criminal law the last resort in the regulation of conduct. Civil society further consolidated the idea that before cyber crimes can be legislated, it is necessary to guarantee rights and define liabilities on the net. A civil rights framework was necessary for the internet in Brazil. The federal government took over the project and, in partnership with the Center for Technology and Society of the Law School at the Fundação Getúlio Vargas (CTS/FGV), conducted an online public consultation in two phases.

The public consultations occurred between 2009 and 2010 and resulted in approximately 2,000 comments from many different sectors. In both phases a participatory online platform was used, allowing views and comments on the contributions already received. One of the important references in the draft of the text was the Internet Governance and Use Principles, established by a resolution of the Brazilian Internet Steering Committee (CGI.br). After the public consultation, the wording of the bill was concluded by the executive branch and it was sent to the Chamber of Deputies, the lower house of Congress, in 2011. Brazil at the time was already under President Dilma Rousseff.

A special committee was created to discuss the bill, and Congressman Alessandro Molon was appointed as rapporteur. He held a series of public hearings and seminars, as well as a fresh round of online public consultations.

From July 2012 the report was ready to be voted on by the Chamber of Deputies, but there were many pressures that led to repeated delays. The strongest came from telecommunications companies, but negotiations were also necessary when it came to the issue of copyright with Rede Globo, a powerful media group in Brazil, and with sectors engaged in the fight against cyber crime regarding

1 The Global Multistakeholder Meeting on the Future of Internet Governance, held on 23-24 April in Brazil. www.netmundial.br

2 See more about Bill No. 84/99 and the beginning of the Marco Civil at Pereira, C., Maciel, M., & Francisco. P. (2011). Marco Civil da Internet: uma questão de princípio. *Revista poliTICS*. https://www.politics.org.br/sites/default/files/poliTICS_no7_souza_maciel_francisco.pdf

3 The campaign was known on the net as Mega No (“Mega Não”).

the matter of the retention of log files. Edward Snowden's espionage claims directly involving the Brazilian government, in the second half of 2013, brought Rousseff into the discussion, and pulled the Marco Civil back onto the legislative agenda.

The executive branch determined discussion of the bill in Congress to be of “constitutional urgency”, and it came to lock the agenda of votes in the lower house on 28 October 2013 (in line with the Brazilian constitution, if a bill granted “urgency” has not been voted on within 45 days, deliberation on all other legislative matters is suspended in that house of Congress until voting is concluded). Nevertheless, resistance, a congressional recess and political manoeuvring delayed its approval for almost five more months – until it was finally approved on 25 March 2014. In the Senate, the pressure for approval, the proximity of the NETmundial event, and a composition of senators more favourable to the government helped the voting to take less than one month. Through all this, mobilisation of civil society through online campaigns, messages being sent to members of Congress, increased public awareness through social media networks, public events and lectures, and the physical presence of activists in the halls and plenary sessions of the National Congress, were fundamental.⁴

Data protection and privacy: One of the pillars of the Marco Civil

Privacy protection and personal data protection are, separately, two of the principles provided for by law to regulate the use of the internet in Brazil (in Article 3). The clauses in the Marco Civil dealing with these protections were strengthened after Edward Snowden's public allegations of mass surveillance, and an important set of such provisions are set forth in Article 7 of the law. Such provisions ensure the inviolability and secrecy of the flow of communications on the internet and of stored private data, except if disclosure is required by court order. The inviolability and secrecy of data and communications are rights guaranteed under the Brazilian Federal Constitution, but the judiciary understands that such provisions are only applicable to the flow of communications, not to communications that are stored. The Marco Civil represents a breakthrough in the protection of stored data.

Another advance concerns the more detailed provision of the law that requires express (not implied) consent from the subject for the future collection, use, storage and handling of personal data, which should be given separately from any other contractual clauses. In addition, the user must have access to clear and complete information about the processes of storage, including the system of protection of connectivity logs and data recording access to applications. The disclosure of personal data to third parties may only occur if there is express consent, informed and free. Subject to the principle of purpose, the same article provides that personal data may only be used for purposes that justify their collection, when not prohibited by law, and are specified in the services agreement or the terms of use of internet applications.

As a corollary to Article 7, Article 8 of the Marco Civil states that the guarantee of the right to privacy and freedom of expression in communications is a prerequisite for the full exercise of the right to access the internet. Accordingly, any contractual clause in breach of these provisions, such as those involving harm to the inviolability and privacy of communications on the internet, will be considered null and void.

In order to fight the surveillance reported by Snowden, Article 11 determines that Brazilian law related to privacy must be respected by internet connectivity and applications providers when collecting personal data, logs and communications content when this occurs in the country or involves a terminal located in Brazil. This obligation also applies to legal entities domiciled abroad, provided that they offer services to the Brazilian public or that any member of their business group has a business unit in the country.

Part of the law is also aimed at establishing parameters for the retention and availability of logs for connectivity and access to applications. Generally, the obligation to make these logs available depends on a court order. As regards retention, the Marco Civil provides for two cases in which it can occur. The first, in Article 13, refers to connectivity logs (date and time of beginning and end of a connection, its duration and the IP address). The system administrator must keep them private, and in a controlled and safe environment, for a period of one year, according to the regulations. The second, in Article 15, refers to logs of access to applications (date and time of use of an application from a particular IP address). In the case of applications whose providers are legal for-profit entities, the retention of these logs shall be compulsory for six months, also pursuant to the regulations.

Initially provided for as optional, the compulsory character of the retention was a late change to the bill, the result of pressure from the federal police and related sectors, causing great controversy among civil society organisations. Finally, it is important to mention that connectivity providers are prohibited from storing access to applications logs, and may not store these together with connectivity logs.

The provisions commented on here do not comprise all the Marco Civil rules applicable to privacy and personal data, but represent many of them.⁵ There are also two other pillars of the law that are worth noting.

One is net neutrality, which is guaranteed as one of the principles governing the use of the internet in Brazil. In order to give effect to it, Article 9 establishes that the entity responsible for transmission, switching or routing must treat any data packs equally, irrespective of content, origin and destination, service, terminal or application. The article also forbids these entities from blocking, monitoring, filtering or analysing the contents of the data packs. Two exceptions are provided, and these may result in discrimination or the degradation of data traffic: i) due to technical requirements necessary for the adequate supply of services and applications, and ii) for prioritising emergency services. Even in these cases, there are conditions that providers must meet, such as refraining from doing harm to users and not engaging in anti-competitive conduct. Exceptions will be regulated by presidential decree, after input from the National Telecommunications Agency and CGI.br. While telecommunications companies have managed to include the principle that grants “freedom of business models” among the principles of law, it is the only clause which includes the phrase “provided they do not conflict with other principles under this law” – including net neutrality, detailed in Article 9.

Another important pillar is the issue of intermediary liability with respect to third-party content. According to the general rule laid down in Article 19 of the law, civil liability for third-party content may only occur if the provider of applications fails to comply with a court order requiring the removal of the content. This provision is to ensure due process, as well as the competent judicial scrutiny on the various rights involved in removal requests. There are, however, two exceptions worth noting. In the case of content protected by copyright, until a specific

provision of law is adopted for the application of this rule, the current Brazilian Copyright Act remains applicable, which allows a much more restrictive approach to access to knowledge. The second exception is the notice and takedown for breaches of privacy by disclosure of nudity or private sexual acts without the consent of the participants. However, the notification must be made by the participant or his/her legal representative, aiming to avoid moralistic and judgmental censorship which is not rare at all on the net.

Action steps

The reaction that initially consolidated the idea of a civil rights framework for the internet in Brazil was strengthened with the release of the documents leaked by Snowden. The idea that the regulation of the internet should move away from a persecutory, surveillance approach in order to guarantee the right to privacy and other rights has been reinforced. However, such a conception of internet regulation cannot settle without considerable difficulties – and the Marco Civil is an expression of this. Despite the mobilisation, civil society was not able to contain the pressure for mandatory retention of logs. However, it did succeed in restricting the time period that logs could be retained – a period shorter than the authorities wanted.

The regulation on the retention of logs, especially logs that record a user's access to applications, may further limit the types of service providers required to retain logs and improve transparency and control mechanisms related to data retention. Moreover, a specific bill on protection of personal data is expected to be sent to the Brazilian Congress soon. This can minimise the problematic aspects of the Marco Civil which, in general terms, introduces important regulations for the protection of user's privacy on the internet into Brazilian legislation. Beyond this point, the law has other important advances, notably the provisions on net neutrality and intermediary liability. In both cases, the guarantee of rights was set against commercial interests and the threat of censorship. In the future, we can expect pressure to continue to build with regard to exceptions to net neutrality, and changes to the Copyright Act, which is also expected to be sent to Congress.

If disputes follow the approval of the Marco Civil, including the challenges surrounding its effectiveness and continuity, it is certain that these disputes will at least begin from an informed perspective. This includes considering the internet as a rights-based issue, essential to the exercise of citizenship, and which requires the guarantee of privacy and freedom of expression.

⁴ Idec made an online tool available that sent thousands of emails to members of the House of Representatives; Avaaz collected 350,000 signatures supporting the Bill through online petitions. Numerous organisations and activists mobilised using these and other tools forming a cohesive and coordinated front. See: marcocivil.org.br

⁵ For further analysis, see Doneda, D. (2014). *Privacy and data protection in the Marco Civil da Internet*. www.privacylatam.com/?p=239; an unofficial translation of the law is available at: theodd.wordpress.com/2014/03/28/marco-civil-da-internet-unofficial-english-translation

BULGARIA

Zigzagging away



BlueLink.net
Pavel Antonov
www.bluelink.net

Introduction

Over 40 representatives of internet service providers (ISPs) gathered on 10 June 2014 in the imposing grey building of Bulgaria's Ministry of Interior (Министерство на вътрешните работи – MVR). The meeting was called by the State Agency of Technical Operations (Държавна агенция „Технически операции“ – DATO) and did not go easy, according to a report by Bulgaria's authoritative business weekly Capital. ISPs were asked to provide DATO and the State Agency for National Security (Държавна агенция „Национална сигурност“ – DАNS) with unlimited real-time access to all internet traffic, with data storing options. Apart from concerns that the cost of equipment and technology necessary for fulfilling such a request might be too high, especially for smaller providers, it raised alarm for at least two more reasons: it confronted recent civil society accomplishments against excessive surveillance in Bulgaria; and the piece of European Union (EU) law that it was legally grounded in had just been abolished by the Union's highest court in Luxembourg.

This report seeks to explain the political and policy context that perpetuates internet surveillance by Bulgaria's security services and averts civil society's efforts to limit them. The following analysis is based on unstructured online interviews and query responses from internet rights activists, ISP proprietors and members of the “Free and Neutral Internet” Bulgarian language group on Facebook¹ during April-May 2014.

Policy and political background

In fact, DATO's surveillance requirements were anything but new. They were added to Bulgaria's Electronic Communications Act (Закон за електронните комуникации – ZES) back in 2010 to comply with the EU's Data Retention Directive 2006/24/EC. The former EU Data Retention Directive was originally transposed into MVR's Ordinance 40 as early as 2008, but its texts

regarding access to stored information were cancelled by Bulgaria's Constitutional Court in 2009 and consecutively added to ZES. Remarkably, Ordinance 40 was never cancelled and is still technically in force, including a requirement for ISPs to send yearly reports to the Minister of Interior.

The ZES surveillance provisions oblige telecommunications operators to ensure real-time possibility for security services to “capture” electronic messages, “monitor” communication continuously, and access “data related to a certain call”. If real-time is not possible, ISPs should provide requested data as soon as possible. They need to also maintain special interfaces that allow the transferring of captured electronic communication to DATO and DАNS, following specifications approved by DATO's chair. ISPs are expected to both provide details about every call and its content, and establish the identity of their users. But no one ever put pressure on ISPs to actually implement these requirements, so they never did – apart from the country's three GSM (mobile) operators, *Capital* reported.²

A separate Special Surveillance Devices Act adopted in 1999 stipulates that surveillance requests can be filed by MVR, DАNS or a prosecutor's office. Then a district judge's approval is required before DATO implements them.

On 8 April 2014 the European Court of Justice invalidated the EU's Data Retention Directive because it contradicts the Union's human rights and personal protection principles.³ But how to comply with the ruling was left up to each member state to decide. And while none of the political parties represented in Bulgaria's parliament have made a move to ease ZES's draconic e-surveillance requirements since April, all of a sudden in June DATO called up ISPs asking them to tighten their implementation.

The “state” of state security

It was not a coincidence that the awkward meeting between ISPs and law enforcement agencies took place in the once notorious building which used to

host the most redoubtable units of the Committee for State Security – Bulgaria's equivalent of the KGB during the authoritarian rule of 1944-1989. Haunted by memories of mass surveillance and terror from these times, Bulgaria's civil society has been alert for over two decades against the activities of the former and present – supposedly reformed – security and enforcement agencies of its democratic government. And for a good reason: the former regime's state security staff, agents and informants have held a tight grasp of Bulgaria's post-socialist politics, governments, business and mass media.⁴ As a result, over the years, the public saw various initiatives fail or get significantly watered down,⁵ while individuals and groups linked to the former state security apparatus almost inevitably held political and economic power.

Instead of getting its security services reformed and accountable, Bulgaria's democratic institutions seemed to be getting subdued and further infiltrated by them, their non-transparent and manipulative methods, and their abusive and controlling culture. The country's late accession to the EU in 2007 did not bring the expected improvements, and progress monitoring reports by the EU indicate systematic problems with the independence of the judiciary and corruption of authorities and law enforcement,⁶ while Freedom House reports reflect a decline in freedom of speech and human rights, among others.⁷

Civil society to the rescue

For a while the third sector compensated to some extent for the decline of democratic institutions. Empowered by the increasing availability of high-speed internet in Bulgaria, social networks like Facebook and Twitter, or local networking sites such as Association for Progressive Communications (APC) member BlueLink.net,⁸ mass protests in 2012 forced Bulgaria to retract from signing

the Anti-Counterfeiting Trade Agreement (ACTA).⁹ Suggestively, its centre-right government at the time was led by Prime Minister Boyko Borissov, who had started his political career as Chief Secretary of MVR and held a police general's rank. In spite of backing off from ACTA, Borissov's government was accused of excessive and often illegitimate use of electronic surveillance.¹⁰ Allegedly, the main illicit surveillance culprit was Borissov's interior minister at the time and trusted in-party ally Tsvetan Tsvetanov. A former Police Academy gymnastics instructor, Tsvetanov was criticised for – and eventually charged with – sanctioning allegedly illicit eavesdropping by security services.¹¹

An escalating row of public protests over a piling number of environmental and social problems eventually forced Borissov's government prematurely out of power in February 2013. Soon after, senior prosecutors investigated MVR to discover a lack of clear rules on the use of surveillance and dereliction of duty by senior officials, and faced obstruction by an official who allegedly destroyed evidence.¹² Already in opposition, Tsvetanov was taken to court on various counts related to the use of surveillance equipment and eavesdropping; final rulings are pending. Raychin Raychev, chair of Future 21 Century Foundation and an internet rights activist based in Plovdiv, found it only natural that the internet and other surveillance peaked during the rule of Borissov. He blamed the phenomenon on the mentality and origin of key government figures and Borissov himself; then their snobbishness and eagerness to show off.

Mounting criticism created an expectation that the government of Bulgaria's Socialist Party and Muslim minority-based Movement for Rights and Freedoms that took power after preliminary elections would significantly tighten up surveillance procedures and decrease surveillance practices. But an analysis by the Sofia City Court released in February revealed a disappointing discovery: phone and internet tapping requests were actually on the rise during the next government's tenure in office.

4 Hristov, H. (2013). Държавна сигурност и влиянието върху политическия елит по време на прехода [State security and its influence over the political elite during the time of transition]. Report presented at the East Europe's Transition in the Documents of Communist Secret Services conference held by the Committee for disclosing and announcing affiliation of Bulgarian citizens to the State Security and Intelligence services of the Bulgarian People's Army, Sofia, Bulgaria, 26 November. www.comdos.bg/media/Novini/Doklad-Hr.Hristov-26-11-2013.doc

5 Ibid.

6 European Commission. (2014, January 22). *Report from the Commission to the European Parliament and the Council: On Progress in Bulgaria under the Co-operation and Verification Mechanism*. ec.europa.eu/cvm/docs/com_2014_36_en.pdf

7 Freedom House. (2014). *Freedom of the Press Report: Bulgaria*. www.freedomhouse.org/country/bulgaria

8 www.bluelink.net

9 Chipeva, N. (2012, February 11). Thousands march in Bulgarian cities against ACTA: Photo gallery. *The Sofia Echo*. sofiaecho.com/2012/02/11/1764539-thousands-march-in-bulgarian-cities-against-acta-photo-gallery

10 Nikolov, K. (2013, April 20). Гарантирано от ГЕРБ: Пълен произвол с подслушването [Guaranteed by GERB: Completely Arbitrary Surveillance]. *Mediapool*. www.mediapool.bg/garantirano-ot-gerb-palen-proizvol-s-podslushvaneto-news205487.html

11 Leviev-Sawyer, C. (2013, April 16). Borissov and GERB back Tsvetanov in eavesdropping controversy. *The Sofia Globe*. sofiaglobe.com/2013/04/16/borissov-and-gerb-back-tsvetanov-in-eavesdropping-controversy

12 Ibid.

1 <https://www.facebook.com/groups/bginternetfreedom>

The Court reported some 8,345 requests for phone and internet traffic surveillance filed during 2013 by the police and DANS, with each request containing tens of phone numbers and IP addresses.¹³ The number appeared to have grown significantly compared to 2011, when the requests were 6,918, although court refusals had also increased from 12% in 2012 to 14.3% in 2013.

The number of cases where law requirements were neglected is on the rise, confirmed Atanas Chobanov, a Paris-based investigative journalist and co-publisher of *BalkanLeaks.eu* and whistleblowing online journal *Bivol.bg*. He sees the genesis of the problem in the fact that the secret services have access to the technical possibilities for surveillance and it is easier for them to use it, in spite of using other methods for investigation which are supposed to be used first. As a WikiLeaks' Bulgarian partner, *Bivol.bg* revealed in 2013 that Bulgaria's government is among the clients of FinSpy – a software product by Dreamlab and Gamma International, specialised for internet and phone surveillance.¹⁴

Internet surveillance is as serious as it was in the beginning of the previous government's term, commented Delian Delchev, a senior networking engineer and IT consultant based in Sofia. Delchev, who is the administrator of the Free and Neutral Internet Bulgarian language group on Facebook, assessed all recent attempts to reform surveillance mechanisms as incomplete, including the separation of DATO from MVR's structure and allowing DANS, the military and customs to request surveillance requests directly. Another reason for concern for Delchev is the political appointment of DATO's chair, whose position is not subject to any public or civic scrutiny and accountability.

The increase in the number of requests was not the only sign of policy zigzagging over e-surveillance. In May 2014 state prosecutors suddenly burst into the offices of DATO and DANS to investigate the legality of their surveillance methods and practices.¹⁵ Just a month later DATO suddenly became eager to get ISPs to fulfil their surveillance obligations under ZES.

Respecting laws and changing laws

In spite of all this most ISPs fulfil their obligations under ZES article 250a consciously and respect the law, said Assen Totin, a former ISP manager, now working for a small telecommunications operator. It is smaller "one-block LAN [network]"-type providers who turn a blind eye to the law, not making any effort to comply with it. "Not because they embrace the European Charter for Human Rights, but because most Bulgarians think that the laws apply for everyone else but them – and it is a pity that no one can bring them back to shape," Totin commented. The EU's Data Retention Directive may be invalidated, but Bulgarian law provisions that comply with it are still valid and no serious operator could unilaterally decide to stop complying with them, Totin explained. Failure to do so might lead to substantial fines of up to USD 68,400 – a serious amount even for large players. Benefits from non-compliance are questionable, with substantial possibilities for negative consequences in terms of bad public relations, said Totin.

But as an industry insider he sees clearly how hard it is for providers to comply with e-surveillance obligations. Larger operators receive some tens of requests for data access every day. Handling them requires a great resource of people, labour and so on, especially given that in order to "cover" a specific subject of "operational interest", much more information is often required than actually needed. For example, instead of simply asking whether X was in area Y at a given point in time, a request arrives that information of all users who appeared in the area should be handed over. And little of the requested information is acceptable as legitimate proof by Bulgarian courts, Totin explained. The Committee for Protection of Personal Data (Комисията за защита на лични данни – KZLD) is the body authorised under ZES to keep track of ISPs' compliance with this part of the law – namely, whether data under article 250a is accessible only for the appropriate persons, whether it is destroyed afterwards and so on. ISPs account in front of KZLD on a yearly basis. Totin thinks that the committee did a lot to make the life of ISPs easier, and listened to most recommendations by larger operators and by the Society of Electronic Communications – one of the professional associations in the sector – particularly with regard to legitimising refusals of access to information whereby a request did not meet the requisites of the law, and also in defending the ISPs' position that they should not interpret the data provided.

A representative of another trade association, the Society of Independent Internet Suppliers, was quoted by *Capital* as saying that DATO's requests

are unconstitutional and in breach of EU law and individual privacy rights, and that ISPs might sue the state in the International Human Rights Court in Strasbourg over them.

As former associate to the Sofia-based Centre for the Study of Democracy, Totin believes that abiding by applicable law is a must in a democratic society, and that there are legitimate ways to change a bad law. A couple of days after the EU court's decision was announced, Totin sent a complaint to the Ombudsman's Office as a private individual, asking him to alert the Constitutional Court. Ombudsman Konstantin Penchev was quick to act and a case is now pending at the Constitutional Court for the cancellation of the ZES requirements affected by the cancelled directive.¹⁶ There is a proposal to get an opinion from the Communications Regulation Committee (Комисия за регулиране на съобщенията – KRS) and all interested parties might send their opinions to them. Eventual success in the Constitutional Court might be of substantial importance for demonstrating the superiority of public interest over applicable law.

Conclusions

For 25 years since 1989, Bulgaria's political and economic landscape remains marked by power structures linked to the security services of the former authoritarian regime. The style and methods of the former state security persist in today's unreformed security and enforcement agencies that tend to practise excessive and often unnecessary internet surveillance. Internet surveillance is over-regulated, with different regulations appearing in various legal texts, and regulated by different bodies. Policy zigzagging and conflicting signals sent by different institutions and politicians – depending if they are in opposition or in power – creates the sense that no significant motivation to limit internet surveillance exists in Bulgaria's governing circles. With business, politics, mass media and justice marked by corruption, non-transparency and lack of public accountability, civil society remains often the most viable guardian of privacy and human rights online. EU institutions, a few independent journalism publications, and the few functioning democratic institutions, such as the Ombudsman, also play their part.

The cancellation of the EU's Data Retention Directive by the European Court of Justice offers Bulgaria and all member states a great opportunity to redesign their national legislations so that internet surveillance

should not hamper fundamental rights of privacy and freedom of expression. But the resistance of conservative structures linked to the state security apparatus slows down and often reverses such changes. A paralysing legal and administrative framework imposes new technological and financial burdens on ISPs who are willing to comply with data retention and surveillance requirements. The idea of refusing to comply with the applicable law's draconian requirement is new to most ISPs, but there is already the thought of legally challenging the obsolete national law provisions. Conscious citizens and internet connectivity proprietors abide by the law, but are willing to take legal action to remove the obsolete legal texts that force them to spy on internet and phone users.

Action steps

Some steps that could lead Bulgaria to resolving the problems with excessive and sometimes illicit internet surveillance include:

- An in-depth assessment of the existing administrative and legal framework to establish all norms and agencies that regulate internet surveillance.
- Conceptualising a complex set of changes that would lead to minimising the number of surveillance requests and strengthening the ability of both special services and ISPs to cooperate effectively.
- Having Ordinance 40 of MVR ultimately cancelled.
- Raising public awareness of the negative implications of excessive internet surveillance and creating political demand for limiting it; limitations that politicians need to comply with when they get elected.
- Building broad coalitions of actors who are interested in limiting internet surveillance, including ISPs, human rights advocates, pro-democracy think tanks and other groups that could participate in decision making when it comes to surveillance.
- Removing the internet surveillance provisions related to the former EU Data Retention Directive from ZES.
- Concentrating efforts on policy advocacy at the EU level to obtain a favourable replacement for the cancelled Data Retention Directive that would have a lasting impact over internet surveillance policies at national and EU level.

¹³ Sofia News Agency. (2014, February 17). Number of Surveillance Requests in Bulgaria on the Rise. *Novinite.com*. www.novinite.com/articles/158260/Number-of-Surveillance-Requests-in-Bulgaria-On-the-Rise

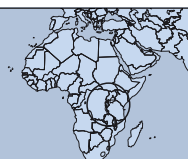
¹⁴ Bivol. (2013, September 4). WIKILEAKS: БЪЛГАРИЯ РЕАЛНО ИЗПОЛЗВА ШПИОНСКИЯ СОФТУЕР FINSPY [WikiLeaks: Bulgaria effectively uses FinSpy spying software]. *Bivol.bg*. <https://bivol.bg/finspy-bulgaria.html>

¹⁵ Angarev, P., & Dachkova, D. (2014, May 16). Прокуратурата изненадващо влезе в спецслужбите заради подслушването [Prosecutors surprisingly entered into special services because of surveillance]. *Sega*. www.segabg.com/article.php?id=698787

¹⁶ Mihaylova, P. (2014, June 20). Op. cit.

BURUNDI AND EAST AFRICA

Government surveillance in East Africa



Collaboration on International ICT Policy in East and Southern Africa (CIPESA)

Lillian Nalwoga
www.cipesa.org

Introduction

Internet access and use of its related technologies continue to grow in East Africa. This can be partly attributed to the undersea cables that established landing sites along the Kenyan and Tanzanian coasts between 2009 and 2010,¹ consequently opening up the region to increased bandwidth and speeds. Other factors include a reduction in access costs and the proliferation of mobile phones.

Currently Kenya leads in internet access with 21.2 million users, or 52.3% of its total population,² compared to 8.67% in 2008,³ while in Tanzania internet users were reported at 9.3 million at the end of 2013⁴ compared to 4.9 million in 2010.⁵ Meanwhile, internet usage also increased in landlocked Uganda, Rwanda and Burundi. By the end of 2013, Uganda's internet penetration stood at 20% compared to 12.5% in 2010, while that of Rwanda currently stands at 19.5%, having doubled from 2010. Meanwhile, Burundi and Ethiopia have the lowest proportion of internet users, at 1.32% and 1.5%⁶ of the population, respectively.

Policy and political background

While East Africa has enjoyed relative stability, there have been cases of unrest in Burundi, Rwanda, Ethiopia, Uganda and Kenya in recent years. Tanzania continues to be the most peaceful country, while Kenya has recently been hit by terror attacks and

earlier in 2007-2008, by election-based violence. The instability which the countries have experienced makes promoting national unity and national security, including fighting terrorism, pertinent concerns in the region. Despite this, the region has recognised that information and communications technologies (ICTs) can be used to advance governance and development. Governments in all these countries have enacted national ICT policies and other legal and regulatory frameworks to further facilitate and foster development in the digital age. Many of them have formed ICT Ministries – although they still make only negligible funding to these ministries and ICT development in general.

Between 2010 and 2014, various laws were introduced and have been criticised for curtailing online freedoms in these countries.⁷ Often guised under the pretext of promoting national security and fighting cyber crime, these laws allow for interception of communications, censorship or the monitoring of online user activity. In many instances, the laws contradict the rights provided for in national constitutions.

All countries in East Africa have legal provisions, reinforced by state agencies, that enable the lawful surveillance and monitoring of communications. These include the Regulation of Interception of Communications Act, 2010 in Uganda; the Rwanda 2013 Interception of Communication Law and 2001 Law Governing Telecommunications; the Kenya Information and Communications (Amendment) Act 2013⁸ and National Intelligence Service Act (Act No. 28 of 2012);⁹ and the Prevention of Terrorism Act, 2002¹⁰ in Tanzania. In Ethiopia, the Telecom Fraud Offence Proclamation No. 761/2012¹¹ allows for state moni-

toring of telecom subscriber information, and two agencies reconstituted in 2013 – the National Intelligence and Security Service (NISS) and Information Network Security Agency (INSA)¹² are actively involved in monitoring citizens' communications.

In Burundi, Article 29 of its 2013 Media Law makes it mandatory for news agencies, including online publications, to disclose certain information to the regulatory body, the National Communication Council (CNC). In Uganda, the Anti-Pornography Act, 2014 and Anti-Homosexuality Act, 2014 have been criticised for placing tough provisions on intermediaries regarding content hosted on their networks. Violators face hefty fines or even risk losing their licences.¹³

Ambiguous laws fuelling digital surveillance in East Africa

Internet rights violations in East Africa can be traced back as early as 2006 when the Ugandan government ordered the blocking of two websites. One of them, www.radiokatwe.com, a political news and commentary website, was accused of publishing anti-government gossip,¹⁴ while the other, www.monitor.co.ug, the online version of the independent newspaper *Daily Monitor*, was temporarily blocked on the eve of the 2006 elections in a bid to stop it from publishing independent polling results.¹⁵ Other governments have since then followed suit by frequently blocking or filtering website content deemed to be critical of their actions.

In Tanzania, at least five cases of website blocking and interference have been reported. In 2009, the www.zeutamu.com blog was shut down and its author was arrested for publishing allegedly doctored photos of the Tanzanian president, while in 2011 the Tanzanian government was reported to have tried to clone the website of jammiforums.com, a discussions group, in an attempt to control its content.¹⁶ Earlier in 2008, the founders of Jammiforums, then called Jamboforums.com, were arrested and detained for one day, the website's

computers were confiscated by the authorities, and their website was shut down for five days.¹⁷ In October 2013, the Tanzanian newspaper *Mwananchi* was ordered to stop publishing online following a three-month ban over "seditious" content.¹⁸

Ethiopia has the most tightly controlled telecoms sector, and ranks lowest with regard to internet access. It, however, tops the list for having the most blocked websites in the region. These include the websites of human rights defenders, opposition parties, bloggers, news agencies – *Al Jazeera*, *Al Arabiya* and the *Washington Post* – and several social media platforms.¹⁹

In Rwanda, the government ordered the blocking of the website for the *Umuvugizi* newspaper in 2010.²⁰ It is also reported that several websites belonging to opposition members and other citizens deemed critical of the Rwandan government continued to be blocked between 2010 and 2013.²¹ Burundi joined the league with one reported case involving the blocking of the comments section on www.iwacu-burundi.org, when the media regulator deemed some readers' comments to be a "threat to national security".²²

State actors in some of these countries have made public announcements expressing their intention to monitor online users' communications. In Uganda, for instance, on 30 May 2013, the security minister announced plans to monitor "social media users who are bent to cause a threat to national security."²³ In the same year, Facebook reported that two requests were received from the Ugandan government regarding details of one its users.²⁴ Al-

1 Song, S. (2014, March). African Undersea Cables. *Many Possibilities*. <https://manypossibilities.net/african-undersea-cables>

2 Communications Commission of Kenya. (2013). Quarterly Sector Statistics Report: Second Quarter of the Financial Year 2013/14. www.ca.go.ke/images/downloads/STATISTICS/Sector%20Statistics%20Report%20Q2%202013-14.pdf

3 www.itu.int/en/ITU-D/Statistics/Documents/statistics/2014/Individuals_Internet_2000-2013.xls

4 Tanzania Communications Regulatory Authority (2013). Telecom Statistics. www.tkra.go.tz/images/documents/telecommunication/telecomStatsDec13.pdf

5 www.itu.int/en/ITU-D/Statistics/Documents/statistics/2014/Individuals_Internet_2000-2013.xls

6 Ibid.

7 CIPESA. (2014). *State of Internet Freedoms in East Africa 2014: An Investigation into the Policies and Practices Defining Internet Freedom in East Africa*. www.cipesa.org/?wpfb_dl=76

8 The Kenya Information and Communications Amendment Act 2013. www.cck.go.ke/regulations/downloads/KenyaInformationandCommunications_Amendment_Act2013_.pdf

9 Communication for Implementation of the Constitution. (2012). The National Intelligence Service Act, 2012. www.cickkenya.org/index.php/legislation/acts/item/241-the-national-intelligence-service-act-2012

10 The Prevention of Terrorism Act, 2002. www.immigration.go.tz/downloads/Tanzania_Prevention%20of%20Terrorism%20Act%202002%20.pdf

11 Abyssinia Law. (2012). Telecom Fraud Offence Proclamation, No. 761/2012. www.abyssinialaw.com/uploads/761.pdf

12 chilot.files.wordpress.com/2013/10/national-intelligence-and-security-service-re-establishment-proclamation-english.pdf

13 APCNews (2014, May 19). New laws in Uganda make internet providers more vulnerable to liability and state intervention. *APCNews*. <https://www.apc.org/en/news/new-laws-uganda-make-internet-providers-more-vulne>; Nafuka, J. (2014, April 22). New laws in Uganda restrict citizens' rights. *CIPESA*. www.cipesa.org/2014/04/new-laws-in-uganda-restrict-citizens-rights

14 Privacy International. (2006). *Uganda: Privacy issues*. <https://www.privacyinternational.org/reports/uganda/iii-privacy-issues>

15 The Monitor (2006, February 26). Government jams Monitor radio, site. *UPC*. www.upcparty.net/memboard/election7_260206.htm

16 Allen, K. (2011, June 16). African jitters over blogs and social media. *BBC News*. www.bbc.co.uk/news/world-africa-13786143#story_continues_1

17 Balancing Act. (2008). Tanzanian Government detains two website editors. *Balancing Act*. www.balancingact-africa.com/news/en/issue-no-395/internet/tanzanian-government/en#sthash.AHUqz7O.dpuf

18 The Citizen. (2013, October 1). Government now bans 'Mwananchi' website. *The Citizen*. www.thecitizen.co.tz/News/Government-now-bans-Mwananchi-website/-/1840392/20140814/-/item/0/-/ph66mgz/-/index.html

19 CIPESA. (2014). *State of Internet Freedoms in Ethiopia 2014*. opennet.africa.org/wp-content/uploads/researchandpubs/State%20of%20Internet%20Freedoms%20in%20Ethiopia%202014.pdf

20 Reporters Without Borders. (2010, June 11). Persecution of independent newspapers extended to online versions. *Reporters Without Borders*. en.rsf.org/rwanda-persecution-of-independent-11-06-2010,37718.html

21 Freedom House. (2013). *Freedom on the Net 2013*. <http://freedomhouse.org/report/freedom-net/2013/rwanda#>. UgKP9rH8uoM

22 Reporters Without Borders. (2013, May 31). Burundi - Media regulator suspends comments on press group's website. *Thomson Reuters Foundation*. www.trust.org/item/20130531164503-qium7/?source%20=%20hoppartner

23 CIPESA. (2013, June 10). Uganda's assurances on social media monitoring ring hollow. *CIPESA*. www.cipesa.org/2013/06/ugandas-assurances-on-social-media-monitoring-ring-hollow

24 <https://govtrequests.facebook.com/country/Uganda/2013-H2>

though both requests were rejected by Facebook, the state-owned newspaper *Sunday Vision* reported that a former head of political intelligence in the president's office was arrested on suspicion of being the owner of the Facebook account "Tom Voltaire Okwalinga", which is strongly critical of the government.²⁵

In Burundi, Ethiopia and Rwanda, online users are constantly intimidated and arrested over content posted online, often cited as threatening national security or inciting violence among the public. Ethiopia has been faulted by many digital rights defenders and to date tops the list of African countries that are constantly intimidating, monitoring, intercepting communications and issuing criminal sanctions against users who post content online.²⁶ In April 2014, six members of the blogging group "Zoneg" and three freelance journalists associated with the group were arrested following accusations of working with foreign organisations and rights activists through "using social media to destabilise the country."²⁷ Rwanda is also reported to actively intercept communications, as was seen in 2012 when records of emails, phone calls and text messages of opposition activists were produced in court as evidence.²⁸ Another incident was recorded in April 2014, when private messages exchanged via WhatsApp and Skype between a local journalist and musician were produced as evidence in court during a treason trial.²⁹

According to research conducted by the Collaboration on International ICT Policy for East and Southern Africa (CIPESA), in Kenya, Tanzania, Burundi and Rwanda, governments' interest in citizens' social media activity has also been motivated by the need to combat online hate speech. Although hate speech is a genuine concern, measures taken to combat it are often said to violate online user privacy and freedom of expression.³⁰ Kenya is reported to have blocked access to one website, www.ma-

shada.com, for its failure to moderate hate speech ahead of the 2013 elections.³¹ In 2013, the Kenyan government was also looking for 14 bloggers for allegedly posting hate speech messages, with one arrested and charged under Section 29(b) of the Kenya Information and Communications Act, 2013, for posting an "offensive tweet".³²

Kenya, Tanzania and Uganda have each been reported to have made requests to internet intermediaries to release information on particular users' details. In 2012, Google listed Kenya among the eight African countries which had requested particulars about its users. The Kenyan request, which was rejected, involved the removal of content from a blogger site following a court order in a defamation case.³³ Similarly, in the last quarter of 2013, Kenya topped the list of African countries that made requests to the search company. A total of eight requests were made, with Google fully or partially complying with 63% of these.³⁴

Telecom giant Vodafone, in its first Law Enforcement Disclosure Report released in June 2014, revealed that the governments of Kenya and Tanzania actively monitored its subscribers' communications by issuing data requests to the telecom companies.³⁵ Tanzania was reported to have made the highest number of requests in all of the African countries for which Vodafone provided statistics – 98,785 requests. Statistics about requests made in Kenya could not be revealed due to legal restrictions in the country.³⁶ Lawful interception of communications is provided for in Tanzania under Section 9 of the Electronic and Postal Communications Act 2010 and Section 31 of the Prevention of Terrorism Act, 2002; and in Kenya under the National Intelligence Service Act, 2012, and Section 27 of the Kenya Information and Communications (Amendment) Act 2013. However, Vodafone also noted that it had

not received any demands for technical assistance to enable interception of communications in these countries.³⁷

Conclusions

The increase in internet access speed, reduction in internet costs and proliferation of easy-to-use digital tools have led to a shift in the way citizens and governments engage with each other and share information in East Africa. However, this is being threatened by clauses in legal and regulatory frameworks in these countries.

Although there is indeed cause for governments to protect national security and fight cyber crime, creating a balance between promoting national security and protecting internet rights, including the rights to information, freedom of expression, privacy and data protection, is becoming controversial in many respects. As seen in the cited violations, legal frameworks are being used to arrest, intimidate, monitor and intercept communications of sometimes innocent online users expressing legitimate opinions. Moreover, the legal frameworks often curtail constitutionally guaranteed rights. It is also feared that these laws and their associated violations are triggering self-censorship, a practice that may limit internet growth and have a chilling effect on freedom of association, even in the offline world, in these countries.³⁸

In all the six focus countries, data protection and privacy laws do not exist, despite mandatory user registration exercises for voice and data communications and lawful interception of communications. This is coupled with a general lack of knowledge on what constitutes internet freedoms and limited capacity and skills by both state and non-state actors to safeguard internet freedoms.³⁹

Action steps

An urgent call to advocate for the amendment of laws and regulations that curtail freedom of expression online, user privacy and the right to information needs to be made in all these countries. Countries should commit to the implementation of progressive laws that allow for the enjoyment of internet rights. There needs to be a push for meaningful multi-stakeholder participation in policy-making processes to deter the passage of regressive laws.

Capacity building for both state and non-state actors needs to be undertaken to empower them with the necessary knowledge and skills on internet rights. This will allow state actors to understand what constitutes internet rights so that they are better placed to handle cases arising from perceived violations. Non-state actors including human rights activists, digital rights defenders, bloggers and journalists need capacity development in the area of digital safety. Among other things, they need skills to better understand legal provisions so that they do not fall on the wrong side of the law.

There is a need for more openness from all actors – including state agencies, telecom companies and content hosts – in disclosing information about online freedom violations. State agencies should become more transparent by sharing findings from investigations and prosecutions of digital offences with the public. All telecom companies should take Vodafone's lead by revealing all government requests for intercepting, monitoring or censoring communications. This will serve as a best practice and also create more awareness about state surveillance.

25 CIPESA. (2014). *State of Internet Freedoms in Uganda 2014*. opennet.africa.org/wp-content/uploads/researchandpubs/State%20of%20Internet%20Freedoms%20in%20Uganda%202014.pdf

26 CIPESA. (2014). *State of Internet Freedoms in Ethiopia 2014*. opennet.africa.org/wp-content/uploads/researchandpubs/State%20of%20Internet%20Freedoms%20in%20Ethiopia%202014.pdf

27 Addis Standard. (2014, April 28). Ethiopia files charges against a group of bloggers, journalists detained over the weekend. *AllAfrica*. allafrica.com/stories/201404281454.html

28 Freedom House. (2013). Op. cit.

29 The East African. (2014, April 26). Phone evidence used in terror, treason case. *The East African*. www.theafrican.co.ke/news/Phone-evidence-used-in-terror/-/2558/2294196/-/klwpvi/-/index.html

30 CIPESA. (2014). *State of Internet Freedoms in East Africa 2014: An Investigation into the Policies and Practices Defining Internet Freedom in East Africa*. www.cipesa.org/?wpfb_dl=76

31 Diaspora Messenger. (2013, January 30). Kenya's popular forum Mashada.com shut down in hate speech Crackdown. *Diaspora Messenger*. diasporamessenger.com/kenyas-popular-forum-mashada-com-shut-down-in-hate-speech-crackdown

32 Jambo. (2013, May 15). Robert Alai arrested for alleged "libelous" twitter post. *Jambonewspot.com*. www.jambonewspot.com/robert-alai-arrested-for-alleged-libelous-twitter-post/

33 CIPESA. (2013, September 9). Online freedoms under siege as African countries seek social media users' information. *CIPESA*. www.cipesa.org/2013/09/online-freedoms-under-siege-as-african-countries-seek-social-media-users-information/#more-1623

34 Google. (2013). Google Transparent Report – Kenya. <http://www.google.com/transparencyreport/userdatarequests/KE/>

35 Vodafone. (2014). Law Enforcement Report. http://www.vodafone.com/content/sustainabilityreport/2014/index/operating_responsibly/privacy_and_security/law_enforcement.html

36 Kalemera, A., & Nanfuka, J. (2014, July 2). Vodafone reveals government requests for subscriber information. *OpenNet Africa*. opennet.africa.org/vodafone-reveals-government-requests-for-subscriber-information

37 Vodafone. (2014). Country-by-country disclosure of law enforcement assistance demands. www.vodafone.com/content/sustainabilityreport/2014/index/operating_responsibly/privacy_and_security/law_enforcement/country_by_country.html

38 CIPESA. (2014). *State of Internet Freedoms in East Africa 2014: An Investigation into the Policies and Practices Defining Internet Freedom in East Africa*. www.cipesa.org/?wpfb_dl=76

39 Ibid.

CAMEROON

The stammerings of Cameroon's communications surveillance



PROTEGE QV

Sylvie Siyam and Serge Daho
www.protegeqv.org

Introduction

The Republic of Cameroon is a country in the west central Africa region. It is bordered by Nigeria, Chad, the Central African Republic, Equatorial Guinea, Gabon and the Republic of Congo.

In this country of nearly 21,700,000 people,¹ of which 1,006,494 are internet users² (representing roughly 5% of the population), according to the International Telecommunication Union (ITU), it is a real challenge to identify the presence of communications monitoring by the state. Nonetheless, we know that under the guise of national security and intelligence gathering, citizens' computers and internet communications are spied on by the government.

This was demonstrated when MTN's Twitter service in Cameroon was shut down on 8 March 2011. Wary about the role played by Twitter and other social networks in sparking an Egypt or Tunisia-style uprising, the government blocked MTN's Twitter service³ for security reasons during what were later called "hunger riots" in our country.

Policy and political background

Since independence, Cameroon's successive constitutions have proclaimed its people's commitment to human rights as set out in the United Nations Universal Declaration of Human Rights and the African Charter on Human and Peoples' Rights. Our country is also party to major international and regional human rights conventions, including the International Covenant on Civil and Political Rights (ICCPR).

At the national level, the preamble to the constitution declares the Cameroonian people's

commitment to the freedom of communication and expression.

Many laws and decrees dealing with freedom of communication and expression and with telecommunications and communications exist in Cameroon, some of which impact on surveillance:

- Law N° 98/014 of 14 July 1998, which regulates telecommunications.
- Law N° 2004/016 of 22 July 2004 creating the National Commission on Human Rights and Freedoms. The commission is an independent institution set up to promote and protect human rights in the country. Though important, none of its statutory provisions hint at the surveillance of communication.
- Law N° 2010/021 of 21 December 2010 governing electronic commerce.
- Law N° 2010/013 of 21 December 2010 governing electronic communications in Cameroon.
- Law N° 2010/012 of 21 December 2010 on cyber security and cyber crime. The latter "governs the security framework of electronic communication networks and information systems, defines and punishes offences related to the use of information and communication technologies in Cameroon." While this law was hailed by some as a much-needed step in the right direction to curb Cameroon's nascent or burgeoning cyber crimes industry, others have criticised it for being light on internet security and heavy on sanctions, particularly with regard to sanctioning online expression.
- Decree N° 2002/092/PR of 8 April 2002 creating the National Agency for Information and Communications Technologies (ANTIC). The ANTIC was created to facilitate and accelerate the uptake of ICTs in Cameroon so that they can contribute to the development of the country.
- Decree N° 2012/180/PR of 10 April 2012 assigning new missions to the ANTIC, including the regulation of electronic security activities and the regulation of the internet in Cameroon. With this decree, the ANTIC became the key actor in terms of restrictions imposed by the government on the free flow of online information.

- Decree N° 2013/0399/PM of 27 February 2013 establishing the modalities of protection for electronic communications consumers. This decree clearly states that when it comes to electronic services, the consumer is entitled to have his or her protection kept private.

"Weeding them out":

Evidence of surveillance in Cameroon

There are few credible reports that the government monitors email or other internet-related activities in Cameroon. However, as certainly as everywhere throughout the world, Cameroon's administration does spy on citizens' emails to checkmate the activities of unscrupulous people capable of threatening its internal security. In 2009, the government launched a campaign aimed at capturing the personal information of mobile phone holders, allegedly "to ban the unfair use of the mobile phone [in a way that can prejudice] law and public order and ... citizens' safety."

The government's monopoly over all mobile and internet infrastructures through its sole, state-owned telecom operator, CAMTEL (Cameroon Telecommunications), facilitates communications surveillance. During an interview given to the online media outfit Cameroon-Info.Net,⁴ Woungly Massaga, a Cameroonian dissident, stated his phones have always been tapped.

On 19 March 2014, the general manager of the ANTIC gave an interview to the government's daily newspaper *Cameroon Tribune* during which he further provided details on how social networks and websites are watched in Cameroon. To deal with ill-intentioned persons and the terrorist groups who use social networks to recruit followers and spread propaganda, he said, "The ANTIC uses state-of-the-art tools or cutting-edge tools to permanently watch social networks. This consists of browsing the various profiles on the social networks to detect illicit content representing a potential threat for the national security and the image of Cameroon, and to weed them out."⁵

When it comes to websites, the ANTIC uses a technical platform that scans web content using keywords to detect those inciting hatred, being

slandrous, or representing a danger for the state. Though it is still unclear which technologies are used to monitor telecoms activity in Cameroon,⁶ the interview shed light on the process that led to the shutting down of MTN's Twitter service in Cameroon from the 8 to the 18 March 2011 during peaceful protests. Prior to that, on 22 February 2011, Cameroonian government spokesperson Issa Tchiroma Bakary summoned journalists to his office for a media briefing in which he issued a warning directed at Cameroonians in the diaspora using social media tools such as Facebook and Twitter to call for a march to end the 29-year rule of President Paul Biya. The protest was to coincide with an opposition-led march in Douala to honour demonstrators killed by security forces during February 2008 anti-government protests.

A coalition of organisations led by Privacy International, Access and the Electronic Frontier Foundation has outlined a set of 13 International Principles on the Application of Human Rights to Communications Surveillance.⁷ These include proportionality, competent judicial authority, due process and user notification. Did the blocking of MTN's Twitter⁸ service meet these requirements?

At the time Twitter was blocked, only around 50 people⁹ were affected by the suspension of MTN's service – so was it worth blocking it? This raises the proportionality principle: was there a high degree of probability that a serious crime was about to be committed by MTN's Twitter users?

The principles state: "Determinations related to communications surveillance must be made by a competent judicial authority that is impartial and independent." Cameroon of course lacks a judicial mechanism to protect people from unlawful government surveillance. As a consequence, no judicial warrant was obtained to shut down MTN's service.

Another of the 13 Principles that was ignored by the government is the "due process" principle that requires states to respect and guarantee individuals' human rights by ensuring that lawful procedures surrounding communications surveillance are properly recorded and available to the general public. Cameroonian Minister of Communications and

¹ countryeconomy.com/demography/population/cameroon

² www.internetworldstats.com. According to the World Bank, internet users are people with access to the worldwide network. This may include users who access the internet at least several times a week and those who access it only once within a period of several months.

³ MTN is a mobile telephone company that in March 2011 was the sole Twitter service provider in Cameroon.

⁴ Nangué, Y. (2014, May 19). Interview de Woungly Massaga, Homme politique et nationaliste Camerounais: "Le Cameroun est une véritable bombe à retardement". *Cameroon-Info.Net*. www.cameroon-info.net/stories/0,61441,@cameroun-20-mai-2014-interview-de-woungly-massaga-homme-politique-et-nationalist.html

⁵ Cameroon Tribune. (2014, March 29). [Interview] Cameroun: Dr Ebot Ebot Enow Directeur Général de l'Agence Nationale des TIC. *Afro Concept News*. www.afroconceptnews.com/2014/03/29/interview-cameroun-dr-ebot-ebot-enow-directeur-general-de-lagence-nationale-des-tic

⁶ It is worth pointing out that the Chinese telecom giants ZTE and Huawei, major players in the African and global telecom industry, are CAMTEL's telecom equipment suppliers in Cameroon.

⁷ https://en.necessaryandproportionate.org/text

⁸ The Twitter via SMS service offered by MTN Cameroon, one of three telecommunications operators in the country, allowed anyone with a regular phone to punch in a code and start receiving tweets for free.

⁹ The deal between MTN Cameroon and Twitter was concluded on December 2010 when the smartphone adoption and internet penetration rates were relatively low in Cameroon.

government spokesman Issa Tchiroma told Agence France Presse that “it was the government’s job to protect the nation,” and that the Twitter service was blocked “for the highest interest of the state.” While this may be true, Cameroon is party to the International Covenant on Civil and Political Rights (ICCPR), and Article 19 of the ICCPR guarantees the “freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers.” Article 9 of the African Charter on Human and Peoples’ Rights, to which our country is also party, guarantees that every individual shall have the “right to receive information” and “to express and disseminate his opinions within the law.” The government’s job is not only “to protect” the nation, but also to protect and guarantee its citizens’ rights, and one of the most fundamental of these is the right to communicate – the internet has become a key means by which individuals can exercise their right to freedom of opinion and expression.¹⁰

Concerning the “user notification” principle, individuals should be notified of a decision authorising communications surveillance with enough time and information to enable them to appeal the decision. An 8 March 2011 tweet by Bouba Kaele, marketing manager of the Cameroon division of MTN, announced that “[f]or security reasons, the government of Cameroon requests the suspension of the Twitter SMS integration on the network.” MTN later confirmed the suspension without explanation: “Twitter SMS Connectivity Service suspended from March 07, 2011 till further notice.” As a result, Twitter users were not informed prior to the service shutdown and the suspension caught them by surprise. The shutdown prompted an outcry from Reporters Without Borders, which condemned the lack of transparency surrounding the block and feared its implications for online freedom of expression in Cameroon. They said: “We hope the blocking of Twitter via SMS is not a prelude to other kinds of censorship of mobile phone services or tighter controls on the internet. Everything suggests that the authorities are trying to stop microblogging. We deplore the apparent readiness to impose censorship for the least reason, especially when the target is the peaceful expression of opinions.”¹¹

Conclusion

Nearly every country in the world recognises the right to privacy explicitly in its constitution. At a minimum, these provisions include rights of inviolability of the home and secrecy of communications. Though it exists, communications surveillance, as far as we know, is not pervasive in Cameroon. Nevertheless, from our story, we learned that the government decision did not take into account people’s legitimate and fundamental right to freely seek and receive information or to communicate. Most agree that national security¹² and the fight against terrorism might justify restrictions on the free flow of online information. However, these restrictions must be founded upon evidence that there is a high degree of probability that a serious crime will be committed.

Cameroon’s MTN Twitter shutdown can also be seen as a reminder that we lack both judicial and legislative mechanisms to protect people from unlawful government surveillance. Then, what are the reactions of different stakeholders since “the same rights that people have offline must also be protected online”?¹³

Officials have always been wary about the internet and other social networks, for they allow individuals to express their ideas and opinions directly to a world audience, and easily to each other. Since the Arab Spring – and mostly in Africa – the possibility of the internet and social media networks empowering citizens and the media in mobilisation is considered a real threat by some governments. However, civil society has so far paid little attention to the issue of surveillance, given that very few cases have been reported. Communications surveillance is also disconnected from the daily concerns of the Cameroonians, given that only 5% of the population are internet users.

Finally, MTN is a South African-based mobile operator, and although this report does not address this issue directly, the complicity of foreign companies colluding in state monitoring activities needs to be addressed.

Action steps

With the increasing sophistication of information technology, concerns over privacy violations are now greater than at any time in recent history. So it

is legitimate to express fears about a possible encroachment on privacy. Therefore, we suggest the following action steps in Cameroon:

- Laws that already exist that protect the rights to freedom of expression and privacy should be implemented in order to prevent abuse of emergency powers that can shut down networks or intercept communications.
- Cameroon’s parliament must appoint an intelligence and security committee to oversee intelligence and security activities that reports directly to parliament.
- Parliament could also appoint an independent intelligence service commissioner and a communications interception commissioner among former senior judges whose reports, once again, should be addressed directly to the parliament.
- Legal safeguards to limit the scope and determine the grounds of possible surveillance and institutions and officials competent to authorise and carry out communications surveillance should be developed.

- The National Commission on Human Rights and Freedoms should be empowered to make sure that surveillance occurs only as provided in law, that it occurs only when necessary and that it is proportionate to the aim being achieved.
- The government must communicate with the public on how it uses its surveillance powers. This reporting should include the number of data requests made to telecommunications operators and to other mobile and internet service providers, and the number of individuals or accounts that were implicated.¹⁴
- The developers of surveillance tools should take immediate steps to address their misuse. This may require them to be more transparent, and to develop internal company policies against misuse by governments or other stakeholders.

¹⁰ UN Human Rights Council, “The promotion, protection and enjoyment of human rights on the Internet”, Resolution 20 (2012), UN Doc A/HRC/20/L.13.

¹¹ Reporters Without Borders. (2011, March 22). Government blocks Twitter via SMS service. *IFEX*. www.ifex.org/cameroon/2011/03/25/twitter_blocked

¹² Communications surveillance might also endanger the social peace, as was the case in Cameroon some two years ago when WikiLeaks, the famous leaks website, reported the tribalist statements of former justice minister Amadou Ali regarding President Paul Biya’s succession.

¹³ According to the resolution adopted on 5 July 2012 by the UN Human Rights Council.

¹⁴ Human Rights Watch. (2014). “*They Know Everything We Do*”: Telecom and Internet Surveillance in Ethiopia. www.hrw.org/reports/2014/03/25/they-know-everything-we-do « *they know everything we do* »

CANADA

Surveillance and metadata collection in Canada



Alternatives

Catherine Pappas and Stephane Couture
www.alternatives.ca

Introduction

Following revelations from US spy contractor Edward Snowden, it has become increasingly clear that Canada's intelligence agencies are routinely collecting personal data from a variety of sources for both political and economic reasons. In October 2013, a journalist associated with the British newspaper *The Guardian*, Glenn Greenwald, exposed how the Communications Security Establishment of Canada (CSEC) was monitoring Brazil's mining and energy industries, possibly on behalf of Canadian mining corporations. A few weeks later, new documents leaked to the Canadian Broadcasting Corporation (CBC) revealed that the Canadian government allowed the US National Security Agency (NSA) to conduct widespread surveillance while world leaders met at the 2010 G8 summit in Huntsville and G20 summit in Toronto. But allegations earlier this year about CSEC spying on airline passengers have hit closer to home, creating a great deal of concern over the nature of the government's surveillance activities.

Using the case of CSEC's collection of metadata through public airport Wi-Fi networks as a concrete example, this report will provide an analysis of the political and legal framework for understanding privacy and data protection laws and regulations in Canada in the age of ubiquitous surveillance. Looking at changes in technology, laws and regulations as well as political practices, it will try to show how some of today's trends have potentially serious implications for Canadian democracy.

Policy and political background

Privacy in Canada is a fundamental but not an absolute human right. The right to privacy has always been measured with respect to other rights or societal goals, such as prevention of crime and the need to protect national security. But in the post 9/11 era, anti-terrorism legislation reduced judicial controls and eliminated or weakened oversight. Combined with fast technological transformations, this has undoubtedly undermined the application of Canadian

privacy and data protection laws and regulations. Today, many fear that the country is at a turning point with regard to the protection of privacy.

In December 2001, the "omnibus" Anti-terrorism Act (Bill C-36) reasserted the CSEC's authority, redefined its mandate and concealed it in law as an autonomous entity directly accountable to the National Defence Minister. Its budget grew from 96.3 million Canadian dollars in 1999 to an estimated 829 million dollars in 2014.¹ Most importantly perhaps, Bill C-36 introduced a new provision that allowed CSEC to request ministerial authorisation for intercepting private communications for foreign intelligence purposes,² giving the agency greater legal cover to undertake its actions.

Over the last decade, there have also been many attempts to implement new laws that would grant additional powers and tools to collect data and conduct investigations using new digital technologies. Introduced as a way to modernise investigative techniques (Bill C-74, in 2005), to combat criminal electronic communications (B-52 in 2010), child pornography (Bill C-30 in 2012), or cyber bullying (Bill C-13, in 2014), these so-called *lawful access* provisions would force telecommunications operators and internet providers to disclose information about subscribers without the need for a warrant or a judicial order and, in some cases, without the permission to notify them about the data collection. Faced with overwhelming opposition from Canadians, so far, none of these bills have been adopted.

CSEC and the expanding scope of surveillance through metadata collection

A key policy issue given prominence these days is the legality of the Canadian government's vast metadata collection programmes. On 30 January 2014, a document initially leaked by Snowden and obtained by CBC News³ revealed that CSEC has

been collecting metadata to monitor the activities of public airport wireless internet users. The leaked document describes the data collection project that occurred for over a two-week period in a major Canadian airport. With this data, CSEC was able to track travellers several days after they left the airport and connected their wireless devices to other Wi-Fi systems in Canadian cities or US airports. It could also track back the travellers' whereabouts the days before their arrival at the airport. IP profiling was then used to map travel patterns and geographic locations over a period of time.

The leaked document described the CSEC operation as a trial run of a powerful new software programme, developed jointly by CSEC with the help of the NSA, that could track "any target that makes occasional forays into other cities/regions." Although the authorities in charge of the Wi-Fi systems have denied providing any data to the government, one analyst suggests that it was "presumably obtained with the cooperation of Canada's major telecom companies."⁴ The leaked document also mentions a "proof of concept" – possibly a previous pilot project – in which a modest-sized city was "swept" and a telecommunications system providing services to some 300,000 users was accessed. The CBC report on the leak also mentions intentions of sharing technologies and data collected with official spying partners.

This Snowden leak on CSEC's metadata collection programme came several months after the Canadian daily, the *Globe and Mail*, revealed that CSEC has been collecting Canadian metadata on "telephone and internet traffic records."⁵ According to documents obtained by the newspaper, metadata collection programmes were authorised under two ministerial directives (in 2005 and 2011) on the collection and use of metadata. In light of these revelations, many suspect that the Wi-Fi data collection programme is not an isolated case and that information continues to be collected from other public Wi-Fi hubs across the country indiscriminately, over longer periods of time, and without our knowledge, to create metadata trails of individual users.⁶

CSEC has been legally mandated to "acquire and use information from the global information infrastructure for the purpose of providing foreign intelligence," to "provide advice, guidance and services to help ensure the protection of electronic information and of information infrastructures of importance to the Government of Canada," and to "provide technical and operational assistance to federal law enforcement and security agencies in the performance of their lawful duties."⁷ The agency also shares information it collects or acquires with the other members of the Five Eyes Intelligence community, that is, the US, the United Kingdom (UK), Australia and New Zealand.⁸

CSEC's operations remain one of Canada's best kept secrets. Contrary to other law enforcement and intelligence agencies, such as the Canadian Security Intelligence Service (CSIS – similar to the CIA in the US) and the Royal Canadian Mounted Police (RCMP), CSEC is not designated as an agency under the Access to Information Act and the Privacy Act and, because of this, does not allow independent oversight by the Information Commissioner and the Privacy Commissioner.⁹ Its only oversight is from the CSEC Commissioner, a watchdog role currently held by retired Québec judge Jean Pierre Plouffe, who reports to and is accountable to the Minister of Defence. According to Wesley Wark, an expert on national security, intelligence and terrorism, "the performance of the CSEC Commissioner's function has been hamstrung by an inability to communicate to the Canadian public and by the long-drawn-out battle to bring sufficient agreed clarity to CSEC's legal mandate with regard to the interception of private communications under Ministerial authorization."¹⁰

Often described as the digital envelope that carries the actual content over networks, metadata is not data *per se*, but refers to all the information used to identify, manage, describe or route data over a given network. Metadata can contain the date, time, duration and location of a communication, phone number or internet protocol address, as well as the ID of the sender and the recipient. Even if metadata

1 Office of the Parliamentary Budget Officer. (2014). *Main estimates 2014-15*. www.pbo-dpb.gc.ca/files/files/2014-15_Main_Estimates_Report_EN.pdf

2 Parliament of Canada. (2001). *Statutes of Canada 2001: Bill C-36*. www.parl.gc.ca/content/hoc/Bills/371/Government/C-36/c-36_4/c-36_4.pdf

3 Weston, G. (2014, January 31). CSEC used airport Wi-Fi to track Canadian travellers: Edward Snowden documents. *CBC News*. www.cbc.ca/news/politics/csec-used-airport-wi-fi-to-track-canadian-travellers-edward-snowden-documents-1.2517881

4 Geist, M. (2014, February 4). Against Oversight: Why Fixing the Oversight of Canadian Surveillance Won't Solve the Problem. *Michael Geist*. www.michaelgeist.ca/2014/02/csec-surveillance-problem

5 Freeze, C., & Stueck, W. (2013, October 22). Civil liberties groups launch lawsuit again. *The Globe and Mail*. www.theglobeandmail.com/news/national/canadian-eavesdropping-agency-facing-lawsuit-from-civil-liberties-group/article14984074

6 McGuire, P. (2014, February 4). The Harper government insists it's legal to collect metadata. *VICE Canada*. www.vice.com/en_ca/print/the-harper-government-insists-its-legal-to-collect-metadata

7 Communications Security Establishment Canada (CSEC). (2013). What we do and why we do it. www.cse-cst.gc.ca/home-accueil/inside-interieur/what-nos-eng.html

8 en.wikipedia.org/wiki/Five_Eyes

9 Cavoukian, A. (2003). *National Security in a Post-9/11 World: The rise of surveillance... the demise of privacy?* Toronto: Information and Privacy Commissioner/Ontario. www.ipc.on.ca/images/Resources/up-nat_sec.pdf

10 Wark, W. (2012). *Electronic Communications Interception and Privacy: Can the imperatives of privacy and national security be reconciled?* Ottawa: Office of the Privacy Commissioner of Canada. cips.uottawa.ca/wp-content/uploads/2012/04/WARK_WorkingPaper_April2012.pdf

does not reveal the content of a conversation, the massive collection of metadata and its cross-linking can reveal much of the values, relationships and activities of an individual. Experts argue that metadata can provide the agency with a fairly accurate snapshot of an individual user, but the government continues to deny that metadata collection violates privacy rights, playing on the dichotomy between content and metadata to justify its programme and sideline privacy concerns. “Metadata is information associated with a telecommunication... and not a communication,” stated a briefing note to the then Defence Minister Peter McKay in 2011, right before he approved the ministerial directive on 21 November 2011.¹¹

According to CSEC governing legislation moreover, the programme is allegedly conducted under its foreign intelligence mandate and CSEC cannot target Canadians or persons in Canada. On 29 January 2014, following the airport Wi-Fi metadata collection, the chief of CSEC, John Forster, argued that the agency’s activities are only directed “at foreign entities, and not at Canadians or anyone in Canada,”¹² although he later stressed that CSEC “is legally authorized to collect and analyze metadata.”¹³

Civil society actors and advocates for the privacy rights of Canadians, on the other hand, worry that this and other operations led by CSEC lack public accountability or oversight and do not respect its mandate. Interviewed by the CBC, the province of Ontario’s Privacy Commissioner Ann Cavoukian stated that “this resembles the activities of a totalitarian state, not a free and open society.”¹⁴

But civil society criticism of CSEC operations is not new. In October 2013, the British Columbia Civil Liberties Association (BCCLA), a Canadian non-profit advocacy group, filed a lawsuit aimed at CSEC for “illegal search and seizure”, requesting that the agency stop certain surveillance activities.¹⁵ The BCCLA argued that the agency’s metadata collection

programme authorised by the minister revealed private information about Canadians or persons in Canada, which infringes Article 8 of the Canadian Charter of Rights and Freedoms, guarding against unreasonable search and seizure.¹⁶ OpenMedia, a Canadian advocacy group very active on internet and information and communications technology (ICT) policies, has also supported the BCCLA’s claim and launched a campaign against spying on Canadians.¹⁷

Conclusion

The metadata collection case raises many questions pertaining to privacy rights in Canada. First, it shows that CSEC activities are far more expansive than previously believed. CSEC seems to be collecting metadata widely with the help of major telecommunications companies. In Canada, public agencies and private businesses have traditionally been subject to different privacy laws. The tighter privacy laws governing the state were meant to protect Canadians from pervasive surveillance. But now that information openly flows from one side to the other without this being regulated by our privacy laws (as the government allegedly acquired some of the bulk data from telecommunications companies without a legal warrant), it raises deep concerns for accountability. In addition to this, the introduction of new lawful access legislation giving law enforcement officials warrantless access to private online information poses an even greater threat to democracy and civil liberties in Canada. A positive note in this story is a recent judgment by the Supreme Court that ruled the disclosure of private online information to government and police without a warrant was unconstitutional, making a step in the right direction for the protection of privacy rights in Canada.¹⁸

Secondly, the case described above highlights the inability of Canadian laws and regulations to deal with metadata. As Canadian technology policy analyst Michael Geist has suggested, the fact that the government insists on the legality of the programme might indicate that the problem lies in the law itself rather than its application, as much of the legal framework fails to acknowledge the broader privacy implications of metadata. There are also considerable discrepancies in the definition of “personal information” found in privacy laws governing the private and public sector, as

well as within federal and provincial privacy legislation.¹⁹ Furthermore, over the years, technological transformations have weakened many of the barriers that were used to protect the privacy rights of Canadians and have rendered obsolete some privacy laws and regulations. Discussions surrounding the legality of the metadata collection programme have therefore been based on interpretation and differing views without having a clear legal framework to work from.

A third area of concern is with the very mandate for Canada’s spy agency. It has become increasingly difficult to delineate the borders of a telecommunications network based on national boundaries. From this perspective, how can one guarantee that this widespread collection of metadata remains within the geographic boundaries of CSEC’s mandate?

Action steps

There have been several positive steps taken by different legislative bodies in Canada to reassert the privacy rights of Canadians. The Senate Standing Committee on National Security and Defence, for instance, is examining CSEC’s programme and potential areas of reform. Civil society groups, on the other hand, are leading campaigns that press for greater protection of privacy rights and open debate on the limits of metadata collection and geography. In May 2014, a coalition of civil society groups and academics released the Ottawa Statement, which sets out recommendations aimed at putting a stop

to government spying on innocent Canadians.²⁰ But still much remains to be done for protecting the privacy rights of Canadians, including:

- Engaging in a full, transparent and participatory public process in order to ensure that laws and regulations pertaining to privacy and the protection of data are in compliance with the Canadian Charter of Rights and Freedoms and acknowledge the United Nations’ reaffirmation of privacy as a fundamental human right.
- Cultivating a better understanding and consideration of the privacy implications of metadata, in particular the way massive collection and cross-linking of this information can reveal much of the values, relationships and activities of an individual.
- Ensuring greater oversight of the operations of CSEC and other surveillance agencies in Canada.
- Putting an immediate halt to plans for introducing further lawful access provisions that would allow for authorities to access metadata through telecommunications agencies without any warrant.
- Strengthening the involvement of civil society in favour of privacy rights through public campaigning, advocacy and education.

11 Freeze, C. (2013, June 15). How Canada’s shadowy metadata-gathering program went awry. *The Globe and Mail*. www.theglobeandmail.com/news/national/how-canadas-shadowy-metadata-gathering-program-went-awry/article12580225/?page=all

12 Forster, J. (2014, January 29). Letter to the Editor re: Globe and Mail editorial, January 29, 2014. *Communications Security Establishment Canada (CSEC)*. www.cse-cst.gc.ca/home-accueil/media/media-2014-01-29-eng.html

13 CSE. (2014, January 30). CSE statement re: January 30 CBC story. *Communications Security Establishment Canada (CSEC)*. www.cse-cst.gc.ca/home-accueil/media/media-2014-01-30-eng.html

14 Weston, G. (2014). Op. cit.

15 British Columbia Civil Liberties Association. (2013). Civil claim to the Attorney General of Canada, 22 October. bccla.org/wp-content/uploads/2013/10/2013-10-22-Notice-of-Civil-Claim.pdf

16 Ibid.

17 <https://openmedia.ca/csec>

18 R. v. Spencer, 2014. scc-csc.lexum.com/scc-csc/scc-csc/en/item/14233/index.do

19 Lyon, D. (2014). *Transparent Lives: Surveillance in Canada*. Edmonton: Athabasca University.

20 OpenMedia.ca. (2014, May 22). Canada’s leading privacy experts unite behind Ottawa Statement, offer high-level proposals to rein in mass surveillance. *OpenMedia.ca*. <https://openmedia.ca/news/canada%E2%80%99s-leading-privacy-experts-unite-behind-ottawa-statement-offer-high-level-proposals-rein-mass>

CHILE

Monitoring back



ONG Derechos Digitales

Juan Carlos Lara
www.derechosdigitales.org

Introduction

Despite being a small country, Chile has shown strong signs of being a friendly country for commerce and entrepreneurship, especially when it comes to foreign investment. This was a major trend that started under the military dictatorship, increasing over the last 25 years. A national commitment to peace, internally and externally, has allowed Chile to stand as a beacon of free trade, social peace, and steady economic growth.

In this environment, it is understandable that from a policy-making perspective, emphasis is given to the best possible conditions for entrepreneurs to carry out their business. This has included privatisation and low taxes, as well as lowering other barriers to commerce. Many say an ambience of social peace allows for better economic security. The low barriers to commerce and sense of security, along with the free market environment, extend to what has been considered one of the most important commodities of the economy of the 21st century: personal information.

While the world debates the nature of and need for the collection of personal data by governments, Chile still does not consider data privacy a matter of great concern. Unfortunately, this has led to an environment where commerce is king, even when it comes to handling the personal data of Chilean citizens. Are they safe from the processing of data by national and even foreign companies? Are Chileans safe from private surveillance, and how do international principles apply when it is businesses, not governments, that are behind the processing of data?

Background

Chile has been singled out as one of the countries with the most progressive laws regarding the internet. This includes a net neutrality law, and a copyright law that allows for notice and takedown of infringing content only when there is a court order. Several administrations have also attempted

to create a “digital agenda” to promote the use of technology, and in doing so foster economic growth.

From a social standpoint, Chile stands out for being a peaceful nation in comparative terms, both in its relationship to its neighbours, as well as within the country. No important terrorist network, whether national, foreign or international, has been reported to carry out activities within the Chilean borders. Intelligence activity is focused on the possibility of social unrest and, especially, on drug cartels operating within the country.

On the other hand, the Chilean government has not been especially concerned with data privacy. Chile stands out from all other Latin American countries (except for El Salvador) because of its lack of constitutional protection of personal data, and a lack of proper legal channels for addressing different violations of data protection laws. And while practices in relation to the protection of personal information are seemingly changing in state agencies (as around the world), there have been instances of the violation of privacy rights, but without these having much impact on policy or law.

Privacy and data: When businesses have more power than states

As with any other regulatory framework that attempts to represent different interests, Chilean data protection laws occur in an environment where the interests of information privacy are not only unclear, but also unbalanced. This is not because of anything the state has done (at least, not in an alarming way). Chile has enacted some of the most progressive legislation addressing difficult issues related to technology, as the copyright reform¹ and net neutrality² laws have shown. Pioneering attitudes from Chilean legislators were already seen regarding data privacy: in 1999, Chile became the first Latin American country with a comprehensive data protection law.³ However, the existence of such a law is not necessarily synonymous with a complete system of safeguards for either personal data or even privacy in general, for different reasons.

¹ Law No. 20.435, 4 May 2010.

² Law No. 20.453, 26 August 2010.

³ Law No. 19.628, 28 August 1999.

First, the national data protection law is not strictly in line with constitutional guarantees as provided by the 1980 constitution, drafted during the military dictatorship that put in place Chile's very liberal economic system. The constitution recognises several fundamental rights, including the protection of private life and the protection of private communications, but not the protection of personal data (unlike almost every other country in the region). These rights are enforceable not only against breaches by the state, but also against attacks or threats by private entities. And because personal data is not part of the constitutional framework, constitutional action can be carried out against breaches of private life or private communications, yet not against the gathering and processing of personal data. Because of this, reliance for protection must be placed upon the law directly.

Second, Chile's data protection law provides the framework for all processing and treatment of personal data, whether by public or private entities, while also respecting the rights recognised in the constitution. From a state intelligence perspective, most efforts have been linked to the collection and processing of all kinds of information with clear focuses: the so-called war on drugs, the prevention of attacks by (very minor) anarchist groups; the assessment of public perceptions regarding diplomatic or political events; and the control of indigenous communities in the southern region of the country.⁴ However, the last issue is quite sensitive to changes in executive power: the current local authority empathises with much of the local indigenous community,⁵ while the former authority condemned their most violent actions as terrorist (with the disagreement of the judiciary).⁶

Third, Chile's privacy rules, covering personal life, private communications and personal data, have all seemingly placed both the interests of free trade and the interests of security above other interests. This is most evident in three aspects, which we

will look at in greater depth below later, that serve as examples of a national attitude towards privacy: one, by broadly allowing practices of private surveillance, for alleged security purposes, in places such as the workplace; two, by legally allowing copyright holders to send alleged online copyright infringers private notices using IP addresses; and three – and most problematically – by legally allowing any person or company to collect and process personal information, as long as they abide by the legal framework established by the data protection law. To this, we might add the legal permission to send unsolicited commercial offers (including spam email).

No control over personal data (except for companies)

Chile's data protection law allows the handling of personal data by any person or company, public or private, including the creation and transfer of databases containing personal data. This is why it is considered a set of rules for enabling the free flow of information between database traffickers. And although the law recognises a series of rights for an individual's data, these rights must be exercised through the civil courts of law, in lengthy and expensive proceedings, which constitute an insurmountable barrier for the average citizen. The lack of a data protection authority adds a lack of institutional strength to an already ineffective piece of legislation. In fact, to date, after the law has been in force for more than 14 years, following this route has resulted in no sentences for the unlawful handling of personal data. Paradoxically, it has also meant that Chilean companies are not eligible to offer certain kinds of services that require intensive handling of personal data, since the country cannot guarantee an adequate level of protection of personal data as required by the European Union.

This state of affairs has allowed personal information to circulate freely in Chile, and legally, through multiple companies dedicated to the handling of personal data. This data is frequently exchanged among companies that offer commercial, financial, health and telecommunications services, among others, seriously affecting the right to a private life guaranteed by the constitution. The existence of a unique ID number for each citizen has only made it easier to identify a set of data belonging to an individual, in practice replacing a person's name as an identifier in several information systems.

In short: Chile's privacy and personal data protection rules place those interests under the control

⁴ An elderly couple died in a fire in their countryside house, allegedly started by members of a Mapuche indigenous community. This led to criticism of the National Intelligence Agency due to a lack of information provided prior to the attack. Pinochet, J. (2013, November 9). La inteligencia en Chile en los tiempos de Snowden. *La Tercera*. diario.latercera.com/2013/11/09/01/contenido/reportajes/25-150344-9-la-inteligencia-en-chile-en-los-tiempos-de-snowden.shtml

⁵ Chile's latest change in government brought a new authority to the region, Francisco Huenchumilla, who is of Mapuche origin and who, unlike his predecessors, has called for a peaceful solution to the unrest, and an end to the classification of Mapuche activists as “terrorists”.

⁶ Although prosecution of violent acts in Araucanía has been pursued under the Anti-Terrorism Law, the courts have systematically rejected this classification.

of private companies. Examples of this are many. Large amounts of personal data leaked from public services⁷ or mishandled by banks and other private companies⁸ could be subject to commercial traffic among private companies, and these practices have not been subject to legal penalties.

In 2009, a lawyer publicly accused her medical insurance company of handing over her medical information, including her medical history and diagnosis, to a chain of pharmacies. She discovered the following when purchasing medication in one of their stores: the pharmacy not only had her name and profile, but also knew her medical condition, supposedly protected not only by data protection laws, but by laws guaranteeing medical privacy. The system allowed the pharmacist to suggest medical products for this person. However, while the administrative authority fined two insurance companies, these companies claimed that exchanging this information was not only legal but also widespread, customary, and even necessary.⁹ In April 2013, years after this scandal, a different insurance company proudly announced a new agreement with similar goals with a different pharmaceutical chain.¹⁰ The 13 International Principles on the Application of Human Rights to Communications Surveillance¹¹ have been drafted and signed by hundreds of institutions and individuals from all corners of the world, demanding state action under strict rules of necessity, proportionality, transparency, accountability, legality and more. But it is hard to assess the damage that can be caused when, in fact, there are private companies with more information at their disposal than even the state has or could have, for the mere fact that commerce is an interest whose strength far surpasses the interests of national security.

Conclusions

Over the last several months, a great deal of public attention has been focused on the capacities of states to gather and process personal information and to conduct communications surveillance, which some have justified in the aftermath of terrorist attacks that have replaced Cold War fears in the public conscience. Such overreach of intelligence services, however, does not seem as easily justified by states which do not face the threat of war, or have more peaceful international relations. But in either case, personal information is still an important resource for different objectives.

Chile has a personal data law which from the beginning seemed to be tailor-made for big companies, and which calls into question the ability of Chile's legislators to address the problems that the information age raises for the protection of fundamental rights and freedoms. In practice, this means that personal data in Chile is not as much under the control of the state as it is in "no man's land", due to a weak set of rights and paltry enforcement mechanisms. This situation forces those who are affected to go to court to gain any effective penalties for abuses. These abuses, because they happen under the opaque practices of private companies, are beyond public scrutiny.

Several reforms to the law are currently being discussed, while some others have resulted in minor adjustments. So far, no reform bill includes the creation of an agency for the protection of personal data, which would give citizens effective tools to protect themselves from the constant abuses that exist today; nor does any bill address the free-for-all in personal information databases that is currently part of the system. Numerous groups with corporate interests seek to maintain the status quo, on the grounds that they are defending the free flow of information, and are against all obstacles that a more effective system would create for entrepreneurship.

How do principles of state surveillance apply when it is not the action of the state that endangers or threatens the interests of privacy? Unfortunately, they do not impact directly as well as they do indirectly, by reaffirming the need for privacy safeguards in any environment where the right to privacy is endangered (or any other fundamental right, for that matter). Because companies are, in this area, even more powerful than the state in their ability to affect or impact on the population, actions aimed at the state, while always convenient to ensure fundamental rights and freedoms, seem less urgent than to demand a constitutional and legal framework that ensures such freedoms are also not subject to the whims of private companies.

Action steps

The protection of fundamental rights and freedoms in this day and age demands action not only to confront powerful states, but also to confront increasingly complex and powerful private entities. This requires strong action from civil society to, in the first place, educate and empower people in the rights that they hold, in order to enforce them and make others respect them.

Secondly, and addressing both private and state power, campaigns should push for the implementation of changes to the law that recognise and enforce stronger privacy rights in different areas

– not only to enact the principles that should frame state action for security purposes, but also to create rules that prevent abuse by private agents.

Thirdly, constant effort is needed to ensure that any legal provisions are fully compliant with international human rights standards and the constitutional framework of Chile. This means, monitor back: demand information from public entities through transparency mechanisms, and demand active public oversight of the action of private agents regarding personal information and private communications. Such strong action will allow citizens to keep in check the threats to privacy that are wrongly touted as legal or necessary.

7 Cooperativa.cl. (2014, March 27). Investigan copia irregular de la base de datos del Registro Civil. *Cooperativa.cl*. www.cooperativa.cl/noticias/pais/servicios-publicos/registro-civil/investigan-copia-irregular-de-la-base-de-datos-del-registro-civil/2014-03-27/093754.html

8 Álvarez, C. (2012, July 3). Banco de Chile reconoce error: envió datos personales a otros clientes por correo electrónico. *Biobiochile.cl*. www.biobiochile.cl/2012/07/03/banco-de-chile-reconoce-error-en-envio-de-datos-personales-a-traves-de-correo-electronico.shtml

9 Jara Roman, S. (2009, May 26). Isapres hacen sus descargos en polémica por intercambio de información con farmacias. *Terra*. economia.terra.cl/noticias/noticia.aspx?idNoticia=200905261057_INV_78098854

10 Diario Financiero. (2013, March 27). Isapre Cruz Blanca sella alianza con Farmacias Ahumada. *Diario Financiero*.

11 <https://en.necessaryandproportionate.org/text>

CHINA

Discourse deferred: PRC netizens swap public microblogs for the not-so-private digital dinner table



Danwei

Hudson Lockett
Danwei.com

Introduction

Before the internet, complaints about sensitive issues in mainland China were confined largely to small private gatherings – often around the dinner table, away from prying cadres’ ears. Today, to better understand the role that online surveillance may now play in the People’s Republic of China (PRC), it must be analysed in the context of a broader information control apparatus and the mainland’s unique social media environment.

With foreign social media platforms like Twitter blocked on the mainland, homegrown microblogs, or weibo (微博), finally came into their own in the early 2010s as a *de facto* public sphere. The rapid spread of information on Sina Corp’s Weibo (新浪微博) microblog platform concerning the 2011 Wenzhou high-speed rail crash (see GISWatch 2011),¹ together with its subsequent role in the scandal leading to the ouster of top leadership candidate Bo Xilai (see GISWatch 2012),² drove that point further home for the ruling Chinese Communist Party (CCP). Even Sina’s in-company censorship efforts seemed unable to quiet the beast it had birthed.

Two new actors have since swung a pair of sledgehammers to the knees of mainland microblogs, forever changing the country’s online ecosystem. The first is the popular app WeChat (branded locally in Mandarin as Weixin 微信, or “micro-message”) developed by Tencent Holdings Limited. WeChat began as a smartphone instant-messaging service, but soon evolved into a versatile private social networking platform and communications tool whose functions even included limited public microblogging. By the end of 2013 it had unseated Sina’s Weibo as the social networking platform of choice.

The second actor is current CCP General Secretary and PRC President Xi Jinping, who was

elevated to the former office in November 2012, and assumed the latter as a matter of course in March 2013. Xi wasted little time in launching a renewed crackdown on dissent – a key front of which was the unruly and critical online chatter that his predecessors had left unquashed. He would confront it with gusto.

Background

Surveillance of the internet’s Chinese-language public face has become increasingly sophisticated as the CCP has sought to use it both as a means to keep tabs on public opinion and a tool to monitor and control speech. Officials are typically mum on the more Orwellian aspects of this effort, but local, privately owned companies such as XD Tech (线点科技) openly offer mass surveillance, analysis and keyword alert services to both central and local governments. XD Tech, which opened for business in Beijing in 2005, lists two of the most important party organs among its clients: the General Office of the CCP’s Central Committee, and the powerful and secretive Central Organisation Department responsible for choosing where Party officials are posted for every step in their careers. Other major clients include the Public Security Department of Guangdong Province, state-owned Bank of China and all three mainland telecom operators (also state-owned).

However, survey results published in March 2014 commissioned by the BBC World Service showed that 76% of Chinese respondents said they felt free from government monitoring – the highest proportion of any country polled.³ Unlike censorship, the surveillance of private information, especially when stored server-side rather than on user devices, can be difficult to verify.⁴ Evidence of government surveillance of WeChat and other such private communication platforms was previously

harder to come by. But a few days before Xi Jinping’s ascent to CCP leadership in late 2012, dissident Hu Jia posted on Twitter (translated):

Tencent-developed “WeChat” is extraordinarily popular on the mainland. Domestic Security Police use it to investigate communications between mainland dissidents. The voice messages, text and pictures we use WeChat to send all go directly into Domestic Security’s technical investigation system, and are just as easily monitored as phone calls and text messages.

That week Hu Jia told the *South China Morning Post* that he had long expected his phone calls and text messages to be tapped by state-owned telecom providers, but previously assumed that WeChat was not compromised. Now he claimed Domestic Security officers had recited, word for word, private voice-message exchanges between him and his friends shortly after they had occurred on WeChat. He said friends had also been interrogated about WeChat conversations that took place only an hour earlier, and gave an example of Domestic Security officers using information from voice messages to track him in real time when he and a friend tried to change a meeting’s venue at the last minute.

Part 1: Twilight of the microblogs (2013)

Once Xi became general secretary his administration wasted little time in launching vigorous crackdowns on both official corruption and dissent. The two drives conflicted when a group called the New Citizens’ Movement pushed for officials to declare their assets and follow rule of law as outlined in the PRC’s constitution. These calls, online and off, were silenced, and the group’s leaders detained or arrested and brought to trial under various pretexts.

That August, one year since WeChat’s user base had surpassed Sina Weibo’s, Tencent added microblog-like “public” accounts to its now flagship service/software. Standard private accounts were still limited in how many people could join a given “friend circle” (100, as of this writing), but all users could now follow unlimited *public* accounts, each of which could send one message a day to all subscribers.

Then, on 10 September, the Supreme People’s Court and the Supreme People’s Procuratorate issued a landmark joint interpretation of PRC criminal law that gave further firepower to censorship efforts: authors of any Weibo or WeChat posts that had been “re-tweeted” 500 times or viewed 5,000 times would be legally liable for any misinformation or illicit content authorities found therein.

While such rulings are not binding precedents that determine subsequent court decisions in the PRC, the message was clear: posts containing unsanctioned information or opinions could result in real punishment.

In fact, a name-and-shame campaign targeting Sina Weibo’s most influential verified users (“Big Vs”) was already underway. In late August, Chinese-American angel investor and Weibo heavyweight Charles Xue was arrested in Beijing on charges of soliciting a prostitute. But in an on-air confession broadcast nationwide, a handcuffed Xue spoke only of his regret over abusing his power to spread misinformation and rumours among his 12 million followers. This intensified crackdown added momentum to already powerful market forces: Weibo activity further waned as WeChat’s moon waxed gibbous.

Critical online discourse went to ground at the apparently more private WeChat, but the October arrest of venture capitalist Wang Gongquan, a backer of the New Citizens Movement, soon called the platform’s privacy into question. When Sina shuttered his Weibo account with 1.5 million followers in 2012, Wang shifted to a standard WeChat account to continue his activism. However, the more private nature of this venue did not stop authorities from detaining and then formally arresting Wang the following year on charges of disturbing public order.

A report by the Public Opinion Monitoring Centre of the state-run *People’s Daily* announced on 30 October that the campaign against Big V’s had succeeded – the government had retaken online space for the Party. The state-run *Beijing Youth Daily* capped the year off on 13 November by claiming Sina had taken action against 103,673 accounts for flouting online behaviour guidelines announced that summer, through measures ranging from temporarily restricting users’ ability to post to permanent account deletion.

Part 2: Dawn of the digital dinner table (2014)

After a few months’ lull, Xinhua reported on 27 February that Xi Jinping was now heading “a central internet security and informatisation leading group” and had that day presided over its first meeting. (Xi has become the leader of other such internal leadership committees since his ascent, and has established other new ones for policy change and domestic security.) A same-day report on CCTV said Xi had emphasised the need for a firm hold on the guidance of public opinion online.

Then on 13 March, WeChat saw its first real purge: Tencent deleted at least 40 critical public

¹ www.giswatch.org/en/country-report/civil-society-participation/china

² www.giswatch.org/en/country-report/internet-and-corruption/china

³ Globescan. (2014, March 31). One-in-Two Say Internet Unsafe Place for Expressing Views: Global Poll. *Globescan*. www.globescan.com/news-and-analysis/press-releases/press-releases-2014/307-one-in-two-say-internet-unsafe-place-for-expressing-views-global-poll.html

⁴ The Citizen Lab. (2013). *Asia Chats: Analyzing Information Controls and Privacy in Asian Messaging Applications*. <https://citizenlab.org/2013/11/asia-chats-analyzing-information-controls-privacy-asian-messaging-applications>

accounts, some with hundreds of thousands of subscribers. On 15 March, the *South China Morning Post* reported that according to an unnamed industry source, a team of government censors were stationed at Tencent's Guangzhou office for a week before the crackdown; censors instructed the company to practice self-censorship on accounts posting "sensitive content on national politics", and named certain accounts that had to be shuttered.

But as March dragged on a major labour dispute in Southern China would provide contrasting examples of WeChat's potential in both grassroots organising and surveillance. Tens of thousands of workers for shoe manufacturer Yue Yuen used WeChat to coordinate a crippling strike in Guangdong without help from their sanctioned, government-run provincial union; meanwhile police detained labour advocate Lin Dong from the Shenzhen Chunfeng Labour Dispute Service Centre on the grounds that he had posted inaccurate information online. The centre's director Zhang Zhiru told the *South China Morning Post* that Lin had only sent a private WeChat group message to 11 people about the issue, and had noted the information was unverified. While the strike was ultimately successful and Lin was released after 30 days in custody, the biggest guns were still waiting in the wings.

On the morning of 27 May authorities announced a social media crackdown one week before the 25th anniversary of the 4 June massacre that ended the Tiananmen Square protests. The special month-long operation specifically targeting WeChat and similar apps would be carried out by major government organs including the State Internet Information Office, the Ministry of Industry and Information Technology, and the Ministry of Public Security. Their stated focus was on public accounts with social mobilisation power. Less attention was given to a new development in how Tencent would approach the social feature that had long been one of WeChat's central conceits: private friend circles.

After WeChat was explicitly named at the crackdown's outset, Tencent and six competitors quickly published a list of 10 proposed industry "initiatives" to help create a "clean internet"; these included a new commitment to further scrutinise private groups. The companies called on industry peers to "intensify management of friend circles and regulate related functions, intensify the inspection and management of friend circles' content, and resolutely shut down accounts that transmit illegal and harmful information via friend circles."

Tencent then announced on 10 June that during the year's first six months it had already shuttered

20 million private WeChat accounts with the help of authorities, in addition to 30,000 public accounts it had deemed fraudulent. In announcing the move, dubbed "Operation Thunder", Tencent claimed the accounts had been guilty of engaging in phishing schemes or prostitution. That day it also announced that the search engine Sogou (搜狗) of the eponymous company it had acquired last year was now capable of searching public WeChat accounts, allowing users to look them up and browse their posts' contents.

Almost as an afterthought the campaign turned its eyes to Apple: the Ministry of Industry and Information Technology announced it would take new measures to regulate the company's iMessage service. A group chat function similar to WeChat's friend circles was added to the Apple instant-messaging app in October 2011; Chinese tech industry news site *Techweb* reported the new measures would include tools to monitor and prevent spam messages, which it claimed had cost users millions of RMB. Finally, following a pro-democracy march in Hong Kong on 1 July that drew a historic turnout of hundreds of thousands according to organisers, messaging apps Line and KaoKao Talk began experiencing issues, with the former rendered completely inaccessible.

Conclusions

Survey results indicate a widespread belief that surveillance on the mainland does not affect or bother with most people's affairs. Until recently even experienced dissidents believed themselves free from snooping eyes and ears on WeChat. Hu and Wang's cases show us that assumptions about what is private online in the PRC do not always hold true, particularly when one uses a supposedly private space to organise. In mainland China the internet and everything in it can reasonably be viewed as public space – that is, ultimately belonging to the state.

Operation of online communications platforms by private companies is a privilege, not a right. The threat of its rescindment will compel corporations to comply with state demands lest they lose permission to stay online. Sina's failure to effectively clamp down on recalcitrant expression eventually prompted more severe government action, though user migration to WeChat was already well underway before this. By more promptly complying with government directives and effectively dealing preemptively with areas of potential concern, Tencent may be able to keep WeChat from coming to the same grisly end.

Much still depends on how netizens take advantage of WeChat's many functions. The massive March strike in Guangdong shows that even friend circles limited to 100 members can spread information rapidly enough between overlapping groups to mobilise tens of thousands, while labour advocate Lin Dong's detainment shows that even very small-scale group communication can serve as a pretext for detention if one helps effectively focus and direct the momentum of such large-scale movements. But even Tencent's in-company surveillance and control efforts may not be as all-powerful as the past year seems to imply. In light of how private PRC companies already provide surveillance services individually to different sectors of the government and Party, the publicly projected monolithic censorship and surveillance effort of Xi's administration may belie an unseen and far more piecemeal approach.

For now, though, critical conversations online have taken refuge in a space that those around before the internet may find familiar: a sort of a digital dinner table, albeit one where conversations are much more easily listened in on. Complaints will continue in semi-private, but this suits the CCP just fine: where before all eyes were struggling to follow a flurry of public microblogs, now only the party has potential access to a comprehensive view of online discourse that could ultimately strengthen its hold on power. While it may not be able to fully stamp out dissent, neither does the party seem likely to face a Snowden of its own any time soon.

Of course, few saw the fall of Bo Xilai coming, either – aside perhaps from Bo's former right-hand man Wang Lijun, who fled to the closest US consulate when he feared his old boss might have him killed, a stack of classified documents in hand for use as a bargaining chip (see again GISWatch 2012).

Action steps

The following action steps can be suggested for China:

- The same basic precautions recommended against National Security Agency (NSA) surveillance all hold true in the PRC: cryptographic anonymity tools are necessary for true privacy in communication. However, unlike in the US, public debate and opposition to the state's surveillance of its own citizens appears impossible without broader public consciousness of these endeavours and systemic political changes.
- Applications and online services made by PRC companies whose servers are on the mainland can be considered to be at least potentially compromised.
- Mobile communication seems particularly vulnerable to surveillance, and likely cannot be relied on for anonymity; this is doubly true if a user is a dissident or known member of advocacy or activist groups that serve organisational purposes.
- While not touched on above, foreign news organisations and businesses are often subject to state-directed hacking efforts in the PRC. WeChat and other such local networking apps, while convenient, essentially create a detailed record of user activity and contacts that can help undermine other efforts to maintain privacy and confidentiality.

COLOMBIA

Hacking information on the peace talks in Colombia



Colnodo

Ariel Barbosa (with the collaboration of Olga Paz)
www.colnodo.apc.org

Introduction

Colombia is a country with one of the highest internet penetration rates in Latin America. This is due to governmental policies and high investment from the private sector, aimed at opening and consolidating new markets.

One of the most recognised ministries in the current government, based on its initiatives and success, is the Ministry of ICTs. One of its leading initiatives is the Vive Digital Programme, which aims to expand not only ICT infrastructure but also the demand for internet services in the country. One of the outcomes of this strategy is that Colombia has more mobile phones than inhabitants and more than 60% of the population are internet users.

Although there has been great progress in providing internet access, services, applications and content, the country is still behind in defining adequate policies in order to strike the right balance between state surveillance and the right to privacy of citizens. Many recent cases have demonstrated the lack of effective policies and regulations controlling information and data storage, and appropriate penalties in cases where information has been illegally disclosed and obtained from citizens and public servants. Some of these cases are: the “chuzadas” (particularly phone hacking) carried out by the former Security Administrative Department (DAS); Operation Andromeda; the hacking of phones and computers of participants in the agrarian strike of 2013; and, most recently, the hacking of phones and computers to sabotage the recent presidential election campaign.

Faced with these events, which caused great concern among the public, the government decided to draft a cyber security and cyber defence policy. The first step taken was to seek the technical assistance of the Organization of American States (OAS), which recommended the inclusion of civil society in defining the policy. However, the complete text of

the policy has not been disclosed to the public and there is growing fear that it will only be disclosed when finalised, without the participation of civil society, which would help prevent imbalances between citizen rights and state surveillance.

Policies and regulation on cyber security and cyber defence

In comparison to other countries in the region, Colombia has made great progress in its technological and technical capacity, closing the gap with developed countries. However, regarding institutional coordination and operations there is still much to be done in terms of design and implementation.

One of the first policies outlining the guidelines for cyber security and cyber defence dates from 14 July 2011 (National Council for Economic and Social Policy – CONPES 3701).² This policy includes the national and international background, and spells out the regulations in the country regarding these issues. Based on this policy, the Cyber Joint Command, the Cyber Police Centre, the Colombian Information Security Coordination Centre (CSIRT) and the Response Group for Cyber Incidents in Colombia were created. These entities work together with the Army Technical Intelligence Central (Citec) and the Police Intelligence Directorate (Dipol).

Following the first state phone hacking scandal, known as “chuzadas” and carried out by the DAS, the national government closed DAS and passed the Intelligence Bill, which became law on 17 April 2013.

This law was put to the test following a second scandal known as “Andromeda”, which revealed the failures in enforcing the law, mainly by members of the army who over several months spied illegally on civil servants and important public figures. In 2014, the government began to draft the cyber defence and cyber security policies, a process in which several civil society organisations (among them Colnodo) asked to be involved – as recommended by the OAS.



“Buggy”, the “Ethical Hacking Community” centre where the Andromeda operation was carried out. PHOTO: eltiempo.com

Peace talks in Colombia

Since the 1950s at least three generations of Colombians have endured an internal conflict in the country caused by the huge inequality in the distribution of wealth – a conflict whose main actors have been different guerrilla groups and the country’s armed forces.

In October 2012, President Juan Manuel Santos confirmed that the government was holding peace talks with FARC, the largest guerrilla group in the country, and the oldest in the world. The news was received both with optimism and scepticism given the failed attempts at peace talks in the past with the same guerrilla group during former president Andrés Pastrana’s administration (one of the most infamous incidents during those talks, which took place in January 1999, is known as “the empty chair”, referring to the absence of the FARC commander, Manuel Marulanda).³

This cycle of internal conflict and failed peace talks allowed intelligence agencies free rein, and some of their activities have not been fully identified.

Andromeda, a front for illegal surveillance of the peace talks

The distrust surrounding the peace talks was confirmed when on 3 February 2014, the weekly magazine *Semana*, which has one of the highest circulations in the country, published an article

exposing “a military intelligence front where not all activities were legal”⁴ that started operating one month before President Santos initiated the new peace talks. The investigation revealed how the military intelligence set up a front for their operations, and used this as a base to illegally surveil members of the government and public figures involved in the peace talks.

The surveillance base was located in a building in a residential neighbourhood in Bogotá. On the second floor, above a restaurant on the ground floor, there was a so-called “Ethical Hacking Community” centre, offering courses on website design and information security and publications on how to spy on a chat site and how to create and detect web attacks, among others.

This centre had been legally opened and was registered in the Bogotá Chamber of Commerce on 12 September 2012. *Semana*’s investigation revealed a series of illegal phone and computer hackings carried out by members of the national army, and a military hacking information centre located in a room known as the “Grey Room”.⁵

The name of this secret operation was “Andromeda”, and an official from the Number One Army Technical Intelligence Battalion (Bitec-1) was in charge of the operation. This battalion is part of Citec, recognised for its success in fighting the FARC by infiltrating their communications – in the past

¹ “Chuzada” is a term used in Colombia when someone secretly taps a phone line without consent.

² www.mintic.gov.co/portal/604/articles-3510_documento.pdf

³ es.wikipedia.org/wiki/Di%C3%A1logos_de_paz_entre_el_gobierno_Pastrana_y_las_FARC

⁴ www.semana.com/nacion/articulo/alguien-espio-los-negociadores-de-la-habana/376076-3

⁵ www.semana.com//nacion/articulo/la-sala-desde-donde-se-hacian-las-chuzadas-del-ejercito/376079-3

this had led to the freeing of kidnapped citizens. However, *Semana* had evidence of how it was also carrying out espionage activities that compromised national security, and was engaged in the illegal phone hacking of recognised public figures. These actions were carried out by members of the army, but also by students, hackers, and participants in so-called Campus Parties (an annual event devoted to technological innovation, digital culture and research). They were not only paid, but handsomely rewarded depending on the political weight of the public figure and the difficulty of gaining access to their information.

After the *Semana* revelations, President Santos consulted internally, and, given the lack of clarity on the issue, asked for a public enquiry to determine “which dark forces are spying on our negotiators in Havana,” where the talks are being held. “They are trying to sabotage the peace process. We need to know if (...) there are loose cannons in the intelligence agencies,” he declared.

The Andrés Sepúlveda case: Intelligence information gathered in the middle of the presidential election campaign

Campaigning for presidential elections began in 2013, but gained momentum in 2014. The first round of the presidential elections took place on Sunday 25 May. Six candidates from different political parties took part in the presidential race. One of them was President Santos, who was looking for re-election. His most important contender was Oscar Iván Zuluaga, who was the candidate for the Democratic Centre – the political party of former president Alvaro Uribe – and who publicly expressed his disagreement with the peace talks in Havana.

The presidential elections were dogged by yet another espionage scandal. The national newspaper *El Tiempo* revealed that at the beginning of May 2014,⁶ a man called Andrés Sepúlveda had confessed before a prosecutor and a deputy attorney general to his involvement in hacking information on the peace talks, and how it was about to be sold to the National Intelligence Directorate (DNI).

One of the most disturbing events in those weeks was the broadcasting of a video⁷ in which Sepúlveda introduces himself as a contractor for cyber security and social networks and discloses part of the information illegally obtained to Zuluaga.⁸

The strategy, from what can be seen in the video, was to publish the information obtained from military sources through the website *dialogosavoces.com* and a Twitter account (<https://twitter.com/dialogosavoces>) in order to attack the peace talks and the government.

However, it is difficult to determine if these revelations affected the election process, and the voting. After the scandal was revealed by *El Tiempo*, the first round of presidential elections led to a run-off between Santos and Zuluaga. Santos was re-elected with a 5% advantage over his rival.

Drafting the Cyber Security and Cyber Defence Policy in Colombia

Simultaneously, and partly because of these issues, Colombia has been drafting a Cyber Security and Cyber Defence Policy, which began just when the Andromeda scandal was revealed.⁹ For this purpose, a commission was formed, but without the active participation of civil society groups in Colombia. This commission has been limited to governmental officials, national experts in information security and representatives from the private sector with crucial infrastructure, such as the financial and energy sectors.

In March 2014 the non-profit organisations Dejusticia, the Karisma Foundation, the Foundation for Press Freedom (FLIP) and Colnodo sent an open letter to President Santos¹⁰ asking that they be included in the surveillance commission. The aim of the organisations was for human and internet rights, specifically the right to privacy, to be represented in the policy-making process.

The Colombian government requested technical assistance from the OAS, whose report was presented on 4 April 2014. Its main recommendation was to create an entity that would oversee the operations of agencies in the armed forces in charge of cyber security, and which would report directly to the president. The OAS also recommended that this agency should be directed by a civilian and not a military person,¹¹ and that the government should aim to “harmonise the Colombian legislation with international legislation (Budapest Convention), particularly on issues of criminal procedural law.” This would enable the implementation of clear policies to prevent human rights violations and to protect the country’s sovereignty.

The OAS has contributed an interesting perspective to the conception of the Cyber Security and Cyber Defence Policy, since it openly declares the importance of incorporating the Budapest Convention in the policy in order to balance national security issues with the defence of human rights.

The Andromeda and Andrés Sepúlveda information hacking cases have yet to come before the court. These cases exposed the flaws in the Intelligence Law (1621 of 17 April 2013) and ultimately the law failed the test. The reason is partly the lack of a centralised body directly responsible to the president, as proposed by the OAS.

Action steps

Civil society organisations should stay actively involved in the design of policies on cyber security and cyber defence in Colombia in order to keep a balance between the defence of the state and privacy rights. It goes without saying that the government should create spaces for civil society participation.

The mission of civil society is to ensure that when laws are created, limits must be defined, as

well as to remind the government that its utmost priority is to protect its citizens. The government needs to ensure that laws are “necessary and proportionate” according to the 13 International Principles on the Application of Human Rights to Communications Surveillance¹² – particularly when the crucial peace negotiation process, which has been going on for two years, could be gravely affected.

It is important for these new laws to consider the following points:

- Communications metadata could be more relevant than content.
- To collect information without permission is a crime, even if no one gets to use the information.
- When information about a citizen is requested to solve a court case, it should be because it is necessary, adequate and proportionate.
- It is important to strike a balance between privacy and cyber defence. That is, the right to privacy is equal to the right to build safe communications systems.

6 www.eltiempo.com/politica/justicia/los-archivos-del-hacker-sepulveda-acusado-de-espiar-proceso-de-paz/13972255

7 www.semana.com/nacion/articulo/el-video-del-hacker-con-oscar-ivan-zuluaga/388438-3

8 www.eltiempo.com/politica/justicia/los-archivos-del-hacker-sepulveda-acusado-de-espiar-proceso-de-paz/13972255

9 www.enter.co/chips-bits/seguridad/ciberdefensa-colombia-politica

10 colnodo.apc.org/destacamos.shtml?apc=l-xx-1-&x=3777

11 www.elespectador.com/noticias/judicial/colombia-no-se-rajo-el-tema-de-ciberseguridad-y-ciberde-articulo-485831

12 <https://en.necessaryandproportionate.org/text>

CONGO, REPUBLIC OF

Civil society and cyber surveillance in the Republic of Congo



AZUR Développement

Romeo Mbengou
www.azurdev.org

Introduction

Information and communications technologies (ICTs) now hold an important place in our daily lives. They are the source of many benefits, including easy and rapid exchanges and communication, data storage, and the digitisation of administrative procedures. However, technologies must be respectful of the privacy of users. This obligation applies to all, with few exceptions, and both to institutions and to individuals.

Yet, according to the revelations of Edward Snowden on the work of the US National Security Agency (NSA), it has now been established that we are not protected from spying eyes. Everything we do is monitored and followed by others for one reason or another. This is cyber surveillance: that is to say, the technical control of electronic communications. Some use it as a means to spy on what others are doing to prepare for any eventuality; others in order to do harm. Whether for one reason or another, cyber surveillance, except in cases where it is permitted by law, is harmful for users because it is a violation of fundamental human rights, including the right to have your privacy respected.

As a world phenomenon, cyber surveillance is ignored by some, its threat is minimised by others, and it is even non-existent in some countries. So, what is the situation in the Republic of Congo? How does civil society consider cyber surveillance? Several Congolese civil society organisations use ICTs in their everyday work. Do they feel monitored on the web? What about the Congolese legislation?

These are the questions that this report will try to answer. To do this, it is important to provide an overview of the legal framework for ICTs in Congo, before analysing civil society awareness of cyber surveillance in the country. This has been done through interviews with civil society organisations.

Overview of the legal framework for ICTs

The legal framework for ICTs in the Congo currently includes:

- The Congolese Constitution of 20 January 2002, which states in Article 19 that “everyone has the right to freely express and disseminate his opinions in speech, writing, image, or any other means of communication...” Article 20 says that “the secrecy of correspondence, telecommunications or any other form of communication cannot be violated except in the cases provided by law.”
- Law No. 8-2001 of 12 November 2001 on the freedom of information and communication. This law guarantees the freedom to access information and communicate, including on the internet.
- Law No. 9-2009 of 25 November 2009 regulating the electronic communications sector. This law describes the conditions for the installation and operation of networks and electronic communications services. In Article 6 it states that “electronic communications activities are practiced freely in accordance with the terms of the legislation and regulations.” This law, which also deals with the protection of users’ privacy, prohibits cyber surveillance. Article 125 states: “It is unlawful for any person other than the users to listen to, record, or store communications and traffic data related to them, or submit it to any other means of interception or surveillance without the consent of the users concerned, except when legally authorised to do so...”¹
- Law No. 11-2009 of 25 November 2009 establishing the regulatory agency of postal and electronic communications. In Article 5 it states that the agency promotes and protects the interests of users in the field of postal and electronic communications.

Other laws are being drafted, including a law on the protection of personal data, a law on cyber security, a law on the fight against cyber crime, a framework law on the Congolese information society and

¹ Law No. 9-2009 of 25 November 2009 regulating the electronic communications sector.

digital economy, and a plan for national broadband development in the Congo.

Use of ICTs by civil society

Congolese civil society organisations are working in several areas, including the defence and promotion of human rights in general, the preservation of the environment, the fight against poverty, the fight against corruption, the fight against HIV/AIDS, and the promotion of ICTs.

These organisations, such as the Congolese Observatory of Human Rights (OCDH), have worked and are working on sensitive issues concerning human rights, and, in the course of their work, they use ICTs. Some organisations have computers on which they can store sensitive data resulting from the analysis or investigation of violations of human rights. This data could include email addresses and phone numbers. The phone is the most frequently used way to contact a civil society organisation in the Congo. Very few organisations maintain a website, a blog or a Facebook account.

Analysis of cyber surveillance in the Congo

Interviews with civil society organisations involved in human rights and ICTs conducted for this report suggest that many are unaware of cyber surveillance. They also pointed to the lack of a government policy on cyber surveillance, and the lack of an independent body securing personal data.

Civil society’s understanding of cyber surveillance

As suggested, it appears that a number of civil society organisations in the Congo have no clear understanding of cyber surveillance. This is largely due to them not having, for the most part, extensive knowledge of and experience in using computers and the internet. Given that they are seldom presented with circumstances that could draw their attention to cyber surveillance, several organisations do not suspect any surveillance, interception or control over the internet.

Loamba Moke, president of the Association for Human and Prisoners’ Rights (ADHUC), commented, “The concept of cyber surveillance is unfamiliar to us. It is unclear whether our email communications are intercepted or stored, and we don’t know how to secure our data on the internet.” In other words, they do not have the expertise necessary to secure their communications, but are also unable to detect the interception or monitoring of their electronic communications. A similar point of view is held by Wilfrid Ngoyi Nzamba, executive secretary of the

Congolese Association of ICT Consumer Products and Services, who argues that there is a clear lack of evidence on the existence of cyber surveillance. He states that “there is no cyber surveillance in Congo” – but for him the reasons include the fact that there are few people qualified to carry out surveillance in a country where there are still a lot of “computer illiterate” citizens among the population.

However, other organisations are more aware of digital security. This is the case with the Organisation for the Development of Human Rights in Congo (ODDHC), which conducted training on digital security for human rights defenders with the support of the Multi-Actor Joint Programme (PCPA) in March 2013. According to Sylvie Mfoutou Banga, president of the ODDHC, “The risk of the piracy of information from human rights advocates has led us to develop this training on human rights and digital security.” Several topics were discussed during the workshop: how to create safe passwords, how to download and install free antivirus protection off the internet, and how to work on the internet without leaving digital traces. Regarding phones, Mfoutou does not know if her phone is tapped.

Another organisation, the Group of Journalists for Peace (GJP), has received training on the secure communications software FrontlineSMS and FrontlineCloud. Tools like these “allow members of an NGO to communicate safely,” said Natalie Christine Foundou, the president of GJP. In 2013, AZUR Développement, in collaboration with the Association for Progressive Communications (APC), organised training on the protection of privacy in the management of online data on women and girl victims of violence.²

Lack of a common national policy on data protection

In the current institutional set-up, there is no common policy on data management, protection and privacy. Each institution or agency, both private and public, is obliged to manage its data in such a way that no data theft can happen. However, the reason why there is no common policy on data protection is simple: email services and websites are not hosted in Congo, but abroad, particularly in France and the United States. Only over the past three years have there been efforts to set up the Congolese Agency for Internet Naming (ACNIC). This new organisation will now manage the internet country code domain “.cg”.

“If Congolese civil society or any other person is subject to control or cyber surveillance, this would not be on the part of national authorities, but rather

² www.violencedomestique-congo.net

foreign institutions; and they will be monitored not as Congolese civil society necessarily, but as Yahoo or Google users,” said Davy Silou, a computer engineer and independent consultant. He also mentioned that some computers used by civil society are often not secure, and do not use the original licences.

In addition, training in ICTs must remain a priority for the Ministry of Posts and Telecommunications, responsible for new technologies, and the Ministry of Higher Education, as a national data protection programme will require a high level of skills. There is still no computer course in the one and only public institution for higher education, the Marien Ngouabi University of Brazzaville. Investment in research and development are insufficient to be able to develop skilled human resources in the ICT sector in Congo. Cisco courses are offered at an approximate cost of 40,000 FCFA (USD 80) per module.

ICT incubator projects are insufficient. The company VMK created the Bantu Hub, a technology hub located in Brazzaville, which serves as a shared working space and an incubator for business start-ups. Bantu Hub hosts various activities that help to share knowledge and learning about ICTs.

Lack of an independent body ensuring data protection and civil liberties

The Republic of Congo also lacks an independent body for the protection of personal data and individual freedoms on the internet in Congo.

Article 130 of Law No. 9-2009 of 25 November 2009 regulating the electronic communications sector, appears to offer an opportunity for abuse. According to a provision, “for the purposes of defence and security, the fight against paedophilia and terrorism, network operators open to the public or electronic communications operators are required... to store the data for electronic communications. Individually designated and authorised governmental agents who have a special responsibility for this task may require operators and persons to share the data that has been stored and processed.”³

The difference is that in other countries, citizen identification files are protected by independent bodies such as the National Commission for Computing and Civil Liberties (CNIL) in France, to ensure that electronic communications and data are at the

service of the citizen, and that his or her privacy and personal freedoms are not violated. This is not yet the case for the Republic of Congo. Under these conditions, one may wonder if Congolese citizens and civil society in particular are actually safe from intrusion or control on the part of public and private authorities.

Conclusion

In light of the previous analysis, while the legal framework does not encourage the practice of data protection, it is clear that it is also difficult to identify or document if cyber surveillance is taking place. The skills at the disposal of civil society are very limited to do this. It is therefore important to equip Congolese civil society organisations with knowledge of security tools to prevent intrusion into or control of their communications. Beyond civil society, the government should invest enough in training, research and development in order to develop capacity in the field of ICTs, including ensuring data protection.

Action steps

In order to do the above, the implementation of the following recommendations may be necessary.

The government should:

- Adopt laws on the protection of personal data.
- Establish an independent body for overseeing the management of personal data.
- Create a computer training and internet course in higher education.
- Invest in ICT research and development.

Civil society should:

- Create awareness and train civil society on cyber surveillance.
- Build the capacity of civil society organisations so they can secure their personal data.
- Advocate for the adoption of a more protective legal framework for civil liberties on the internet.

International partners and organisations should:

- Provide financial and technical resources to civil society for awareness-raising programmes and training on internet safety.

COSTA RICA

Universal health data in Costa Rica: The potential for surveillance from a human rights perspective



Cooperativa Sulá Batsú

Kemly Camacho and Adriana Sánchez
sulabatsu.com

Introduction

In May and June 2014, the guild for primary and secondary teachers in Costa Rica embarked on a lengthy strike over errors in the payment of their wages – the result of problems in the management of their personal data. The strike led to a lot of restlessness over the management of public computer systems in general, and showed the social, economic and political consequences of technological applications. National interest in the administration of personal data in public information systems such as health records grew.

Since the mid-20th century, Costa Rica has had a universal health care system based on a citizen partnership (or solidarity) model. In terms of data, every citizen of the country has a record containing their personal and health information. To date, most of these files are still paper-based, so that every time a patient is seen in consultation by the Costa Rican Social Security System (CCSS), the doctor should have a physical folder that includes all of the patient’s medical history.

It is easy to imagine the consequences that the manual handling of this information can generate in terms of errors, delays, loss of data and incomplete test results. Because of this, there has been an increase in legal actions brought before the Constitutional Court by Costa Ricans claiming that their right to health has been compromised. Addressing this issue is particularly important in a national context where there is strong pressure for privatisation.

Looking for a comprehensive and long-term solution, the Constitutional Court issued a ruling directing the CCSS to solve this problem by issuing a single electronic health record (EDUS) in 2012. This decision is supported by a bill passed by the Legislative Assembly in 2013, where the project has been declared a national project, and a period of five years given for its development. EDUS is described in the bill as follows:

The Single Electronic Health Record is the repository of patient data in digital form, stored

and exchanged securely, and that can be accessed by multiple authorised users. It contains retrospective, current and prospective information and its main purpose is to support the efficiency, quality and integrity of health care.¹

Due to the universal nature of the Costa Rican health care system, we can say that when EDUS is implemented it will be a national treasure of information and useful data for decision making in public health. It will help to improve the efficiency of the service, and support transparency, accountability and citizen oversight. However, EDUS may also be of high value to multiple interests outside the public health care system, such as private medical enterprises, insurers, employers, pension operators, banks, security agencies, advertising companies, the police and the judiciary, among others. Therefore, the implementation of EDUS by the CCSS is undoubtedly an important step towards strengthening the right to health among the Costa Rican population, but also represents a major national challenge in terms of the potential of this information for citizen surveillance, where the security and privacy of personal data are compromised.

Although pilots of some parts of the project² have started already, EDUS is still in the design and development phase. This is the right time to generate a national discussion – which has not happened – about what the electronic records may represent when it comes to public surveillance. With this purpose in mind, discussions have been held with national stakeholders: civil society, academia, lawyers, doctors, system designers and the CCSS. They have different perspectives on the issue, which are reflected in this report.

A human rights approach

This report focuses on citizen surveillance from a human rights perspective. It is considered a citizen’s right to know how our data is managed, what information is generated from it, and for whom. Given this approach, it is crucial that Costa Ricans participate in defining how the health record is

³ Law No. 9-2009 of 25 November 2009 regulating the electronic communications sector.

¹ Opinion prepared by the Commission on Science, Technology and Education of the Legislative Assembly (2010-2014), July 2011.

² Mainly at the primary care level (according to the proposed plan). See: portal.ccss.sa.cr/EDUS_WEB/edus/EDUS.html

built, which data will be available in the digital files, who will have access to what data, what policies and procedures are governing the privacy and security of the information, and how to ensure that this information will not be used for surveillance and other private purposes. It is also necessary to define the mechanisms of public oversight to ensure processes and agreements on the management of the information are implemented properly.

With the understanding that this is a highly technical process, both from the information technology perspective and from a medical point of view, citizen participation in building EDUS has been absent so far. The process has been defined as a specialised health and computing process, not as a process that has to do with citizen information.

The analysis of EDUS must be performed from different perspectives, which are interrelated and indivisible:

From the perspective of the right to health

As indicated in the bill, the implementation of EDUS is an essential condition to improve the exercise of the right to health in Costa Rica:

The application of this technology in the CCSS aims to reduce waiting lists in health care services, improve the quality of care and eliminate duplication of administrative procedures related to the data of the insured...

The current fragmentation of health data can be solved through the standardisation and integration of information resulting from the integration of programming languages, technology platforms and operating costs in a single system.³

From discussions with stakeholders, several important challenges have been identified:

- There is a great risk in seeing EDUS as the magic solution to the fundamental problems of the CCSS. But as noted by the Comptroller General of the Republic, following the implementation of the information system, a complete reorganisation of the institution must be undertaken, so that this public investment does not become an unnecessary expense.
- There is resistance to change by a large group of health care workers in general and doctors in particular, who consider EDUS a system that can be used to control their performance.

3 Affirmative opinion prepared by the Commission on Science, Technology and Education of the Legislative Assembly (2010-2014), July 2011.

- Cost and time represent a major risk to project success. Some of those consulted feel that there is a lack of good analysis of what this means now, and what it will mean in the future for CCSS, and raise concerns that EDUS may unbalance CCSS's budget if a good projection is not made.
- The success of EDUS will be determined by other national issues that are not under the control of the CCSS, such as access to the internet throughout the country.
- The need to think about other models where the electronic health record is administered by each citizen (as with personal bank accounts) has been proposed.

From the perspective of citizen oversight of the health care system

Having a system such as EDUS would have a high value for the control and supervision of health services, as well as accountability and transparency in the provision of universal service. A condition for this to be possible is to have accessible, updated and available information to enable citizens to learn, evaluate and propose actions to strengthen the universal health care system.

At present there is no information on the functioning of the health care system available for public examination. Those interested in exercising this role as citizens must look at various files (often with little information), request authorisation to access public information, and learn to analyse complex and disconnected data.

Until now, the development process of EDUS has not referred to the integration of information modules that allow citizen oversight. Civil society has not developed or proposed actions in this regard and seems to be unaware of the positive impact this can have on universal service and citizen surveillance.

From the perspective of citizen surveillance

In terms of citizen surveillance, it is important to mention that when the EDUS bill was discussed, the Commission on Technical Affairs of the Legislative Assembly addressed the confidentiality of data for the first time as a human rights issue that must be regulated. It indicated that the technological solution chosen for the creation of the records should have certain characteristics, including security: "The electronic record and the software solutions that interact with it must meet the criteria established for this purpose in the scientific, ethical and administrative technology field, in order to ensure integrity, confidentiality and availability in the use,

TABLE 1.		
Summary of discussions on EDUS with key stakeholders		
	Right to health	Citizen surveillance
Progress	Greater control and monitoring of the provision of health care services Greater efficiency in health care services Would strengthen universal service Facilitates the prioritisation of care according to health conditions	There is a good data protection law Favours an analysis of the health care system for decision making Facilitates accountability and transparency Allows greater control and oversight by citizens It is an opportunity to have an open database available to the public
Risks	Information should belong to the people, not the health care system. To ensure universality it is essential that all citizens have equal access to their electronic records, no matter where they are geographically. Doctors are seeing electronic records as a way to control their performance. There is resistance to change. The financial cost of the project is very high and the state does not have the resources to develop it. It also has associated long-term costs that are not contemplated. Implementation time is very short for the complete system. Need for thorough reorganisation of CCSS. Technological solution is seen as the magic solution.	Regulation: Despite the good data protection law, the regulations and accompanying implementation at national level are weak. Technology policies, agreements and conditions for the safeguarding of health data are unclear. There is no specific legal framework for health records. Internal process: There are different views within the CCSS on what to do in terms of technological development in general, and specifically when it comes to EDUS. There is a need to update staff at CCSS on the governance of health technologies, security and data privacy, open government and citizen surveillance. Development process: The CCSS, which oversees the implementation of EDUS, has emphasised the functional aspect of the system rather than the security and privacy of data and the potential of citizens monitoring the data. Civil society, health actors and decision makers are not informed about the development process of EDUS, nor have they discussed aspects of security, privacy and surveillance in these instances.
Source: Prepared by the authors.		

management, storage, maintenance and ownership of the data included in the clinical record.”⁴

However, in conversations for the preparation of this report, the issue of data security from the point of view of system functionality (user profiles related to access rights, for example) was emphasised, instead of the issue of citizen surveillance, which is not seen as an important issue in the development of EDUS. Nevertheless, you can think of citizen surveillance from two angles:

- The provision of health data for surveillance from the private sector, whose interests are very diverse, ranging from strengthening the private health schemes that compete with universal public service, to designing advertising campaigns for specific target audiences.
- The availability of health data for surveillance by the state, whose current and future interests may also be very different, starting with public safety to the repression of social and popular movements.

4 Replacement text for Article 5 of the bill, proposed by the Committee on Technical Issues of the Legislative Assembly, 2012.

The information in the health record belongs by law to the CCSS. Currently the EDUS process involves developers, database administrators (responsible for the “data centre”), support staff and health personnel who have access to different groups of data, which are handled in line with confidentiality clauses. The policies or regulations that will constitute the legal framework for the management and protection of the health records are not yet defined. The existing regulatory framework dates from 1999 and corresponds to physical files. While there is a very good law for data protection in Costa Rica, its regulations and implementation remain weak.

According to the stakeholders interviewed for this report, in the CCSS there are multiple visions of what should be done in terms of the development of information and communications technologies (ICTs), as well as computer systems, including EDUS. A discussed and shared policy, updated in the light of major issues such as the governance of health technologies, citizen surveillance, open government, security and data privacy, and the use of cloud technology, among many other urgent technological considerations, is not available.

Discussions with stakeholders show that addressing citizen surveillance has not been a priority in the development of EDUS up until now. This is compounded by the lack of understanding of the topic and the risks entailed at the technical and political levels. It is possible that the issue of surveillance might not be a priority, because it is not visible.

One can tell that the development of EDUS is caught between two forces: On the one hand the political pressure and the mandates of the Constitutional Court, the Legislative Assembly and the Comptroller General's Office in terms of the right to health; and on the other hand, the need for clearly defined policies, the strengthening of knowledge and skills, and citizen participation to address the system from perspectives that go beyond the technical aspects of computing.

Action steps

To address the issue of citizen surveillance in Costa Rica, the following steps are proposed:

- Continue the discussion with academia, the CCSS, civil society and other stakeholders to strengthen understanding of the topic of citizen surveillance in Costa Rica, specifically in the case of EDUS.
- Civil society should participate in forums where the issue is being addressed (CCSS, the legislature, the Medical Association and the Bar Association, among others).
- Raise awareness in community health committees and associations on the subject of health information systems.
- Create opportunities for citizen participation in the design, development and implementation of EDUS so that it is not perceived as a technical issue but as a matter dealing with the right to information.
- Strengthen the training of staff in the judiciary, the CCSS and the legislature on issues such as citizen surveillance, security and data privacy.
- Strengthen the technical capacity of health staff on the development of public information systems and the importance of managing privacy and data security, as well as the risk of citizen surveillance.

EGYPT

Egypt's internet surveillance: A case of increasing emergency



Leila Hassanin
lhassanin@gmail.com

Introduction

After the overthrow of Hosni Mubarak, Egypt's president for 30 years, on 11 February 2011, the country has been in political, social and economic turmoil due to an unstable transition that is still unfolding. Under Mubarak's regime the information and communications technology (ICT) sector had been a flagship for the Egyptian economy since the early 2000s. To promote its growth and competitiveness, the sector has been modernised and liberalised to the extent of becoming one of the most deregulated and promising economic sectors in Egypt.¹

The government's plan was to make Egypt a regional and global ICT outsourcing hub, on par with leading Asian countries. Egypt positioned itself as an international call centre and competed with Gulf countries in its contribution to Arab content localisation and development. In addition, the country hosts the SEA-ME-WE2, a central communication node linking the Middle East, Southeast Asia and Europe. The IT sector was a potential labour market for many income-seeking youth in Egypt who were encouraged to acquire IT skills from networking and programming to hardware assembly and ICT customer servicing.

In June 2013, 36 million Egyptians, or 43% of the population, were online – an increase of 4.79 million from 2012. Mobile diffusion has literally gone through the roof, at 116%, i.e. 98.8 million in 2013.² Egypt's population was officially estimated at 85 million in 2013.³ This means that many adult Egyptians own more than one mobile phone. Smart-

phone diffusion, however, was estimated at only 5% in 2013, on the lower end in the region.⁴

With all this computer, mobile and internet diffusion, online spaces were also being used in ways that the government did not like. Bloggers and political activists began using mobile phones to organise strikes and demonstrations. Social networks rallied youth to common political causes and blogs were used to vent discontent and alert the public and international media to infringements – political, socioeconomic, gender-related or any other. The Egypt country report in *GISWatch 2009: Access to online information and knowledge* gives examples of online activism and the government's surveillance and control of bloggers and activists.⁵ The same tactics are still being employed, although since February 2011 more repressive measures such as widespread arrests and military trials of activists and bloggers have been taking place.

Internet surveillance

In this report, internet surveillance is defined as “the monitoring of the online behavior, activities, or other changing information, usually of people, and often in a surreptitious manner. It most refers to the observation of individuals or groups by governmental organizations.”⁶

Surveillance includes scanning internet use, but is often conducted in a more intrusive manner involving interception of electronically transmitted information online through special equipment and software. Surveillance is done by direct human observation and automated means. Software captures internet traffic and analyses it. Remote access to individual computers and mobile phones is also widely used. Online open-source intelligence (OSINT), using information available through social media, blogs, forums and so forth, is another important means of information sourcing. In Egypt this is done primarily by the government.

¹ For a more detailed account on Egypt's ICT infrastructure, see Hassanin, L. (2008). Egypt. In APC, *Global Information Society Watch 2008: Access to infrastructure*. www.giswatch.org/country-report/2008/egypt

² Ahram Online. (2013, October 28). Egypt Internet users reach 36 million in June 2013: MCIT. *Ahram Online*. english.ahram.org.eg/NewsContent/3/12/84996/Business/Economy/Egypt-Internet-users-reached--million-in-June--MCI.aspx

³ World Population Review: worldpopulationreview.com/countries/egypt-population

⁴ Ipsos. (2013). Presentation at ArabNet, Beirut, Lebanon, 25 March. www.slideshare.net/IpsosMENA/ipsos-arab-net-presentation-beirut-2013

⁵ Hassanin, L. (2009). Egypt. In APC, *Global Information Society Watch 2009: Access to online information and knowledge*. www.giswatch.org/country-report/20/egypt

⁶ IT Law Wiki: itlaw.wikia.com/wiki/Internet_surveillance

Egypt has not been identified as an “enemy of the internet” by Reporters Without Borders in their 2014 report, despite the known internet surveillance of perceived critics and enemies of incumbent power holders.

Under Mubarak there was an unspoken rule of “let the people vent” as long as there was no outspoken criticism or “foul language” used against the president, his family, or any leading political figure. Citizens, and more specifically journalists and opposition figures, were allowed to voice criticism on socioeconomic and political issues. It was perceived as a political tool to disperse pent-up feelings against an authoritarian regime, and thereby prevent a more damaging building up of political dissatisfaction. Surveillance and control were targeted at specific individuals. As the events of the 25 January Revolution showed, this tactic did not help to dispel deep-set opposition to the Mubarak regime.

Yet overall access to websites was kept open, aside from repeated legal attempts to clamp down on pornographic sites. Islamists have been trying since 2009 to ban porn sites through legal rulings, the latest of which was on 30 March 2012.⁷ These efforts, however, were opposed, mostly by the Ministry of Communications and Information Technology (MCIT), as unenforceable for technical and financial reasons.⁸

It should be pointed out that the average Egyptian surfing the internet has more freedom than her or his user counterpart in the United States, for example. There is scant commercial and business surveillance, and online information is not widely used commercially. There have also been no noted stories of employers using online information against their employees or prospective job seekers.

The emergency law and internet surveillance

Egypt is in a period of political and socioeconomic transition after the popular revolution in early 2011. The initial aspiration for a more democratic system had failed due to a vacuum of order and security. The lawlessness that Egypt was subjected to after Mubarak’s stepping down from power led to

widespread public acceptance of a military hold over the country. President Abdel Fattah El-Sisi has been elected with the hope that he leads with a strong hand. Yet his political power is still in the process of consolidation, with the prospect of a clampdown on some of his most vocal and dangerous opponents continuing.

Internet surveillance in Egypt is closely tied to the “emergency law”, Law No. 162 of 1958.⁹ According to Sadiq Reza, Egypt’s rulers have used emergency rule “to assert and maintain control over the Egyptian populace at large.” This allowed them to establish a government based on emergency rule using exceptional measures of surveillance and control. The legal institution of emergency powers and their enforcement have been “a vehicle for the creation of the modern Egyptian state and a tool for the consolidation and maintenance of political power by the government,” allowing the suppression of opposition.¹⁰

The emergency law’s main stipulations are stated in its third article. The law gives the government a wide margin of control that is loosely defined as follows:

- To restrict people’s freedom of assembly, movement, residence, or passage in specific times and places; arrest suspects or [persons who are] dangerous to public security and order [and] detain them; allow searches of persons and places without being restricted by the provisions of the Criminal Procedure Code; and assign anyone to perform any of these tasks.
- To order the surveillance of letters of any type; supervise censorship; seize journals, newsletters, publications, editorials, cartoons, and any form of expression and advertisement before they are published, and close their publishing places.
- To determine the times of opening and closing of public shops, and order the closure of some or all of these shops.
- To confiscate any property or building, order the sequestration of companies and corporations, and postpone the due dates of loans for what has been confiscated or sequestered.
- To withdraw licences of arms, ammunition, explosive devices, and explosives of all kinds, order their confiscation by the government, and close arms stores, and

- To evict people from areas or isolate these areas; regulate the means of transport through these areas; and limit the means of transport between different regions.¹¹

How does the Egyptian emergency law compare with the 13 International Principles on the Application of Human Rights to Communications Surveillance?¹² The emergency law seems to be diametrically opposed to the latter.

The emergency law has been used almost uninterruptedly since 1981 in Egypt. With the ascendance of the Supreme Council of the Armed Forces (SCAF) from February 2011 to June 2012, the law continued to be in operation. After President Mubarak was deposed, the SCAF became the governing body on 13 February 2011 to oversee the transfer of power to a civilian government elected by the people. The SCAF was created in 1968 by President Abdel Nasser to coordinate military strategies and operations during wars; it was not foreseen that it would become a national governing body. However, during its six-month rule it managed to solidify its new political role through constitutional amendments.

During the SCAF’s rule there were several declarations that the emergency law would come to an end,¹³ but this never happened.¹⁴ The SCAF found it more convenient to have the emergency law at hand to engineer its political hold over the country.

With the election of President Mohamed Morsi as the Muslim Brotherhood government representative from 30 June 2012 to 3 July 2013, the emergency law was also found useful to control unrest and opposition. Notably, in two cases: once to subdue violence in public places in the port cities of Ismailia, Suez and Port Said;¹⁵ and the second time as an excuse to fight “thuggery” – but it was also used to silence the media.¹⁶

The emergency law came into full power and use with Morsi’s removal by the army under General Abdel Fattah al-Sisi on 3 July 2013. The interim government that ruled for 11 months used widespread

surveillance, control and detention against members of the Muslim Brotherhood and youth protestors in the 25 January Revolution. According to WikiThawra, security forces arrested more than 41,000 Egyptians for political transgressions¹⁷ after Morsi’s removal.¹⁸ The arrests were mainly of Muslim Brotherhood supporters, liberal youth and other secular political opponents.

El-Sisi had just been declared president when it was leaked that the Ministry of Interior had advertised an international tender for the surveillance of social networking sites frequented by Egyptians.¹⁹ Nearly simultaneously, Bassem Youssef, the leading Egyptian comic, who rose to fame with his political satire on YouTube after the 2011 revolution, ended his TV show citing unbearable pressure on himself and his family.²⁰

Conclusion

Egypt is going through unprecedented times: the recent past is not pointing to a more open, transparent political system. There is popular backing, after three years of debilitating unrest and chaos, for a strong-armed government – even at the expense of personal freedoms. In addition, the government is also wagging the fundamentalist threat card and justifying the emergency laws and online surveillance and control as a means to protect its people. In the foreseeable future, online surveillance and control will be stepped up by the El-Sisi government. The tracking of and crackdown on dissidents will intensify.

From a non-governmental perspective, at least for now, Egyptians are not seriously in danger of being mined online for commercial and business data and information. As to the availability of websites in general, it remains to be seen if they will continue to enjoy the relatively open internet access they historically had in terms of access.

However, politically speaking, Egypt seems to be looking at a lengthy period of instability with continuous repression of “divergent elements”. This means ongoing online surveillance, among other more traditional surveillance methods. Legally, surveillance has been justified by the government

7 OpenNet Initiative. (2012, March 29). Egypt’s government plans to block all online pornography. *OpenNet Initiative*. <https://opennet.net/blog/2012/03/egypts-government-plans-ban-pornography-online>; Associated Press (2012, November 7). Egypt prosecutor orders ban on online pornography. *USA Today*. www.usatoday.com/story/news/world/2012/11/07/egypt-ban-online-pornography/1689847

8 El-Dabh, B. (2012, November 11). Ministry of Communications details difficulties in porn ban. *Daily News Egypt*. www.dailynewsegypt.com/2012/11/11/ministry-of-communications-details-difficulties-in-porn-ban

9 www.scribd.com/doc/31221133

10 Reza, S. (2007). Endless Emergency: The case of Egypt. , 10(4), 532-553. www.bu.edu/law/faculty/scholarship/workingpapers/documents/RezaSo31208rev.pdf

11 Emergency Law, Law No. 162 of 1958.

12 <https://necessaryandproportionate.org/text>

13 Ahram Online. (2012, May 31). Egypt state of emergency ends for the first time in 30 years. *Ahram Online*. english.ahram.org.eg/NewsContent/1/64/43368/Egypt/Politics-/Egypt-state-of-emergency-ends-for-first-time-in-.aspx

14 Shenker, J. (2011, September 16). Egyptians rally in Tahrir Square against return of emergency laws. *The Guardian*. www.theguardian.com/world/2011/sep/16/egyptians-rally-tahrir-square-laws

15 BBC. (2013, January 28). Egypt unrest: Morsi declares emergency in three cities. *BBC*. www.bbc.com/news/world-21224643

16 Ahram Online. (2012, August 28). President Morsi considering new emergency laws: Justice Minister. *Ahram Online*. english.ahram.org.eg/NewsContentP/1/51440/Egypt/President-Morsi-considering-new-emergency-laws-jus.aspx

17 From 3 July 2013 to 15 May 2014.

18 WikiThawra: Statistical Data Base of the Egyptian Revolution. wikithawra.wordpress.com/author/wikithawra

19 Gamal el-Deen, K. (2014, June 3). Egypt to impose surveillance on social networking sites. *PressTV*. www.presstv.ir/detail/2014/06/03/365344/egypt-to-impose-surveillance-on-social-networking-sites

20 Hendawi, H. (2014, June 2). Egyptian satirist Bassem Youssef ends his TV show. *The Boston Globe*. www.bostonglobe.com/news/world/2014/06/02/egyptian-satirist-bassem-youssef-ends-his-show/7tKEXoyMhjKFVsYcSyojgI/story.html

since 1958 as an attempt to secure the country internally from Islamists and externally from its main enemies, Israel and Iran, and their cronies.

This “state of emergency” was lifted after 11 February 2011, when Mubarak was deposed, but re-instated in September 2011 by the SCAF. The state of emergency gives the government a free hand to suppress meetings, demonstrations and strikes and allows imprisonment, confiscation and detention without a warrant or additional legal justification. It also gives a green light to any form of online surveillance and control.

With El-Sisi as president, there does not seem to be any reason why the emergency law should cease. On the contrary, with the Islamist threat, the new government has more of an alibi to extend it. Egypt’s new government is also using the argument that in Europe and the United States, widespread internet surveillance of citizens is happening.²¹

Action steps

Free online speech is not looking at a promising near future in Egypt. With enormous political, economic and social challenges at play, it is not foreseeable that the emergency law, and consequently internet surveillance, will be reined in any time soon. In fact, recent indications point to the opposite.


Are there any concrete new actions steps? Not really. What can be said is that:

- Journalists, bloggers and civilians have been trained by various international organisations, including Reporters Without Borders, on communication and data protection for years.²²
- Individual surveillance circumvention is notoriously hard and leaky. Egypt is among many countries that face online surveillance and, even with more stable political systems, governments tend to raise the spectre of “terrorism” to justify widespread surveillance, as has been the case with the National Security Agency (NSA) in the US. As the surveillance technology is easily acquired by government agencies and is hard to detect by civilians, it remains doubtful that online surveillance will decrease. In addition, internet service providers (ISPs), search engines, social networks and the like are under legal pressure to comply with governmental requests for data disclosure.

What does that mean for the activist? The usual cat and mouse game of trying to come up with codes and dodging being tracked by encrypting connections. Any code or tracking evasion will be found out sooner or later, so the name of the game is to stay ahead, change often – or maybe it is time to look for a less surveilled communication channel?

ETHIOPIA

The potential impact of digital surveillance on the uptake and use of the internet in Ethiopia



Ethiopian Free and Open Source Software Network (EFOSSNET)
Abebe Chekol
abechekol@yahoo.com

Introduction

Ethiopia is the oldest independent country in Africa and one of the oldest in the world.¹ Politically, Ethiopia is a federal republic under its 1994 constitution. The current ruling party, the Ethiopian People’s Revolutionary Democratic Front (EPRDF), has governed Ethiopia since 1991. Since taking power, the EPRDF has led ambitious reform efforts to initiate a transition to a more democratic system of governance and decentralise authority. Although still considered one of the world’s poorest countries, the second most populous nation in Africa has recorded fast growth over the last five years. In 2012/2013, its economy grew by 9.7%, which made it one Africa’s top-performing economies.²

The latest survey from the World Economic Forum puts Ethiopia at 130th out of 148 countries in its Networked Readiness Index.³ The index measures the ability of economies to leverage information and communications technologies (ICTs) to boost competitiveness and well-being. Internet usage in Ethiopia is still in its infancy, with less than 1.5% of Ethiopians connected to the internet and fewer than 27,000 broadband subscribers countrywide.

In the context of the International Principles on the Application of Human Rights to Communications Surveillance,⁴ this report assesses the ICT development policy and legal environment in Ethiopia, and how digital surveillance could impact on this.

Policy and legal frameworks

Article 26 of the 1994 Ethiopian Constitution states with regard to the “Right to Privacy”: “All persons have the right to the inviolability of their letters, post and communications by means of telephone,

telecommunications and electronic devices.” It further states: “Public officials shall respect and protect these rights. They shall not interfere with the exercise of these rights except in compelling circumstances and in accordance with specific laws which aim to safeguard national security, public safety, the prevention of crime, the protection of health, morals and the rights and freedoms of others.”

There are, therefore, specific laws that allow public officials to interfere with the exercise of the rights of individuals granted in the constitution. These laws are as follows:

*Anti-Terrorism Proclamation No. 652/2009.*⁵ Article 14 of the Anti-Terrorism Proclamation, on “Gathering Information”, proclaims: “To prevent and control a terrorist act, the National Intelligence and Security Service may, upon getting a court warrant: a) intercept or conduct surveillance on the telephone, fax, radio, internet, electronic, postal and similar communications of a person suspected of terrorism; b) enter into any premise in secret to enforce the interception; or c) install or remove instruments.”

*Prevention and Suppression of Money Laundering and Financing of Terrorism Proclamation No. 780/2013.*⁶ Under “Investigative Techniques”, part 4 of Article 25 of this Proclamation declares: “For the purpose of obtaining evidence of money laundering or financing of terrorism or tracing proceeds of crime, the judicial organs may authorize crime investigation authorities, for a specific period, among others, to access computer systems, networks and servers; and to place [an individual] under surveillance or to intercept communication; and to intercept and seize correspondence.”

*Telecom Fraud Offence Proclamation No. 761/2012.*⁷ Under this law, evidence gathered through interception or surveillance in accordance with the Criminal Procedure Code and other rel-

21 Amnesty International. (2014, June 4). Egypt’s plan for mass surveillance of social media an attack on internet privacy and freedom of expression. *Amnesty International*. www.amnesty.org/en/news/egypt-s-attack-internet-privacy-tightens-noose-freedom-expression-2014-06-04

22 Reporters Without Borders. (2014). *Enemies of the Internet 2014*. 12mars.rsf.org/wp-content/uploads/EN_RAPPORT_INTERNET_BD.pdf

1 www.ethioembassy.org.uk/fact%20file/a-z/history.htm
2 World Bank. (2012). *World Atlas*. www.worldatlas.com/aatlas/world.htm
3 Bilbao-Orsorio, B., Dutta, S., & Lanvin, B. (Eds.) (2014). *The Global Information Technology Report 2014: Rewards and Risks of Big Data*. Geneva: World Economic Forum, INSEAD, and Johnson Graduate School of Management, Cornell University.
4 <https://en.necessaryandproportionate.org/text>

5 Federal Democratic Republic of Ethiopia. (2009). Anti-Terrorism Proclamation No. 652/2009.
6 Federal Democratic Republic of Ethiopia. (2013). Proclamation on Prevention and Suppression of Money Laundering and Financing of Terrorism, Proclamation No. 780/2013.
7 Federal Democratic Republic of Ethiopia. (2012). Telecom Fraud Offence Proclamation No. 761/2012.

evant laws will be admissible in court in relation to telecom fraud offences.

Key issues

There has been a proliferation of counter-terrorism legislation globally following 9/11, which is considered a turning point in the history of counter-terrorism.⁸ As indicated above, Ethiopia also passed an anti-terrorism law in July 2009. Since its promulgation, this law and its application have been controversial. A recent BBC article⁹ published on 25 March 2014, referring to a Human Rights Watch (HRW) report on Ethiopia, reported the Ethiopian government's use of imported technology (mainly from European and Chinese firms) to undertake surveillance on the phones and computers of its perceived opponents. The report points out that given that all phone and internet connections in Ethiopia are provided by a state-owned company, the government has the power to monitor communications and have access to all call records of all telephone users in the country. This includes access to recorded conversations that can be used in the interrogation of suspects. According to the HRW report, the government has extended its surveillance to Ethiopians living overseas. Ethiopians living abroad (mainly in the United Kingdom and the United States) have accused the government of using spy software on their computers.

In terms of the legality and legitimate aim of such action, the government has issued the anti-terrorism law on the grounds of the clear and present danger of terrorism in Ethiopia, coupled with the inadequacy of ordinary laws to deal with this reality. Furthermore, it also argues that the United Nations Security Council resolution 1373 (2001) requires countries (including Ethiopia) to pass the law.¹⁰ However, given the fact that digital surveillance is a highly intrusive act that interferes with the rights to privacy and freedom of opinion and expression, the proportionality of its application is feared to undermine the democratic process.

The Ethiopian Television and Radio Agency hosted a debate¹¹ in August 2013 among political parties on a range of issues relating to the Ethiopian anti-terrorism law and its application. While

the incumbent ruling party argues the legitimacy of this law on the grounds of the clear and present danger of terrorism in Ethiopia, the opposition parties argued the impact of this law on democratic rights and processes in the country. Furthermore, this can be considered a means of popularising the law to create awareness among the wider public, given there is little evidence of the level of awareness among the public in general on the use and scope of digital surveillance techniques and powers stated in the law. There is also little awareness both among civil society and the legislature of international principles such as user notification, where individuals should be notified of a decision authorising communications surveillance with enough time and information to enable them to appeal the decision, or the need for independent public oversight mechanisms.

With regard to the international principle on the integrity of communications and systems, where states should not compel service providers or hardware or software vendors to build surveillance or monitoring capability, the anti-terrorism law declares in Article 14 that “any communication service provider shall cooperate when requested by the National Intelligence and Security Service to conduct the interception.”

A recent article in *Addis Fortune*¹² reflects concern for privacy and data protection amidst the growing use of the internet in Ethiopia and global digital intrusion. In this context, the international principle on safeguards for international cooperation suggests applying the higher level of protection for individuals where there are agreements between states. Furthermore, the international principle on safeguards against illegitimate access suggests that states should enact legislation criminalising illegal communications surveillance by public and private actors. In both instances, there is concern that Ethiopia does not have a legal framework that could make authorities liable for a breach of user data and cross-border cyber-security issues. This occurs in the context of a lack of concern from Ethiopian internet users on the subject, and is one important gap that needs to be addressed by the government. Such a gap is also noted in the Information and Communication Technology Policy of 2009, which clearly recognises the need, among other cyber-oriented laws, to issue a data protection law.

As the number of internet users increases over time – the government plans to increase it to 3.69 million by the end of the Growth and Transformation Plan (GTP) period in 2015¹³ – the data privacy of internet users in Ethiopia will undoubtedly become crucial if this sector is to contribute its share to the economy. A recent report from the McKinsey Global Institute¹⁴ indicates that, as in many countries in Africa, the internet's contribution to Ethiopia's gross domestic product (GDP) is 0.6%, which is low compared to the leading countries of Senegal (3.3%) and Kenya (2.9%). Ethiopia falls under the category of countries that perform below their weight, along with Angola, Algeria and Nigeria.

It would therefore be important to assess the implications of digital surveillance on the growth of ICT-based services such as e-commerce¹⁵ and e-government,¹⁶ which are both key sectors given prominent attention in the implementation of the national ICT policy in Ethiopia. The Ministry of Communications and Information Technology is currently implementing the e-government strategy, which aims to develop more than 200 e-services (currently in different phases of implementation) and get 20% of government departments online.¹⁷ There is also evidence of the growing use of ICTs in business, with internet use in companies in Ethiopia rated at 3.6 on a 0 to 7 index range.¹⁸ It is therefore important to review the impact of laws on the growth and use of the internet in various sectors.

For example, although the proclamation on the “Prevention and Suppression of Money Laundering and Financing Terrorism” does not explicitly address e-commerce, there is a need to assess whether the provisions of the law have an impact on e-commerce broadly and electronic fund transfers specifically. Similarly, e-government could be affected by the legislation mentioned above in both positive and negative ways, which requires further investigation. While the intense focus on improving data collection and information practices and systems may contribute to the establishment of government-wide technical standards and best practices that could facilitate the implementation

of new and existing e-government initiatives, it could also promote the use of secure web portals to help ensure the data integrity of transactions between the government and citizens and business. However, concerns about the potential abuses of data collection provisions could jeopardise citizen enthusiasm for carrying out electronic transactions with the government.

With the evolution of the internet and digital communications, new trends are emerging and regulatory interventions are becoming even more complex in the context of these emerging issues – such as the revelations of widespread internet surveillance, human rights imperatives, the line between privacy versus security, and managing critical resources that make the internet possible. In this regard, governments should demonstrate greater transparency as regards their practices in the collection of personal data, taking into account the considerations of national security, citizen rights and public accountability.

Conclusions

The World Summit on the Information Society (WSIS) Action Plan recommends “cooperation among the governments at the United Nations and with all stakeholders as appropriate to enhance user confidence, build trust, and protect both data and network integrity; consider existing and potential threats to ICTs; and address other information security and network security issues.” Though belated in realising the legal framework in changing circumstances, such as the growing ubiquity of the internet, the Ethiopian government has recently started working on these issues. Laws that regulate online behaviour and transactions are in the pipeline. A cyber-crime law, drafted by the Information Network Security Agency, and an e-commerce law, drafted by the Ministry of Communication and Information Technology in collaboration with the United Nations Economic Commission for Africa (UNECA), are examples. In this regard, the Conference of African Union Ministers of Justice adopted the African Union Convention on Cybersecurity and Personal Data Protection in May 2014. The Convention, which was drafted by UNECA in collaboration with the African Union Commission, and which has been reviewed through a series of sub-regional consultations with regional economic communities, is expected to be tabled before the African Union Heads of State and Government for ratification later this year. The Convention covers four areas, namely cyber security, combating cyber crime, electronic transactions (e-transactions), and

8 Kassa, W. D. (2013). Examining Some of the Raisons D’Être for the Ethiopian Anti-Terrorism Law. *Mizan Law Review*, 7(1).

9 BBC. (2014, March 25). Ethiopia uses foreign kit to spy on opponents – HRW. *BBC*. www.bbc.com/news/world-africa-26730437

10 United Nations Security Council Resolution 1373 (2001), adopted by the Security Council at its 4385th meeting, on 28 September 2001.

11 www.youtube.com/watch?v=-g5jhwPAt4U

12 Yilma, K. (2012, June 5). Unprepared Ethiopia faces privacy intrusion. *Addis Fortune*. addisfortune.net/columns/unprepared-ethiopia-faces-privacy-intrusion

13 Ibid.

14 McKinsey & Company. (2013). *Lions go digital: The Internet's transformative potential in Africa*. Johannesburg: McKinsey Global Institute.

15 Commercial transactions on the internet, whether retail business-to-customer or business-to-business or business-to-government, are commonly called electronic commerce, or “e-commerce”.

16 E-government involves using information technology, and especially the internet, to improve the delivery of government services to citizens, business, and other government agencies.

17 McKinsey & Company. (2013). Op. cit.

18 Ibid.

data protection and privacy. Countries will therefore be expected to amend their cyber security and data protection laws to bring them in line with the Convention.

This will help harmonise the existing legislation discussed above with respect to digital surveillance. While many of the provisions related to the surveillance and investigatory powers of law enforcement have raised concerns within the privacy and civil liberties communities, there is also the potential impact that this harmonisation can have on the growing use and application of ICTs in business through e-commerce, and government services through e-government. The challenge is to strike the balance on the use and application of these laws between the need for counter-terrorism measures and the imperative the respect to rights granted in the constitution.

Action steps

While close to 90 countries have so far issued data protection laws, Ethiopia has not. It is noted above that the Information and Communication Technology Policy of 2009, however, clearly recognises the need, among other cyber-oriented laws, to issue a

data protection law.¹⁹ Therefore there is a need for Ethiopia to develop a data protection and privacy law that can harmonise existing laws that affect these rights.

However, as much as establishing the requisite legal framework, raising public awareness about human rights and fundamental freedoms is very crucial. The Ethiopian Human Rights Commission is one stakeholder in this area in Ethiopia. It was established by law with the objective of “educating the public with the view to enhance its tradition of respect for and demand for the enforcement of human rights [through the public] acquiring sufficient awareness regarding human rights.” The Commission needs to scale up its efforts in an era where the human right to privacy is being strongly challenged with the evolution of new and emerging technologies – and new state imperatives, such as countering terrorism.

The laws related to cyber crime and e-commerce need to be reviewed, not only to attune them to emerging challenges, but to address the challenges of data protection and privacy in order to build confidence and trust in the use of ICTs in general and the internet in particular.

Front Page International
Demba Kandeh
www.frontpageinternational.wordpress.com

Introduction

Surrounded by Senegal on three sides and the Atlantic Ocean to the west, The Gambia is the tiniest country in mainland Africa.¹ It is home to 1.8 million people with a land mass of about 11,300 square kilometres. The majority of the population are farmers with a literacy rate of about 38%. Since independence from Britain in 1965, The Gambia so far has had two presidents: Dawda Kairaba Jawara, who led the country to independence and remained in power until he was overthrown in a “bloodless coup” in July 1994, followed by then-Lieutenant Yahya AJJ Jammeh.²

Jammeh’s government criticised Jawara for his slow economic progress in general, and, in a quest to avert what it called “retrogression”, investment in information and communications technologies (ICTs) was considered key.³ Given the opportunity presented by an already relatively good telecommunication network, the government and the UN Development Programme (UNDP) launched The Gambia’s Internet Initiative project in 1998.⁴ The project was aimed at opening a gateway to connect The Gambia to the internet, and to build a national backbone and points of presence (POPs) around the country to provide high-speed internet access to major centres. It also sought to encourage and nurture competition and private sector participation in internet provision. This programme was monitored by a USD 100,000 three-year support project. Project assessment reports for the period 1998-2002 showed that major developments had not just been made in internet connectivity, but that it “increased ICT investment and start-up operations, creating a context of advanced access and

technological capacity.”⁵ However, more than a decade later, all indications are that those gains were never consolidated.

Policy and political background

The internet and other public utilities are regulated under The Gambia Public Utilities Regulatory Authority Act 2001.⁶ The Act, among other things, called for the creation of a public utilities regulatory body. Consequently the Public Utilities Regulatory Authority (PURA) was established to regulate the activities of service providers of some public utilities in various sectors of the economy. The Act to establish the authority only came into force towards the end of 2003, while PURA was formally set up a year later, in 2004. The establishment of PURA was supported by a study on the appropriate regulatory framework for the sector, which included private sector participation, and was funded by the Public Private Infrastructure Advisory Facility (PPIAF) through the World Bank. Nevertheless, expert opinion on PURA in the telecoms sector seems divided, with many being pessimistic of the body’s capabilities *vis à vis* its responsibilities. “PURA is not equipped enough to live up to its challenge of ensuring the proactive and effective implementation of sound policies governing the regulated sectors, such as telecommunications, among others, in a predictable, equitable and transparent manner,” said an expert on the sector who preferred anonymity.

The government of The Gambia, through the Ministry of Communication Infrastructure and Information Technology, pays a lot of attention to ICTs and works toward growth in the sector, most notably when it comes to information technologies (IT). The government believes IT can be of great value in various economic sectors of the country if used wisely, especially for decision making. However, it is evident that the state is fearful of the consequences of the free and uninterrupted flow of information, especially through the use of new technologies – a

¹⁹ Yilma, K. (2012, June 5). Op. cit.

¹ History World, History of The Gambia. www.historyworld.net/wrldhis/plaintexthistories.asp?historyid=ad47

² BBC News, The Gambia country profile. www.bbc.com/news/world-africa-13376517

³ Status of ICT Access, Usage and Exploitation in The Gambia, Final Report, September 2007, available at the Gambia National Library.

⁴ NIC Gambia. www.nic.gm/htmlpages/gm-internet.htm

⁵ Pro-PAG/CUTS Partnership. (2008). *Strengthening Constituencies for Effective Competition Regimes in Select West African Countries: Preliminary Country Paper (PCP) – The Gambia*.

⁶ www.pura.gm

fundamental reason for the tight regulation of the sector.

Communication surveillance in The Gambia

During May 2006, the government obtained the names, addresses, phone numbers and email addresses of all subscribers of a very popular controversial online news site.⁷ The government described the *Freedom Newspaper* subscribers as “informers”, and went on the rampage to arrest and detain them. Several people, most of them journalists, human rights activists and politicians, were arrested and detained for weeks, but released without any court charges. Reports emerged later that the person who hacked into the *Freedom Newspaper* site was a British Telecom client using the IP address of an internet user based in the UK city of Southampton. The hacker erased all of the paper’s content and replaced the welcome page with a message purportedly signed by Pa Nderry M’bai, the publisher and editor. The message said: “I have decided to stop producing the *Freedom Newspaper* as I have pledged an allegiance with my brother Ebou Jallow to join the APRC election campaign.” A former army captain, Jallow used to be the spokesman for President Jammeh’s military junta. The APRC is the president’s party, the Alliance for Patriotic Reorientation and Construction.

M’bai is a self-exiled Gambian journalist.⁸ He launched the *Freedom Newspaper* in early 2006. It is very critical of Jammeh and his government. M’bai used to work for the then tri-weekly newspaper, *The Point* (now a daily paper), co-founded by slain Gambian journalist Deyda Hydara.

The fake message added: “This is a list of the people that were supplying me with information.” It was followed by the names and details of all those who had set up user accounts for the site. With help from the US company that hosts the site, and from Reporters Without Borders, M’bai managed to regain control of the site.

Following the hacking, on 24 May 2006, under the headline “Freedom Newspaper informers exposed”, the pro-government *Daily Observer* newspaper published M’bai’s photo on its front page, describing his paper as “subversive”.

This was met with an outcry from activists. “This case of hacking is serious and revolting,” a statement released by Reporters Without Borders said,

adding that the climate in which Gambian journalists work is totally poisonous.

“Not only was the reputation of a journalist besmirched but a large number of internet users have been put in danger. And it is absolutely astounding that the *Daily Observer* became an accomplice by publishing the list of these so-called informers and describing them as ‘subversive’,” it further noted.

Since this incident in 2006, the government has worked tirelessly to help tighten its control over the telecommunications sector as it grows. The services of experts, analysts and consultants from far and wide were contracted with a view to produce a “legal and regulatory framework” that keeps a firm grip on this emerging sector. The government’s efforts have since yielded dividends, and a number of policies and programmes were introduced with a view to enhance growth in the sector. The most important in our context among the “innovations of the government” was the enactment of the Information and Communications Act 2009.⁹

The Information and Communications Act (ICA) 2009 was adopted with a view to addressing the convergence of the telecommunications, broadcasting and information technology sectors, including the internet. It is important to note key contents of the law. The ICA has 252 provisions and is divided into five chapters: preliminary matters; the regulation of information and communication systems and services; information society issues; regulatory provisions for broadcasting content; and miscellaneous matters. In addition to telecommunications and broadcasting regulation, the Act also effectively deals with cyber crime and the processing of personal data.

The ICA places the regulation of the telecommunications and broadcasting sectors under PURA.

A detailed analysis of the ICA and other media laws in The Gambia by Article 19, an independent international NGO focusing on freedom of expression and media issues, illustrates deep flaws in the legal framework. Article 19 noted at the outset that entrusting the same entity with the regulation of sectors as widely different as water and electricity services and the telecommunications sector is confusing and undesirable. It therefore recommended the creation of a separate public authority with powers to regulate the telecommunications and broadcasting sectors.

Article 19 highlighted as its main concern that the ultimate authority in respect of telecommunications and broadcasting licensing is the minister (i.e. the executive). It pointed to problematic clauses

in sections 7(2), 22, 23, 27, 215, 226, 230 and 232 to 236 in this regard. Section 230(1), for example, provides that “the Minister, on the advice of the Authority, shall issue broadcasting licences in sufficient numbers to meet the public demand for broadcasting services.”

Similarly, sections 232 to 236 provide that upon recommendation by the Authority, the Minister “may” renew, revoke or suspend a broadcasting licence. PURA therefore merely has an advisory role, while the ultimate decision-making power rests with the minister. This, however, contradicts international standards on freedom of expression, which require that all public bodies exercising powers in the areas of broadcast and/or telecommunications regulation be institutionally independent so as to protect them from undue political or commercial interference.

But what is more serious in our case is Section 138 of the ICA, which gives sweeping powers to the national security agencies and investigating authorities to monitor, intercept and store communications in unspecified circumstances. The section further provides that the minister may require information and communication service providers to “implement the capability to allow authorised interception of communications.”

While Section 138 essentially raises issues of privacy of communications, and the protection of private life more generally, it has serious implications for communications. It seems to legitimise general public concerns over the privacy of their “private” communication. This raises more serious issues of surveillance in a country that is already notorious for violations of basic human rights. And indeed, even in places such as The Gambia where internet penetration is more limited than in more developed countries, particularly in the West, the ability of individuals to freely communicate on the internet, using email, social media networks or other web platforms, has become an essential aspect of our daily lives. There are four times more people on the internet¹⁰ in The Gambia today than the population of the capital city of Banjul.¹¹ In this context, unchecked internet surveillance or “monitoring” but also the monitoring of communication in general is perhaps one of the greatest dangers to privacy both online and offline.

Privacy activists and other rights defenders will therefore argue that any restriction on freedoms

must be strictly measured against the three-part test laid down under international law. Those limitations must be clearly defined by law, pursue a legitimate aim and be proportionate to the aim pursued. The interception of private communications in particular should be limited only to the investigation of serious criminal activity.

One can safely argue that despite the need to investigate serious crimes, there is an obvious danger that such unchecked and open powers given to a powerful arm of government (the executive) can be easily abused unless clearly constrained by law. We can conclude that the provisions of the ICA in general and this section in particular substantially fail to meet the requirements of international law as indicated above.

For Article 19, given the breach of the requirement of legal certainty, it is impossible to predict under Section 138 in which circumstances the authorities may intercept or monitor communications.¹² The only exception to this is perhaps Sub-section 2, which bizarrely provides that a user or subscriber fearing for his life or physical integrity may authorise such interception, rather than a judicial authority. This is also a very extreme situation, and unwarranted.

It is clear that Section 138 does not provide for monitoring or interception to be authorised *only* by a judge nor that it should at all times be in compliance with the requirements of necessity or proportionality. Against this background, the fact that information and communication service providers may be required by the minister to “implement the capability to allow authorised interception” is not just less than ideal, but detrimental to the free flow of communications and privacy.

On 3 July 2013, the National Assembly amended the ICA, stipulating a 15-year jail term or a fine of three million Gambian Dalasi (GMD) (approximately USD 75,000), or both a fine and imprisonment, for the offence of spreading “false news” against the government or its public officials on the internet.¹³

While the amendment imposes penalties for “instigating violence against the government or public officials,” it also targets individuals who “caricature or make derogatory statements against officials” or

7 The Daily Observer. (2006, May 24). Gambia: Freedom Newspaper Informers Exposed. *AllAfrica*. allafrica.com/stories/200605250666.html

8 Reporters Without Borders. (2006, May 30). Online newspaper hacked, editor smeared and subscribers threatened. *Reporters Without Borders*. archives.rsf.org/article.php3?id_article=17842

9 www.wipo.int/wipolex/en/details.jsp?id=10478

10 Trading Economics, Internet users in Gambia (2011). www.tradingeconomics.com/gambia/internet-users-wb-data.html

11 Access Gambia, Population Figures for Gambia. www.accessgambia.com/information/population.html

12 Article 19. (2012). *The Gambia: Analysis of Selected Laws on Media – Overview*. www.article19.org/resources.php/resource/3043/en/the-gambia-analysis-of-selected-laws-on-media

13 Article 19. (2013, July 10). The Gambia: New internet law furthers government crackdown on free expression. *Article 19*. www.article19.org/resources.php/resource/37152/en/the-gambia-new-internet-law-furthers-government-crackdown-on-free-expression#sthash.qisIU1J.dpuf

“impersonate public officials.” Activists and rights groups have criticised the amendments severely.¹⁴

The National Assembly had previously come under heavy criticism from activists and rights groups for an amendment of Section 114 of the Criminal Code which raised the jail term of six months or a fine of GMD 500 (about USD 17), or both, up to five years or a fine of GMD 50,000 (about USD 1,700) for persons convicted of giving false information to a public official.¹⁵

According to Article 19, the legal framework for ICTs, including private communications, should not allow state authorities to assume sweeping powers over ICT operators and providers – in particular their equipment or content going through their networks – in undefined circumstances, including in an emergency.¹⁶

Conclusion and action steps

It is evident that the government of The Gambia fears the opportunities for transformative democracy presented by ICTs and the internet in particular. The government is therefore struggling daily to maintain a firm grip on ICTs and the internet. This is also corroborated by the fact that the government has blocked over 20 online news websites and

pages. The popular instant messaging and calling service Viber is also blocked. There are also indications that proxies such as Anonymouse.org and the Tor browser are being blocked in the country. The situation is therefore similar to what occurs in countries such as China, Ethiopia and Iran, as well as some other parts of the Arab world.

The government has denied any involvement in filtering and points to services providers who are suspected of hiding behind vague government regulations. Citizens and human rights groups generally blame the government for the status quo. It is obvious that unless there are concerted efforts, the situation is not likely to change, at least not in the near future.

Advocacy efforts should be directed toward the de-legislation of the ICA Act, as well as the 2013 amendments. This should be followed by strategic planning to create a well-regulated sector. Special efforts should be directed at reviewing and amending Section 138 to bring it more closely in line with international standards for the protection of human rights. In particular, it should be made clear that interception can only be authorised by a judge for the purposes of investigating serious crimes and subject to the requirement of proportionality.

HUNGARY

Data retention and the use of spy software in Hungary



Éva Tormássy
tormassyeva@gmail.com

Introduction

After a series of coordinated suicide attacks in Madrid in 2004 and in central London in 2005, the European Union reacted by passing the so-called Data Retention Directive in 2006. Hungary as a member state of the European Union was obliged to introduce mandatory telecommunication data retention – that is, the retention of data generated or processed through the provision of publicly available electronic communications services or by public communications networks. As a result of the Data Retention Directive, all telecommunication service providers in Hungary have to collect and store so-called metadata, or data which shows who, when, where and with whom anyone tried to communicate or successfully communicated via email or phone. The Directive gave the freedom for the member states to choose the period of time their telecommunication service providers have to keep the data which, also according to the Directive, should be made available to the competent national authorities in specific cases when a suspicion of serious crime arises (e.g. an act of terrorism). According to the Directive, data made available for the purpose of the investigation, detection and prosecution of crimes should only be about the fact (who, where, when and with whom email was exchanged or communication took place by mobile phone), not the content. However, when the directive was implemented, Hungary failed to make the distinction between the fact and the content of the data. There is therefore a danger that the providers kept the content of the communication and the authorities received more information about certain citizens than they should have. The only good news for Hungarian citizens at the time of the implementation was that the decision makers chose the shortest possible period which was allowed, meaning the service providers have to keep the metadata for six months only in Hungary.

New times, old habits

Hungary was a member of the Soviet bloc before 1989, a so-called communist country where the surveillance of citizens by different authorities had a long history, even if this history was not as bloody as in certain other member states of the communist bloc. Most citizens had little personal experience of surveillance, and when the Berlin Wall collapsed in 1989 and the doors to the secret archives opened, many people must have been surprised how much the state knew about them and their private lives.

As a consequence of this, the newly adopted laws after the collapse of communism were very careful when it came to citizens' privacy and respecting the right to a private life. Before Hungary adopted the Data Retention Directive, the law on data retention was tied to judicial authorisation which was given in cases of suspicion of serious crimes. The police or any other authority had to submit a formal request for receiving the data from the service providers; however, with judicial authorisation they had the right to collect the data for three years.

The judicial authorisation was a strong safeguard which disappeared with the implementation of the Data Retention Directive. The implementation took place in 2008, under a socialist-liberal government, and the competent ministry which was responsible for the implementation chose the shortest possible period for data retention because the minister was delegated by the liberal party. But that was the last good news for Hungarian citizens.

The implementation forgot about the basic safeguards in the law. The text was not clear when it came to not storing the content of the data and did not mention the necessity of judicial authorisation, court oversight or any external supervisory mechanism. The law also forgot to prescribe the obligation to inform the person concerned about the use of his/her data, and to inform the person who was under surveillance, as well as the obligation to destroy the data after the end of legal proceedings. Lastly, there was nothing about who guards the guardians: who inspects or monitors the process of destroying the data when the retention time is over. Possibly the worst thing of all was that the authorities were granted direct access to the telecommunication

¹⁴ Joof, M. S. (2013, July 8). The Gambia's Internet Law: RSF very disturbed, Amnesty International shocked. *Front Page International*. frontpageinternational.wordpress.com/2013/07/08/the-gambias-internet-law-rsf-very-disturbed-amnesty-international-shocked

¹⁵ JollofNews. (2013, May 8). Amnesty Int'l Denounces Gambia's Harsh Criminal Law. *JollofNews*. www.jollofnews.com/.../3827-amnesty-intl-denounces-gambias-harsh-cri

¹⁶ Ibid.

service providers' data rooms (a special technical connection has been set up between the companies and the national security authorities). And the security men sitting on the two sides of the table all knew each other from the past and understood each other. Hungary, which has never been able to get rid of its past of secret agents and spies, started its own time travel back into that past.

When Big Brother watches you

In his famous book 1984, George Orwell wrote that "Who controls the past controls the future." This quote – even if it was related to the communist era – expresses the basic societal concern about any state surveillance well. This recognition led many human rights activists to fight against the Data Retention Directive and its national implementation all over Europe. In Hungary, the Hungarian Civil Liberties Union (HCLU) protested against the implementation of the Directive in many ways – without significant result, effect or echo. They submitted amendments to the national law through members of parliament, published articles, and organised civic actions in which citizens asked the service providers to inform them whether they were under surveillance or not, but all attempts remained unsuccessful.

On the other hand, the conservative Hungarian government, which was first elected in 2010 and for a second time in April 2014, became more and more successful in controlling citizens. They knew well that those who control the past control the future. Hungary's parliament moved to increase surveillance of high-level public officials, with the modification of the National Security Law on 24 May 2013. It was designed to allow the state to identify any risks that could lead to someone influencing or blackmailing a person under surveillance, which would in turn cause state security issues, the law says. The range of positions in the secret service's focus is detailed: the people subject to such surveillance are ambassadors, state secretaries, heads of administrative bodies and councils, the management of parliament, the head of the military forces and army generals, police commanders and superintendents, and heads and board members of state-owned companies. The person in question needs to sign an approval for the surveillance to be allowed. Refusal to sign means they lose their jobs. The modification has raised concerns on the part of the ombudsman and civil rights groups, and sparked comments that the secret service's reach into people's private lives would now be "total". The bill also lifts the earlier requirement of a court nod for the secret gathering of information on people

by opening their letters, making audio and video recordings or searching and bugging their homes.

Apart from allowing surveillance of a selected group of people without letting them seek legal remedy, the law provides no regulations that limit who can see the information, what can be done with it, or how long it can be stored. The law also allows for employees to be fired for conduct outside the workplace, for as yet unspecified reasons. It means that Hungary now allows investigation of particular individuals without any need to demonstrate a specific reason why every aspect of a person's life must be reviewed. That is unusual in democratic states. The new national security law has really created an Orwellian landscape in Hungary.

Hungary's ombudsman for basic rights, Mate Szabo, declared that the bill should give those under surveillance the right to appeal the matter and seek legal remedy against any encroachment of their rights in the process. But this remark was ignored in the final version of the law. The HCLU said that the new bill is unconstitutional even if the person in question signs a document to give their consent to the surveillance. The ombudsman is the only one who has the right to appeal to the Constitutional Court – civil rights groups do not. Last June, Szabo initiated a constitutional review. He raised concerns over a lack of external control over the monitoring process and the fact that agencies would not be required to provide a concrete reason or aim for the monitoring activity, which would give the state an unfair power advantage over the individual targeted in the surveillance. Despite the protests, the amendment was enforced on 1 August 2013. However, while the Constitutional Court decision made in March 2014 repealed the amendment, a new parliament set up in late May did not follow the court's decision, meaning that the amendment stood. The Constitutional Court declared in its decision that legislation allowing for secret observation on officials in positions requiring national security screening for 30-day periods twice a year is unconstitutional. According to the top court's ruling, permanent surveillance and secret information gathering would disproportionately restrict the target's privacy rights. The body also threw out stipulations that prevented targeted persons from seeking legal remedy, such as an appeal to a relevant parliamentary committee against the monitoring procedure.

The other story which shows the government's totalitarian attitude to the right to privacy is that in 2013 Hungary appeared on the list of those countries where the infamous governmental spy

software package called FinFisher is used, according to Citizen Lab. Citizen Lab is an interdisciplinary laboratory based at the University of Toronto (Canada), focusing on the intersection of information and communication technologies, human rights and global security. FinFisher's customers can only be governments and in using the software, Hungary joined a group of countries where oppressive regimes are in power. FinFisher is a very sophisticated software package which is able to create access to all data on the infected computer, including emails, document files, voice over internet protocol (VoIP) calls, etc. There were few reactions in Hungary when this news was published, but Átlátszó (Transparent),¹ a Hungarian NGO fighting for freedom of information, submitted a public information request to the Constitution Protection Office on 17 October 2013. It asked the Office to disclose the length of time and the number of times the government used spy software packages, and it asked it to list those that are in use. Within a week the Constitution Protection Office had sent a letter, and refused to respond to their questions, referring to national security interests. According to the website of the Office, "the aim of the Constitution Protection Office is to protect citizens and the constitutional order of Hungary, and to guarantee their security. (...) Its special duty is to provide Hungary with such information for decision making which is not obtainable from other sources."²

While all these unfortunate events happened in Hungary, the First European Constitutional Court suspended the Data Retention Directive after the decision of the Court of Justice of the EU (CJEU). The CJEU declared this April, among other objections, that the interference is not proportionate and that the Directive failed to apply those safeguards which were also missed in the Hungarian implementation and in other national legislation. However, the Hungarian authorities did not immediately react to the news (e.g. in neighbouring Slovakia the Constitutional Court preliminarily suspended the effectiveness of the Slovak implementation of the Data Retention Directive right after the decision of the CJEU).

Conclusions

The following conclusions can be drawn from this report:

- Data retention in general and by definition violates our right to privacy.

- It is necessary to apply certain safeguards: the need for judicial authorisation, court oversight, or any other external supervisory mechanism; authorities should not have direct access to data stored by service providers; there is an obligation to inform the person concerned about the use of his/her data; there is an obligation to inform the person who was under surveillance; there is an obligation to destroy the data after the end of investigative proceedings; and there is an obligation to delegate independent experts to inspect and monitor the process of destroying the data.
- Surveillance mechanisms which target innocent people by collecting information about them simply because they are in certain positions serving the state cannot be justified and should be taken as unconstitutional. One example of this is the amendment of the Hungarian National Security Law, which aims to surveil people who are completely innocent, simply to control them and their private lives. Such acts cannot be justified in a democracy.

Action steps

The following advocacy steps are taking place and recommended for Hungary:

- Citizens and human rights NGOs are planning to initiate a lawsuit against service providers in order to know what personal data is being retained by the providers.
- Following the recent decision by the CJEU, Hungary should revise its law on data retention.
- Hungary should get back onto the democratic road when it comes to surveillance and modify the National Security Law according to the Constitutional Court ruling.
- The use of spy software packages should be more transparent and regulated by law as well. The Constitution Protection Office should have an obligation to make such data publicly available for everybody.
- The need for transparency is obvious. The intersection between national security, surveillance, law enforcement, the role of private companies, citizens' private data and their right to privacy needs to be clear. Transparency reports prepared by companies involved in data retention can be one useful tool to know what is happening in this area. For example, Vodafone made an attempt to publish certain information on this in its worldwide report.

¹ www.atlatszo.hu

² ah.gov.hu/english

INDIA

Communications surveillance, human rights and freedom of expression in India



Digital Empowerment Foundation (DEF)

Ritu Srivastava
www.defindia.org

Introduction

The internet is a key tool to exercise the right to freedom of expression. It not only allows us to exercise the right to receive information, knowledge, ideas and opinions, but also allows us to exercise the right to express these – be it in the form of video, audio or writing. Used as a publishing and communication tool, it enables millions around the world to communicate instantly, gives the common citizen a voice among an audience of millions, and serves as a huge multimedia library of information. One definition says “the internet is as diverse as human thought.”¹

As access to the internet becomes more diverse, including information on prominent social issues is becoming important. United Nations (UN) Special Rapporteur on the Promotion and Protection of the Right to Freedom of Expression and Opinion Frank La Rue underlined in his report submitted to the Human Rights Council (HRC) regarding the unique and transformative nature of the internet that it not only enables individuals to exercise their right to freedom of expression and opinion, but also allows them to exercise other human rights and to promote the progress of society as a whole.² It has been proven that technological advances have been powerful tools for democracy by giving access to all. However, data mining by intelligence agencies blurs lines between legitimate surveillance and arbitrary mass surveillance by governments nationally and internationally.

La Rue also emphasised how government and corporate surveillance are undermining freedom of expression. His report states: “Freedom of expression cannot be ensured without respect to privacy in communications. Privacy and freedom of expression are interlinked and mutually dependent; an

infringement upon one can be both the cause and consequence of an infringement upon the other.”³

His report established the connection between freedom of expression and privacy in communications and called for global attention to the widespread use of surveillance mechanisms by various governments that are violating human rights, such as the right to privacy and freedom of expression. It also makes the point that privacy is a fundamental human right, and is important for democratic society to maintain its human dignity. Furthermore, the right to privacy reinforces other rights, such as freedom of expression and information, and freedom of association, also recognised under human rights law.⁴ However, it is difficult to define exactly what the right to privacy entails. Privacy can be seen from two perspectives – it depends on the type of information we share or the sides of our lives that we want to keep private, and whether or not the information is in the public interest.

Governments worldwide have continued to justify their engagement in wide-ranging surveillance programmes – often at the very limits of the law – arguing national security concerns. While India is the world’s largest democracy and is said to be protecting freedom of speech through its laws and constitution, freedom of expression online is increasingly being restricted in the country. Justifications given for these restrictions are the problem of defamation and the need to maintain national security and peace in society.

This became evident when the Indian government announced the start of the Centralised Monitoring System (CMS) in 2009, a programme to monitor telecommunications in the country. In 2013, Minister of State for Communications and Information Technology Milind Deora initiated the rollout of CMS across India. This report analyses how government surveillance works in India, and how government and private organisations are accessing individuals’ online data, which is a threat to freedom of expression.

Communications surveillance laws in India

The term “communications surveillance” encompasses the monitoring, interception, collection, analysis, use, preservation and retention of, interference with, or access to information which arises from, reflects or is about a person’s communications in the past, present or future. With more and more people accessing the web, the internet user base in India reached 243 million⁵ in 2014. This medium not only enables users to exchange information and deliver services, but also allows political discourse. Platforms like Facebook and Twitter and blogs make it easy for people to communicate and reach a vast audience.

Unlike PRISM, the United States surveillance programme that captured the world’s attention ever since whistleblower Edward Snowden leaked details of global spying to *The Guardian* and *Washington Post*, India silently launched the CMS to monitor internal communications in 2013. The system cost USD 75 million, and will allow the government to access all digital communications and telecommunications in the country.

Since independence, laws in India have prohibited the unlawful interception of communications. For example, Section 26 of the India Post Office Act, 1898 allows the interception of post for the “public good” only. According to this section, this power may be invoked “on the occurrence of any public emergency, or in the interest of the public safety or tranquillity.”⁶ The section also says that “a certificate from the State or Central Government” is required that would serve as conclusive proof as to the existence of a public emergency, or to show that the interception is in the interest of public safety or peace. Similarly, Section 5(2) of the Telegraph Act, 1885 also authorises the interception of messages, but only a) in the event of a public emergency, or in the interest of public safety; and b) if it is necessary or expedient to do so in the interests of the sovereignty and integrity of India, the security of the state, friendly relations with foreign states, or public order, or for preventing incitement to the commission of an offence.⁷

In the case of *Hukam Chand Shyam Lal vs. Union of India and Others*,⁸ the Supreme Court of India in-

terpreted the meaning of “public emergency”. The court considered “public emergency” merely as an “economic emergency”, and justified surveillance under this section unless it raised problems relating to the matters indicated in the section. The court also considered another qualifying term, “public safety”, as “security of the public or their freedom from danger”.

Two separate sections of the Information Technology Act 2000 deal with interception and monitoring of information. Section 69 deals with the “[p]ower to issue directions for interception or monitoring or decryption of any information through any computer resource”.⁹ Section 69B deals with the “monitor[ing] and collect[ion] of traffic data or information generated, transmitted, received or stored in any computer resource”. This monitoring power can be used for cyber security purposes.¹⁰ The term “traffic data” has been defined under Section 69B as “any data identifying or purporting to identify any person, computer system or computer network or any location to or from which communication is or may be transmitted.”

Surveillance is not only limited to individual monitoring. Section 67C of the Information Technology Act deals with “intermediaries”, and requires them to maintain and preserve certain information under their control for a minimum of three months. Failure to do this is punishable with imprisonment for up to three years and a fine under Section 67 C(2). Section 79 of the Information Technology Act¹¹ provides immunity from liability for intermediaries for third party content that is hosted by them. However, in 2011, the Ministry of Information and Technology issued two more sets of rules under this Act – firstly to govern intermediaries such as internet service providers (ISPs) and web platforms, and secondly to govern cybercafés. Both of these sets of

1 ACLU v. Reno, 929 F. Supp. 824, 830-849 (ED Pa. 1996) at 842 (District Court Opinion)

2 Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, 17 April 2013. www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf

3 Ibid.

4 Universal Declaration of Human Rights, Article 12; United Nations International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families, Article 14.

5 Times of India. (2014, January 29). India to have 243 million internet users by June 2014: IAMAI. *Times of India*. timesofindia.indiatimes.com/tech/tech-news/India-to-have-243-million-internet-users-by-June-2014-IAMAI/articleshow/29563698.cms

6 The Indian Post Office Act, 1898. www.indiapost.gov.in/Pdf/Manuals/TheIndianPostOfficeAct1898.pdf

7 The Indian Telegraph Act, 1885. http://www.ijlt.in/pdffiles/Indian-Telegraph-Act-1885.pdf

8 AIR 1976 SC 789, 1976 SCR (2)1060, (1976) 2 SCC 128.

9 Section 69 of the Information Technology Act. www.chmag.in/article/jan2012/powers-government-under-information-technology-act-2000

10 The Monitoring Rules list 10 “cyber security” concerns for which monitoring may be ordered: (a) forecasting of imminent cyber incidents; (b) monitoring network application with traffic data or information on computer resources; (c) identification and determination of viruses/computer contaminants; (d) tracking cyber security breaches or cyber security incidents; (e) tracking computer resources breaching cyber security or spreading viruses/computer contaminants; (f) identifying or tracking of any person who has contravened, or is suspected of having contravened or being likely to contravene cyber security; (g) undertaking forensic investigation of the concerned computer resource as a part of an investigation or internal audit of information security practices in the computer resource; (h) accessing stored information for enforcement of any provisions of the laws relating to cyber security in force at the time; (i) any other matter relating to cyber security.

11 sflc.in/information-technology-act-and-rules-time-to-change

rules severely diminish the freedom of expression of citizens and their right to privacy.

India, which is poised to be one of the biggest markets for video surveillance, registered growth of 20% in this regard in the last quarter of 2013. The Delhi International Airport has installed 3,700 IP surveillance cameras,¹² the “largest single installation of an IP video system anywhere in India.” Both the government and private businesses have enthusiastically embraced CCTV technology, including in municipalities, police departments, airports, banks, schools and supermarkets. Despite the fact that CCTV cameras were installed to tackle terrorism and crime, there are no laws that govern their deployment or use in India. The closest law applies to electronic voyeurism and is contained in Section 66E of the Information Technology Act, which punishes the “capturing, publishing and transmission” of images of any person in a “private area” without their consent, “under circumstances violating the privacy” of that person. This offence is punishable with imprisonment of up to three years or a fine of up to two lakhs rupees (approx. USD 3,000).

Moreover, in 2011, the government expanded its internet surveillance in cybercafés, the primary access points for rural villagers. Users now need to provide their identity card for accessing cybercafés. Requesting this kind of user data is questionable when it is used for prosecuting free speech online and stifling political criticism. India is also one of the worst offenders for takedowns, as well as for requests for user information. The Google Transparency Report shows that on requests for user information it is ranked after the US only.¹³

At the end of 2012, most of the major telecom companies in India agreed to grant the government real-time interception capabilities for the country's one million BlackBerry users.¹⁴ The government is also constantly requesting major web companies to set up their servers in India in order to monitor local communications.

Freedom of expression and communications surveillance

The Constitution of India guarantees freedom of expression under its Article 19(1). However, Article 19(2) restricts the exercise of freedom of expression. Article 19(2) can be enforced by the state in

the interest of the sovereignty and integrity of the state, the security of the state, friendly relations with foreign states, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence.¹⁵ The constitution does not include a freestanding right to privacy. However, the Supreme Court of India has read the right to privacy in Article 21 of the constitution – the right to life and liberty. It states, “No person shall be deprived of his life or personal liberty except according to procedure established by law.”¹⁶ Considering the right to freedom of expression and the right to privacy, the fundamental question is the balance between the two.

For the last few years, a comprehensive Privacy Bill has been under discussion in India, although it has still not been adopted by the government. A draft dated 19 April 2011, entitled “Third Working Draft (For Discussion and Correction) Legislative Department”, was originally leaked, but is now freely available online.¹⁷ The draft supports privacy rights broadly, and includes a strong mechanism to address breaches of the right to privacy, called the Data Protection Authority of India (DPAI). Without privacy laws and safeguards to protect data, the collection and retention of such data can be misused easily, and this could have a chilling effect on free speech among the Indian population. Most Indian members of parliament are aware of the need for a legal framework to protect the privacy of Indian citizens. In 2011, the parliament passed new data protection rules; however, there is still no privacy law in India. Like freedom of expression and freedom of association, privacy is a fundamental human right and underpins human dignity.

A road ahead

The following actions and steps are recommended for India:

- To take better account of the right to privacy and protection from arbitrary interference with privacy. There is also a need to address mass surveillance and unwarranted digital intrusions in India. Both are necessary steps to fight self-censorship and promote freedom of expression.
- Communications surveillance should be regarded as a highly intrusive act that interferes with the rights to privacy and freedom of opinion and expression, threatening the foundations of a democratic society.

- Reform the Information Technology Act provisions 66A and 79 regarding takedown procedures so that authors of content can be notified and offered the opportunity to appeal takedown requests before censorship occurs.
- Revise takedown procedures so that demands for the removal of online content do not apply to the legitimate expression of opinions or content in the public interest. This is important so that freedom of expression is not undermined.
- The internet should not be used by governments as an excuse for introducing new technologies of control or for curtailing existing liberties. Although the right to freedom of expression can be restricted, the circumstances under which this may be done have to be narrowly circumscribed. This is the case when it comes to freedom of expression on the internet, and in any other forum.
- In a country like India where 243 million people access the web through mobile phones, there is a need to reform policy so that regulation of the internet is compatible with the international legal guarantee of the right to freedom of expression. Moreover, there is a need to promote access to the internet as well as the development of local content.
- Service providers or hardware or software vendors should not be compelled to build surveillance or backdoors into their systems, or to

collect or retain particular information purely for state surveillance purposes.

- Finally, there are many aspects involving the right to privacy and freedom of expression that relate to each other and that have not been addressed strongly in Indian legislation, policy or case law. For example, the taking of photographs by individuals (not the media) has not been addressed, nor has the ability of individuals to issue comments anonymously online, or the “right to be forgotten” online and offline. Freedom of expression and privacy support each other in many ways, as the right to express an opinion or thought freely is often protected by providing the individual the privacy (or anonymity) to do so. There is therefore a need to understand various aspects, such as the right to be anonymous, the right to privacy, and the right to be forgotten, with respect to freedom of expression and freedom of association. These issues are being addressed by many countries and at an international level.

It is high time the Indian government took account of the right to privacy and protection instead of interfering with privacy. Addressing the issue of mass surveillance and unwarranted digital intrusions is a vital and important step to fight against self-censorship in India and will automatically promote freedom of expression.

¹² www.indigovision.com/documents/public/project-briefs/Project-Brief-Delhi%20Airport-UK.pdf

¹³ www.google.com/transparencyreport/userdatarequests/IN

¹⁴ Gallagher, R. (2013, February 22). India's spies want data on every BlackBerry customer worldwide. *Slate*. www.slate.com/blogs/future_tense/2013/02/22/india_wants_data_on_every_blackberry_customer_worldwide.html

¹⁵ The Constitution of India, Article 19 (2).

¹⁶ www.legalserviceindia.com/articles/art222.htm

¹⁷ Available at: bourgeoisinspirations.files.wordpress.com/2010/03/draft_right-to-privacy.pdf

INDONESIA

Taming the untameable: Indonesia's effort to control the growing tide of digital communications



Anonymous
Anonymous

Introduction

Following three decades of a restrictive Suharto-led government characterised by “political repression and ideological surveillance,”¹ Indonesia has morphed into a relatively open society with more democratic space. Along with this openness, it has witnessed a massive transformation in the area of information and communications technologies (ICTs). Indonesia has the fourth largest mobile phone market in the world with 278 million subscribers.² By 2015, it is expected that nearly 115 million will have access to the internet.³ The country has been hailed by civil society activists as “regional champion for freedom of expression.”⁴ Indonesia's capital, Jakarta, is called the “social media capital of the world” with more tweets coming from the city than any other capital in the world.⁵ It is the only country in the region to provide protection of free speech through a legal framework called the Transparency of Public Information Law, which guarantees access to state information, and the Press Law, which protects journalistic work as “an important component of [...] free speech and access to information.”⁶

At the same time, legal frameworks continue to tightly limit basic freedoms, justified by arguments concerning traditional values or the maintenance of national security. This is demonstrated through notable legal setbacks, such as the Mass Organisation Law that restricts the right to freedom of association. The Intelligence Law of 2011 enforces further restrictions by allowing the security apparatus “sig-

nificant latitude in intelligence gathering aimed at ‘opponents’ of ‘national stability’.”⁷

The country's first and only cyber law, the Electronic Information and Transaction Law, prohibits the publishing of content to do with gambling, and defamation and threats. The Indonesian parliament has also passed an Anti-pornography Law, which is routinely used to block LGBT (lesbian, gay, bisexual and transgender) content on the internet.⁸ In addition, the country has also adopted a number of laws that prohibit defamation of religion, which is used broadly to block content that provides alternative views on Islam, the religion of the majority of Indonesians.

While the boundaries of expression have widened notably, and are more open generally in Indonesia than in its regional counterparts, the country is a mixed picture of freedom of expression. As suggested, norms of expression are reinforced through a variety of anti-pornographic, anti-blasphemy and anti-defamation laws. In legal terms and in practice, Indonesia has also regularly demonstrated that “national security” or “national stability” interests trump freedom of expression. While censorship is overt, surveillance is less visible but also pervasive, with each carried out by different government agencies.

This report looks at communications surveillance in Indonesia by examining the recent purchases of sophisticated surveillance equipment by the military. It opens up questions about the potential use of this new equipment and what this means for freedom of expression in the country.

Surveillance +

In the book *Democratisation of Post-Suharto Indonesia*, Jun Honna argues that “political repression and ideological surveillance were the major tools used” by Suharto to remain in power.⁹ These “politico-ideological” surveillance tactics were carried out principally by the military, targeting journalists,

students, intellectuals and activists, essentially muzzling dissenting voices in the country. While a relatively free media and civil society activism have flourished in the wake of Suharto's removal, the practice of military surveillance continues. The Indonesian military continues to project a role as the protector of national unity, and to demarcate the limits of political and ideological expression in the country through a range of practices, including surveillance.

Complementing its traditional intelligence collecting approaches, and in parallel with the massive growth of internet use, the military is expanding its online surveillance capability. In January 2013, the *Jakarta Globe* reported that Indonesia's Ministry of Defence purchased GBP 4.2 million (USD 6.7million) worth of surveillance products from Gamma Group, a UK-based company that provides sophisticated surveillance equipment to governments.¹⁰ While the exact type of product procured was not disclosed, Gamma Group sells products ranging from mobile surveillance vans to software like FinFisher, which is capable of monitoring all internet communication in the country.

In fact, FinFisher command and control servers were already found to be at work in Indonesia in 2012. According to a report released by Citizen Lab in 2012, FinFisher products were found on several Indonesian internet service providers (ISPs).¹¹ The Indonesian government has not publicly stated if it is the one deploying this intrusive software or clarified its intended use. Gamma Group, on the other hand, has stated that it only provides services to governments and not private individuals and companies. Based on these statements, one can surmise that complex communication surveillance machinery is in place in Indonesia, and its use only seems to be expanding over time.

Rights activists are concerned about the implications of these findings. “I'm afraid there're not enough mechanisms and self-control to ensure that this technology is not abused,” Andreas Harsono, Indonesia researcher with Human Rights Watch, told the *Jakarta Globe*. “Indonesia has no third-party intelligence gathering mechanism – be [it] a court or a legislative mechanism – to approve wire-tapping. The Gamma equipment is a nightmare.”¹²

The Intelligence Law is applied to intelligence gathering activities in Indonesia. When an updated

version of the law was passed in 2011, rights groups criticised it for its expansive scope and its vague wording, which allows for “significant intelligence gathering over opponents of national stability.”¹³

The government has referred to terrorism, including two bombings in Bali in 2002 and 2005, as well as multiple attacks in Jakarta, as justification for surveillance. While the government has said surveillance products will be used “only for strategic intelligence,”¹⁴ rights groups and activists have warned that it could be used to monitor, and potentially silence, civil society and media.

The current situation in West Papua illustrates the broad application of the government's definition of “opponents of national stability”. West Papua¹⁵ is the easternmost province of Indonesia with a large presence of the military's Special Forces to combat the Papuan separatist movement, the Free Papua Movement (*Organisasi Papua Merdeka* or OPM), who have been engaged in armed resistance. International media are blocked from entering the province and international organisations have been prevented from operating in the region.

In 2011, a report by Human Rights Watch, citing internal military documents, asserted that military surveillance in the province monitored not only the OPM, but a “broad swathe of Papuan political, traditional, and religious leaders and civil society groups.”¹⁶ This surveillance was carried out entirely without “judicial warrant and without clear evidence of wrongdoing.”¹⁷ The internal documents also showed that the intention of the government was to prevent the free flow of information to and from Papua. According to one document: “Current political activity [e.g. by civil society and students] in Papua is very dangerous compared to the activities of Papuan armed groups, because [civil society] influence already reaches abroad.”¹⁸

Physical surveillance and rudimentary surveillance tactics are well known by Papuan activists and journalists. An Indonesian journalist who wished to remain anonymous stated in an interview that phone tapping is common. “When you are in Papua and if you are calling someone, you can hear other people talking. It is called crossed lines, when it is accidental. In Papua, every call you make is like

1 Bünthe, M., & Ufen, A. (eds.) (2009). *Democratisation in Post-Suharto Indonesia*. Oxford: Routledge.

2 Indonesia's population is 247 million. Due to multiple phone subscriptions, this number of mobile subscribers is higher than the population. www.redwing-asia.com/market-data/market-data-telecoms

3 www.slideshare.net/OnDevice/indonesia-the-social-media-capital-of-the-world

4 Southeast Asian Press Alliance. (2013, July 8). Indonesia's Ormas Law: A ready weapon against civil society and free speech. IFEX. https://ifex.org/indonesia/2013/07/08/ormas_law

5 www.slideshare.net/OnDevice/indonesia-the-social-media-capital-of-the-world

6 Southeast Asian Press Alliance. (2013, July 8). Op. cit.

7 Ibid.

8 Citizen Lab and Canada Centre for Global Security Studies. (2014). Islands of Control, Islands of Resistance: Monitoring the 2013 Indonesian IGF. www.citizenlab.org/briefs/29-igf-indonesia/29-igf-indonesia.pdf

9 Bünthe, M., & Ufen, A. (eds.) (2009). Op. cit., p 230.

10 Vit, J. (2013, September 25). TNI surveillance purchase triggers concern in Indonesia. *Jakarta Globe*. www.thejakartaglobe.com/news/tni-surveillance-purchase-triggers-concern-in-indonesia

11 Citizen Lab and Canada Centre for Global Security Studies. (2014). Op. cit.

12 Vit, J. (2013, September 25). Op. cit.

13 Southeast Asian Press Alliance. (2013, July 8). Op. cit.

14 Vit, J. (2013, September 25). Op. cit.

15 Now divided into Papua and West Papua.

16 Human Rights Watch. (2011, August 14). Indonesia: Military documents reveal unlawful spying in Papua. Human Rights Watch. www.hrw.org/news/2011/08/14/indonesia-military-documents-reveal-unlawful-spying-papua

17 Vit, J. (2013, September 25). Op. cit.

18 Human Rights Watch. (2011, August 14). Op. cit.

that.”¹⁹ Intelligence agencies have even set up phone charging booths to collect phone numbers. “When you charge your phone, you have to give them your number. There is evidence of intelligence agencies using phone credit stores to supply numbers to the military. Usually these are targeted at NGOs.”

Papuan journalists and activists say surveillance extends to other forms of communication. “Many times, I have received notification from Gmail that someone tried to access my account,” said Latifah Anum Siregar, head of the Alliance for Democracy for Papua (*Aliansi Demokrasi untuk Papua*).²⁰ “Our website adlp-papua.com has been hacked several times. When that happens data is usually missing, files cannot be downloaded.”

“In the past three years, our website tabloid-jobi.com has been hacked six times. We are also aware of surveillance on the internet,” said Victor Mambor, head of the Alliance of Independent Journalists in Papua.²¹ “Our Twitter and Facebook are being monitored.” Journalists often receive calls and orders from the military asking them to hand over tapes and other recordings, especially if they are covering events relating to political dissent, like demonstrations, Mambor said.

Papuan activists interviewed for this report have also spoken of the practice of self-censorship on social media sites over fears of being physically harmed by security forces. “Now I only trust face-to-face communication. I rarely use the telephone to talk about sensitive issues.”

Even without surveillance, Indonesia has demonstrated a position of not fully supporting freedom of expression on the internet. With a variety of anti-pornographic, anti-defamation and anti-rumour mongering laws, it already blocks content on the internet. As suggested, this has been manifested in blocking content that discusses LGBT rights and content that provides alternative views on religion.

The silencing of local voices from Papua is not limited to strictly political expression. In March 2014, a live video-cast of two Papuan tribesmen speaking at a major environmental conference in the United States was disrupted by an online attack on the site, which rights activists say came from parties linked to the Indonesian government.²²

¹⁹ Interview with an anonymous journalist on 23 May 2014.

²⁰ Interview with Latifah Anum Siregar, head of the Alliance for Democracy for Papua, on 3 June 2014.

²¹ Interview with Victor Mambor, head of the Alliance of Independent Journalists in Papua, on 3 June 2014.

²² Sloan, A. (2014, March 20). Indonesia suspected of hacking to silence abuse allegations. Index on Censorship. www.indexoncensorship.org/2014/03/indonesia-suspected-hacking-silence-abuse-allegations

Opportunities for reform?

There are indications that a multi-pronged surveillance system, employing sophisticated software and taking advantage of weak legal protections for expression, will mean that it will be even easier to suppress freedom of expression on the internet in the future.

There are some potential opportunities that could be leveraged for reform. The Indonesian government hosted the annual global Internet Governance Forum (IGF) in Bali in 2013, which opens up a space for debate surrounding freedom of expression on the internet. The timing of the IGF, directly following the Snowden revelations, raised the profile of surveillance at the forum.

In the immediate future, whether this trend towards openness continues will be influenced by which candidate wins the presidential elections in July 2014. The candidates for president, Prabowo Subianto and Joko Widodo, appear to maintain starkly different positions on these issues. Prabowo is taking a hard-line nationalistic stance that could mean setbacks in terms of rights of expression, as he would appear to be less tolerant of dissent, while Jokowi, as he is known, is campaigning on a platform of transparency.

In the meantime, journalists and activists continue to tolerate limits to their freedom. “I accept this surveillance as the risk of my job. There is nothing we can do except to accept this as part of our everyday reality,” said Mambor. “People in Jakarta may have choices, but we, in Papua, don’t. There is only one internet provider and the service is not good.”

Siregar further echoes this sentiment, stating, “I tell my colleagues that our job is full of risks. Don’t expect that our name is not already recorded by the intelligence [agencies] and our picture and data isn’t in their system already.”

Action steps

Based on the current scenario, the following action steps are recommended for activists and journalists:

- Be aware of the prevalence of surveillance, and take protective measures when communicating online by using secure tools.
- Make your colleagues and associates aware of surveillance; teach them to use secure methods of communications.
- Engage with freedom of expression activists locally and internationally to leverage change in this area.
- Lobby governments for stronger legal protections around freedom of expression.

JAMAICA

Resisting citizen data handover in Jamaica: The case of Digicel vs INDECOM



The University of the West Indies

Hopeton Dunn and Allison Brown
www.mona.uwi.edu

Introduction

A recent Supreme Court ruling in Jamaica prohibiting a state agency from gaining access to the telephone data of Jamaican citizens touches on several of the international principles of human rights in relation to surveillance. In the case, Supreme Court judge Justice Ingrid Mangatal ruled in June 2013 that telecommunications provider Digicel was not compellable under the law to provide customer data or subscriber information to the investigative state agency called the Independent Commission for Investigations (INDECOM). In this report we analyse the circumstances of this ruling and the implications regarding constitutional protections in Jamaica and the Caribbean against unauthorised surveillance by government of the personal data of citizens.

Background

Jamaica is a small independent, English-speaking country in the Caribbean. The most recent census in 2011 tallied a population of just below 2.7 million.¹ The country operates a bi-cameral parliament with a bill of rights and a constitution that emphasises democracy and the rule of law.

Jamaica’s GDP per capita was reported by the Planning Institute of Jamaica in 2010 to be USD 4,979.² Services such as tourism and information and communications technologies (ICTs) remain key contributors to GDP, with traditional products such as bauxite, sugar and bananas playing important roles in employment and GDP output. The current National Development Plan, named Vision 2030, targets developed country status by 2030.

ICTs are a central aspect of the national development plan as they are seen as a growth industry in their own right as well as a driver of economic and social development. A 2011 survey indicated that 94% of the population were mobile phone users, 16% of households had internet access, while 45%

¹ STATIN. (2012). *Population Census Data*. Kingston: STATIN.

² Planning Institute of Jamaica. (2012). *Jamaica Country Assessment (Preliminary Draft)*. Kingston: PIOJ.

of individuals used the internet from anywhere.³ These indicators would have moved upwards significantly since that survey, particularly in the area of mobile broadband usage. The cost of equipment and services is the key hindrance to the growth of the online population in Jamaica.

Policy context

The telecommunications and ICT industry is mainly governed by the Telecommunications Act of 2000, which was amended in 2011. This is supplemented by other pieces of legislation such as the Electronic Transactions Act of 2007 and the Cybercrimes Act of 2010. Key legislation in relation to state surveillance is applied in the Interception of Communications Act of 2002 (amended in 2011) while section 47 of the Telecommunications Act speaks to the protection of customer data by telecommunications service licence holders. Jamaica’s Charter of Human Rights (2011) addresses the right of everyone to privacy of property and of communication. Despite longstanding calls from civil society and the academic community, a Data Protection Act is still in the consultation stage, now promised for introduction to parliament sometime in 2014.⁴ This act would protect the privacy of citizens’ personal data and would regulate the “collection, processing, keeping, use and disclosure” of such data.⁵

Basics of the case

As we thematically consider the issue of communication surveillance in the digital age, the Jamaican case of *Digicel (Jamaica) Limited v The Independent Commission of Investigations*⁶ is of special interest. The case touches on many of the international principles of human rights in relation to surveillance. The matter arose from a request for informa-

³ Dunn, H., Williams, R., Thomas, M., & Brown, A. (2011). *The Caribbean ICT and Broadband Survey Jamaica*. Mona: Telecommunication Policy and Management Programme, University of the West Indies.

⁴ The Data Protection Act will possibly reflect model legislation developed by the ITU-led Harmonization of ICT Policies, Legislation and Regulatory Procedures in the Caribbean (HIPCAR). www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPCAR/Pages/default.aspx

⁵ Angus, G.L. (2014, June 11). Laws far advanced to modernize ICT sector. *Jamaica Information Service*. jis.gov.jm/laws-far-advanced-modernize-ict-sector

⁶ [2013] JMSC Civ. 87.

tion from police monitoring agency INDECOM to dominant telecom provider Digicel in 2011 for call origination data. This data was to have been used in the investigation of the shooting death of Robert “Kentucky Kid” Hill in 2009 at the hands of members of the local security forces. Digicel brought the case to the Jamaican Supreme Court against INDECOM in order to clarify their responsibilities in the sharing of customer data. In summary, the outcome was a Supreme Court ruling which prohibited the state agency INDECOM from gaining access to the telephone data requested.

Digicel (Jamaica) Limited v The Independent Commission of Investigations

Digicel (Jamaica)

Digicel Jamaica is the first telecommunications provider which entered the Jamaican market after its liberalisation in 2000. Prior to that, the market was controlled by the monopoly of Cable and Wireless, which now trades as LIME. Since Digicel's entry a few other firms have entered and left the market, the most recent being Claro (América Móvil), which was acquired by Digicel in 2011. According to a survey completed in 2011, Digicel controlled, at that time, 88% of the mobile market.⁷ Its gains in market share following its acquisition of Claro have not yet been quantified, but Digicel is considered, in legal terms, to be the dominant player in the Jamaican mobile market, with LIME being the only other major player. In 2014 Digicel operates in 32 markets in the Caribbean, Central America and Asia-Pacific.

INDECOM

INDECOM conducts “investigations concerning actions by members of the Security Forces and other agents of the State that result in death or injury to persons or the abuse of the rights of persons; and for connected matters.”⁸ It was put in place by the INDECOM Act of 2010 which replaced the Police Public Complaints Act. INDECOM was to be an independent body set up to investigate injustices carried out by members of the security forces in Jamaica. This is within the context of long-held perceptions of police corruption among the wider society, including what has been seen as “many shooting incidents which have led to the death or serious injury of citizens.”⁹

A commentary in the *Western Mirror* by Robert Dalley earlier this year noted:

In some cases, there are clear facts to substantiate the claim that the person who was shot and killed by the police was brutally murdered, however, because of the fact that the country has corrupt police officers in the force and an underperforming court and judicial system, the police are not prosecuted or charged in any way.¹⁰

The *Digicel v. INDECOM* judgement refers to information from the Bureau of Special Investigations (BSI) stating that from 1999 to 2010, 2,257 persons were killed by the police (an average of 188 per year). Similar statistics have been reported by the local human rights lobby group Jamaicans for Justice. It is useful to point out that the figures indicated do not include the number of these killings which have been investigated and seen as justified by the legal system.

The *Digicel v. INDECOM* case also speaks to several attempts on the part of the local government to address the quandary of police killings and other abuses. Previous attempts include the Police Public Complaints Authority (PPCA) and the BSI mentioned above. However, while the PPCA was under-resourced, underfunded and lacked the needed authority to investigate, there was an ostensible issue of independence as it related to the second team – the BSI – which was located within the Jamaica Constabulary Force (JCF), one of the bodies the unit was required to investigate.

INDECOM was established as a resolution to these issues. The INDECOM Act of 2010 sought to bestow sufficient powers for the Commission to investigate corruption within the security forces. What can be surmised from the preceding section is that at the centre of the establishment of INDECOM is a pursuit of improved human rights practices, particularly in relation to greater accountability among security forces, the investigation of police killings and other alleged abuses by members of the security forces.

The context for INDECOM

The matter of police accountability is a subject which cannot be broached in a vacuum. We are required to highlight the high levels of major crime in Jamaica as a possible contributor to the high levels of police killings. With 1,200 murders committed

in 2013,¹¹ the country has the sixth highest murder rate worldwide.¹² The punishment of execution for capital crimes, although on the books, has not been implemented since 1988. Some police and citizens alike have supported the idea that extrajudicial killings can be justified within the context of controlling major crimes and containing the murder rate. This is the context within which the high number of police killings must be understood.

Details of the case

This case emerged specifically from a request made on 28 September 2011 by INDECOM to Digicel requiring the telecom provider to furnish data on telecommunication services for particular subscribers who had been named in an investigation being undertaken. In the investigation of the death of Hill, the allegation emerged that his shooting was the result of a conspiracy between some named members of the security forces, a cousin of the deceased and another named female. The data was needed for further investigation of this alleged conspiracy. A parallel request was also made to LIME, the contents of which have not been discussed in detail in the judgement. Digicel noted that while it was not unwilling to provide the information, guidance would be needed from the local courts as to what is required of the telecom provider in response to the request from INDECOM. This is particularly in light of other legislation which governs such interactions. LIME, on the other hand, has complied with the request.

INDECOM cited section 21 of the INDECOM Act in its request for the data. A part of section 21 reads:

The Commission may at any time require any member of the security forces, a specified official or any other person who in its opinion is able to give assistance in relation to an investigation under this act, to furnish a statement of such information and produce any document or thing in connection with the investigation that may be in the possession of that member, official or other person.

Section 16 of the Interception of Telecommunications Act was also seen by INDECOM to be supportive of its case, where subsection 2 states:

Where it appears to the designated person that a person providing a telecommunications service is or may be in possession of, or capable of obtaining, any communications data, the designated person may, by notice in writing, require the provider- (a) to disclose to an authorized officer all of the data in his possession or subsequently obtained by him; or (b) if the provider is not already in possession of the data, to obtain the data and so disclose it.

Digicel considered the requirement to provide information to be at odds with section 47 of the Telecom Act, which reads: “Every carrier and service provider shall, subject to subsection (2), regard and deal with as secret and confidential, all information regarding the type, location, use, destination, quantity and technical configuration of services used by their customers.” While exceptions are cited, none of them include that such information can be legally provided to INDECOM. The section does, however, allow for the delivery of such information “for the purpose of the investigation or prosecution of a criminal offence.” Further, the Interception of Communications Act was not seen by Digicel to compel them to furnish the data since INDECOM is not a named “authorized officer”.

In the write-up of the judgement, Justice Ingrid Mangatal noted that Digicel could not be compelled by INDECOM to provide this information as it would be in contravention of section 47 of the Telecom Act and the law cannot force a party to commit a criminal offence. There was also the issue as to whether discretion of the provider could be triggered in this case on the basis of section 47 of the Telecom Act. However, given that the documentation provided by INDECOM did not specify that the information was required for the investigation of a *criminal offence*, it was noted that the discretion of the provider could not be applied.

INDECOM has since challenged this outcome and the case is likely to return to court sometime in 2014.

Case analysis

Our understanding of this case is that the judgement does not prohibit state surveillance, but such surveillance could not be applied in the current case. If INDECOM had been named as an “authorized officer” in the Interception of Communications Act (or some amendment thereof), Digicel would have been compelled to provide whatever information INDECOM had requested. If the request had been worded differently (specifying it was needed to investigate a criminal offence), then Digicel

7 Dunn, H., Williams, R., Thomas, M., & Brown, A. (2011). Op. cit.

8 indecom.gov.jm/about_us.htm

9 Digicel (Jamaica) Limited v The Independent Commission of Investigations [2013] JMSC Civ. 87.

10 Dalley, R. (2014, February 2). ‘We need to reduce police killings in Jamaica’. *Western Mirror*. www.westernmirror.com/index.php/permalink/6659.html

11 Walker, K. (2014, January 1). 2013 bloodier than 2012. *Jamaica Observer*. www.jamaicaobserver.com/news/2013-bloodier-than-2012_15716666

12 Jamaica Observer. (2014, April 11). Jamaica has 6th highest murder rate worldwide – UN report. *Jamaica Observer*. www.jamaicaobserver.com/latestnews/Jamaica-has-6th-highest-homicide-rate-worldwide---UN-report

would have been able to provide the information at their discretion. This certainly raises concerns regarding implications for private citizens whose information could be at risk based on these possible amendments. However, these matters can only be considered in relation to the ostensible purpose of INDECOM, which at its foundation is seen as a preserver and defender of human rights and not an agency in opposition to such rights.

This case touches on many of the International Principles on the Application of Human Rights to Communications Surveillance.¹³ Jamaica continues to uphold the main understanding that value should be placed on the privacy of individuals, and simply because the state can access communications data does not always mean that the state should access such data. There are clearly boundaries and exceptions which are applied, and in the case of *Digicel v. INDECOM*, there is no major opposition to data being provided where there is a “legitimate aim” and adequate “need”. The challenge which faced the Independent Commission was that the laws had not been updated to ensure that the body was able to legally compel telecommunications providers to furnish subscriber data. Discretionary action was also eliminated as a possibility in this case because of the wording of the request to Digicel, and the omission of information which would have made compliance with the request legal.

The key outcome which must be considered is the way in which legislation lags behind developments in the telecoms sector and the gaps in understanding the ever-transforming digital age within which we operate. This is true for telecom practitioners, legal persons, law enforcement and ordinary citizens.

There is also the matter that both major telecom providers who are in control of telecommunications data are non-Jamaican entities which may also be subject to the laws of the countries in which they were initially established and countries where they operate. The role of such entities in preserving the human rights of citizens should be explored,

particularly where communication between countries can be easily monitored in one country or the other. This is of even greater concern given our understanding, through the Snowden case, that it is not necessarily the content of communication which may be monitored but also the metadata and broader patterns of communication.

The relevant matters of user notification, transparency and public oversight are emergent issues which should be tackled in the pending Data Protection Act.

Conclusions and action steps

There remains a general concern that legislation lags behind developments in the telecoms and ICT sector. This case shows one such example. Serious consideration needs to now be given to the powers which the state wishes to grant INDECOM, and to all relevant legislation that needs to be updated. These considerations are to be made in relation to human rights implications as well as to acceptable exceptions to privacy in line with the international context.

The second recommendation has to do with training and capacity building at all levels, so that practitioners and ordinary citizens alike will be able to understand the many issues at work in communications surveillance.

While the state remains a key area for consideration when it comes to communications surveillance, it is critical to contemplate how citizens, companies and foreign countries can also use communications surveillance to violate human rights. Countries like Jamaica need to ensure that legislation is robust and adequate for these threats in meeting national objectives and protecting citizens’ rights.

Finally, the Data Protection Act, which will be under parliamentary consideration in the near future, needs to take into account the International Principles on the Application of Human Rights to Communications Surveillance. In addition, it is also necessary to rationalise the new act with all relevant existing legislative and policy frameworks.

JAPAN

Learning from the past



Japan Computer Access for Empowerment

Hamada Tadahisa
www.jca.or.jp

Introduction

In 2012 the Japanese government passed legislation that presents a number of challenges for progressive civil society activists. Both the so-called Common Number Law and the State Secrets Protection Law reinforce surveillance regulations. Legislation is also pending that will expand the ability of authorities to “wiretap” the country’s citizens. These legislative changes can be seen as part of a process of the increased militarisation of the country, with startling parallels with changes in Japan ahead of World War II.

This new security legislation is far from fair, not only in terms of its content, but how it was developed. The bills were approved by the political majority without sufficient deliberations in parliament. The mass media also did not report on the controversial points before they were passed.

In this report we compare the legal frameworks governing communications surveillance today and those that existed before World War II in Japan. This is an attempt to learn the lessons of history so we do not repeat the mistakes we have made in the past.

Policy and political background

The Japanese government has been trying to develop laws that promote the control of information and surveillance for decades. It planned to introduce a national identification number in 1968, but every time it submitted the bill, the mass media strongly opposed it, and the attempts failed. Eventually, it managed to get the resident registry network bill passed, together with a wiretapping bill and bills related to defence cooperation, in 1999. At that time, the Japanese mass media did not report the deliberations in parliament sufficiently. Instead, they spent all their broadcasting time on a tabloid show: a verbal battle between Mitchy and Satchy, two on-screen women talents.

The government submitted the state secrecy bill in 1985, but failed to have it passed. It revised and submitted a bill on state secrets in 2013, and

managed to get the bill passed. The law is supposed to come into force in December this year – so this year might be one of the turning points in Japanese history. Moreover, a conspiracy bill and a revision of the Wiretapping Law are anticipated in 2014. This, together with the Common Number Law enacted in May 2013, suggests Japan is rapidly slipping into a paranoid surveillance state.

Here is a list of problematic legislation concerning communications surveillance:

- The Wiretapping Law (1999)
- The Computer Surveillance Law (Cyber Criminal Law) (2011)
- The Common Number Law (2013)
- The State Secrets Protection Law (2013).

Japan is one of 36 countries which international watchdog The Citizen Lab¹ shows used FinFisher, a notorious surveillance technology used to surveil internet users.

A tale of two Olympic games in Tokyo

We need to understand that the legislation promoting the regulation and control of information described above is part of a combined approach to legislative changes prepared over the past years, such as legislation defining the nation’s response to foreign military attack (2003) and an act dealing with the protection of citizens in the event of an armed attack (2004).

Many intellectuals have argued that the current situation in Japan closely resembles the situation before World War II. Because of this, we would briefly like to compare the run-up to two Tokyo Olympic Games, one scheduled for 2020, and the other in 1940, which was cancelled due to the war.

That Tokyo will host the 2020 Olympic Games is welcome news for many in the country. However, some people are concerned about the strengthening of the surveillance system for the games, and how this can be used to control citizens in the future.

During the Olympic Games held in London in 2012, the security and surveillance system used there became the centre of attention. The system included a network of CCTV cameras mounted

¹³ <https://en.necessaryandproportionate.org/text>

¹ <https://citizenlab.org>

throughout London, and unmanned aerial vehicles (UAVs), more commonly known as drones.

In 2014, the Tokyo Metropolitan Government started to install five security cameras for each elementary school zone – a target of 6,500 cameras to be installed by 2018. The total expenditure is expected to reach 2.47 billion yen (USD 25 million) over five years.

The 1940 Summer Olympics were originally scheduled to be held in Tokyo, 80 years before the Tokyo Olympic Games scheduled for 2020. However, they were cancelled due to the continuation of the Second Sino-Japanese War. The states of affairs before the two Olympic Games are remarkably alike:

- 1923 The Great Kanto Earthquake (A)
- 1929 The Great Depression (B)
- 1937 The Imperial General Headquarters² . . . (C)
- 1937 Complete revision of the Military Secrets Act (D)
- 1940 The cancelled Tokyo Olympics (E)
- 1941 The Pacific War
- 1995 The Great Hanshin-Awaji Earthquake . . . (A)
- 2008 The Great Recession (B)
- 2011 The Great East Japan Earthquake (A)
- 2013 The National Security Council (C)
- 2013 The State Secrets Protection Law (D)
- 2020 (scheduled) Tokyo Olympics (E)

If we put the series of events leading up to the two games in order as above, we can see how militarisation in Japan progressed (or, is progressing), affected both by government decisions and natural disasters.

The 26 February attempted coup and wiretapping

The greatest attempted coup d'état in modern Japanese history occurred on 26 February 1936. It recently became clear that widespread wiretapping occurred during this time, even though it was illegal under the Constitution of the Empire of Japan in those days.

In the attempted coup, a group of young Imperial Japanese Army (IJA) officers rose in revolt and killed a number of leaders in Japan. While they succeeded initially and were supported by officers associated with the Imperial Way Faction,³ Emperor Hirohito was furious with the rebels. The rebels surrendered on 29 February. This provided the basis for a purge of Imperial Way members from the military. It led to a “unity” cabinet and the end of political

parties by the Imperial Rule Assistance Association⁴ in 1940.

This may have accelerated the movement towards war. The Control Faction⁵ in the Army believed in a military solution to secure resources in Southeast Asia and Oceania. The Imperial Way, however, had focused first on national development rather than expansion. This approach might have led to economic cooperation with China, rather than war.

At least seven weeks before the coup began, the telephones of the masterminds behind the coup were intercepted by Ministry of Communications officials and the military police. Although this fact was kept secret, 20 wiretapping records were discovered in the broadcast centre at NHK, Japan's broadcasting corporation, in 1977. These were shared with the public in the documentary *Martial Instructions to Monitor Phones*, broadcasted on 26 February 1979.

According to a 2007 book by Seiichi Nakata,⁶ the director of the documentary, an extraordinary cabinet meeting held immediately after the outbreak of the coup decided on the wiretapping, even while recognising it as illegal under the Constitution of the Empire of Japan.⁷ However, it became clear that the wiretapping began seven weeks before the incident.⁸ In other words, the Ministry of Communications had been wiretapping without telling other cabinet members.

Moreover, the Imperial Way Faction is thought to have anticipated the possibility of a coup by young Imperial Way officers several years before the incident. In fact, Major Katakura and others wrote a document that served as an outline for countering a coup and using the subsequent repression to establish more political power.⁹ The “outline” includes detailed ideas and measures to be taken to reconstruct politics, diplomacy, defence, the economy, social policy and education, as well as how to manipulate public opinion. Many of these plans were realised by the Control Faction after the coup.¹⁰

The wiretapping records did not only infringe on privacy, but included identity theft and impersonation to falsely implicate someone.¹¹ For example, Kita Ikki, a national socialist intellectual who influenced the Imperial Way Faction, but was not directly

involved in the coup, was sentenced to death as one of the coup participants, and shot five days later. In this case, there is a wiretapping recording made on 28 February of someone pretending to be Kita Ikki, who at that time was already in prison. The person was involved in a smear campaign to paint Kita as the mastermind behind the rebellion, foreseeing the possibility of the recording becoming evidence in court.¹²

What is the lesson that we can learn from these facts? Speaking directly, unchecked, authorities have the potential to corrupt endlessly and may drive society into a dangerous situation. Moreover, surveillance can be too powerful and paranoid, and can result in the fabrication of crimes, instead of assisting legitimate criminal investigation.

By comparing these two periods, we can learn lessons from history and how we should engage the new political administration on issues of communications surveillance and transparency.

The meaning of the surveillance in the present age

Now, if we turn back to today, we can easily see how the need for surveillance has spread into new terrain – including the mass surveillance of citizens online. In part this has prompted the need to revise the Wiretapping Law.

At the House of Councillors plenary session on 12 August 1999, the Wiretapping Law was passed by a majority vote, including the Liberal Democratic Party, the Liberal Party and the Komei Party, and was enforced in August 2000. Since then, the number of wiretapping investigations conducted is reported in parliament every year – it currently stands at about ten a year.

Although it is a legislator's view that emails are also included under the definition of “communication” in the Wiretapping Law, no interception of emails has been reported in parliamentary reports.

However, it is possible to presume that an email delivered to a mail server has ended its “communication” legally, even if the user has not read the email. If so, emails may be confiscated without restriction through simple search and seizure or inspection.

Furthermore, it became possible to “seize” emails on a mail server from a remote personal computer or mobile phone after a Criminal Procedure Code revision.

The Legal System Investigation Commission is considering a revision of the Wiretapping Law. A reform bill is likely to be submitted to an

extraordinary session this autumn, or to an ordinary session of parliament next year. The following is being considered:

- Expanding the ability of authorities to carry out wiretapping.
- Abolishing the need for an employee of a communications company to be present, enabling authorities to intercept communications with a court order using encryption technology and a key.
- Allowing authorities to intercept conversations through “bugging”. The ability to bug a room or other location is a serious concern because all the conversations held in that location will be monitored, and it will become legal to break into a location such as a building and install the bugging devices.

Conclusions

We need to recognise that democracy in Japan is under critical pressure. The government and others create public anxiety, either to do with potential conflict with another country, or within the country, and surveillance is enhanced.

Moreover, many in the mass media have not sufficiently served as a watchdog over authorities or responded to the people's right to know without yielding to pressure from authorities.

The internet, which we use every day, offers the possibility of sharing vital information and promoting a free way of thinking. However, regrettably, the internet itself also now serves as a tool for mass surveillance.

In particular, there is a huge risk in “big data”. It will be possible to identify an individual if data which looks harmless is collected in large quantities. Furthermore, when targeted at a specific individual, the possibility of this leading to a serious invasion of privacy is high.

It is not necessarily the case that Japan will slip into fascism again, but this could be the case, even if democracy has been established. Germany gave Hitler the post of chancellor under the Weimar Constitution. Once we have decided that we will never repeat the past, it is very important for us to learn how fascism rose before World War II.

The Japanese constitution declares: “We, the Japanese people, desire peace for all time and are deeply conscious of the high ideals controlling human relationships, and we have determined to preserve our security and existence, trusting in the justice and faith of the peace-loving peoples of the world.” Japan did not become involved in a war for 69 years after World War II, thanks to this pacifism.

2 en.wikipedia.org/wiki/Imperial_General_Headquarters
3 en.wikipedia.org/wiki/Imperial_Way_Faction

4 en.wikipedia.org/wiki/Imperial_Rule_Assistance_Association
5 en.wikipedia.org/wiki/T%C5%8Dseiha
6 Nakata, S. (2007). *Wiretapping in February 26th Incident* [Tocho 2.26 Jiken]. Tokyo: Bungei Shunju.
7 Ibid., p. 45-46.
8 Ibid., p. 91.
9 Ibid., p. 77.
10 Ibid., p. 78.
11 Ibid., p. 93.

12 Ibid., p. 158-161.

Surveillance is engendered by distrust of others. If a fellow creature's mutual distrust and fear develop, war will break out. Human beings will not be able to survive if they cannot build a society based not on distrust and fear but on trust and cooperation.

Action steps

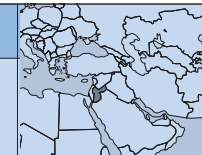
The following actions steps are suggested for Japan:

- Push for transparency in government.
- Establish a privacy commissioner system which is fully independent from the government.

- Advance democracy through the reform of the mass media, promoting alternative media and educating the public in media literacy.
- Abolish laws that aim to surveil and control people.
- Promote and campaign for privacy in communications.
- Conceive of a society based on trust and cooperation, not distrust and fear.

JORDAN

Confiscating the carrier pigeon: Jordan's response to online surveillance



Alarab Alyawm
Yahia Shukeir
alarabalyawm.net

Introduction

Jordan is a small kingdom with around seven million people located in the turbulent Middle East. This small country has two famous features: Petra, one of the new Seven Wonders of the World, and the Dead Sea, which is the lowest sea on the planet (396 metres below sea level). Many historians believe that the Arabic calligraphy was shaped largely in Petra.

Jordan has a reputation for collecting information on every Jordanian from the day of his or her birth. The General Intelligence Department (GID) – known as the *mukhabarat* – is considered a megastore of information. Even before the so-called “defensive democratisation in Jordan”¹ started in the early 1990s, there was a strong belief that the “walls had ears” and that the GID collected daily data on Jordanian citizens, monitoring phone calls, emails, text messages and social media accounts. It then stores the information for years. Such surveillance is aimed at preserving “national security” in the broader sense of the phrase, or to trace particular criminal suspects – but it is also often political in nature.

While some governmental interference in communications may be necessary for preventing terrorism, *carte blanche* power may lead to the violation of users’ privacy. It is believed that security services closely monitor online content in Jordan. In a 2010 case that strengthened these suspicions, Jordanian college student Imad al-Ash was sentenced to two years in prison after security forces accused him of insulting the king in an instant message to a friend.²

Policy and political background

Seventy-three years ago, Jordan passed a bylaw on carrier pigeons (No. 810 of 1941). Article 2 of the

bylaw – which was no doubt related to the eruption of World War II – established that, except for official bodies, it was prohibited for anyone to own carrier pigeons. Those that did were asked to hand them over at the nearest army base within ten days of the bylaw being passed.

The spirit of this bylaw is still behind many of the monitoring practices of the Jordanian government, whether the communication channel is old media like print and audiovisual or new media.

Like many countries in the region, Jordan was hesitant about exactly how to meet the challenge of new technology and whether to respond in a reactive or proactive way when it came to regulating the internet. With the increasing demand for social media, Jordan has expanded control over the internet. Despite suspicions of active monitoring, access to internet content in the kingdom remains largely unfettered, with filtering selectively applied to only a small number of sites. However, this access is tolerated by the government, rather than guaranteed by rule of law. Jordan ranked 38th out of 99 countries on the World Justice Project’s Rule of Law Index.³

Harassment, intimidation and attacks

Jordanian journalist Alaa’ Fazzaa’ was arrested on 9 June 2011 by orders of the State Security Court (SSC), a special military court, over news he published on his electronic news site (www.allofjo.net)⁴ sharing content from a Facebook page calling for the reinstatement of Prince Hamzah as Crown Prince. Fazzaa’ was harassed and intimidated until he was obliged to flee to Sweden in February 2012, seeking political asylum.⁵ News websites have also been subjected to hacking attacks after posting controversial material. For instance, in February 2011, *Ammon News* had its website hacked after publishing a call for reform by tribal leaders. The hackers posted the following text on the website’s front page: “This site was hacked because you work against the security of Jordan.”⁶ The Islamic

1 Robinson, G. E. (1998). Defensive democratization in Jordan. *International Journal of Middle East Studies*, 30(3), 387-410. journals.cambridge.org/action/displayAbstract?fromPage=online&aid=5195724

2 ar.ammannet.net/news/111695

3 World Justice Project. (2014). *Rule of Law Index 2014*. worldjusticeproject.org/sites/default/files/files/wjp_rule_of_law_index_2014_report.pdf

4 khabarjo.net/jordan-news/10397.html

5 US Department of State. (2012). *2011 Human Rights Reports: Jordan*. www.state.gov/j/drl/rls/hrrpt/2011/nea/186431.htm

6 www.ammannonews.net/article.aspx?articleNO=79822

TABLE 1.					
Freedom of expression indicators during the last five years					
	2010	2011	2012	2013	2014
RSF press freedom ranking ¹ (179 countries)	120	128	128	134	141
Freedom House media freedom ranking ² (197 countries)	140 Not free	141 Not free	144 Not free	145 Not free	155 Not free
Freedom House internet freedom ranking ³ (91 countries)	N/A	42	45	46	N/A
1. en.rsff.org/press-freedom-index-2011-2012,1043.html 2. www.freedomhouse.org/report-types/freedom-press#.UzWLSaK9aag 3. freedomhouse.org/report/freedom-net/2011/jordan#.UzW_BaK9aag					

Brotherhood website (www.ikhwan-jor.com) has also been hacked several times.⁷

On 20 February 2012, in an incident reflecting an assault on free expression, an unknown assailant stabbed female blogger and university student Inas Musallam in the stomach with a knife. The assault occurred shortly after she published a blog post criticising Prince Hassan, a former crown prince and uncle to the King of Jordan, for derisive comments he made about pro-reform protesters. Local and international human rights watchdogs condemned the attack. The Public Security Directorate (PSD) confirmed the attack, but alleged Musallam had psychological problems and conflicts with other students, and insinuated that a small amount of drugs had been found in her possession. Human Rights Watch said in a statement that Jordanian authorities should focus on “finding Inas Musallam’s attacker”⁸ – but at the time of writing, Jordanian police have not managed to bring the perpetrators to justice.

While websites usually receive “friendly calls” from officials or security persons requesting that some content be deleted, undesirable articles are forcibly deleted. It is also believed that some governmental agencies hire internet commentators to post comments favourable towards the government in an attempt to influence public opinion, glorifying the Jordanian leadership, criticising the opposition or attacking authors who criticise the government.

Moreover, citizens have reportedly been questioned and arrested for web content they have authored. Physical harassment and cyber attacks against bloggers and staff of online news websites

happen frequently. Such attacks have a chilling effect on internet users.

Striking a balance with online freedoms

All the above-mentioned stories have negatively affected Jordan’s ranking in different freedom of expression indices. Jordan’s scores in the last five years in reports published by Reporters Without Borders (RSF) and Freedom House are illustrated in Table 1.

In October 2011, Jordan adopted amendments to its constitution to improve general freedoms in response to the Arab Spring demonstrations. The new amendments included the creation of a constitutional court, and more guarantees of civil rights and liberties. The amendments touched directly or indirectly on internet freedom. Specifically, terms such as “mass media” and “other means of communication”, which likely encompass online media, were added to provisions that protect freedom of expression and concomitantly allow for its limitation during states of emergency (Article 15).

How to strike the balance between competing rights: the right to privacy and protecting others’ rights and national security?

The Jordanian Constitution provides such balance in the following articles:

Article 7:

1. Personal freedom shall be guaranteed.
2. Every infringement on rights and public freedoms or the inviolability of the private life of Jordanians is a crime punishable by law.

Article 18: All postal and telegraphic correspondence, telephonic communications, and the other communications means shall be regarded as secret and shall not be subject to censorship, viewing, suspension or confiscation except by a judicial order in accordance with the provisions of the law.

Article 128: The laws issued in accordance with this Constitution for the regulation of rights and freedoms may not influence the essence of such rights or affect their fundamentals.

The above-mentioned articles meet the first three principles of the International Principles on the Application of Human Rights to Communications Surveillance (IPAHRCS): legality, legitimacy and necessity.

Political news websites are flourishing in Jordan because the “old media” are considered less free in reporting corruption and wrongdoing by the government. However, the Press and Publications Law No. 8 of 1998 was amended in September 2012, requiring news websites to obtain licences in order to continue to operate in the country, which severely restricts free speech and expression online.

Whenever there is government there are laws to restrict dissent; but the law does not give the government a trump card to curb freedom of expression until it has proof of an overriding legitimate aim. The law requires all news websites to be legally registered and the editors-in-chief of the sites must be members of the Jordan Press Association. The result is a form of cloning old laws to control new media or a “recycling [of] old laws”.⁹

Online editors and site owners are liable for comments posted by other users on their platforms. Websites must keep a record of all comments for six months after initial publication and refrain from publishing any “untruthful” or “irrelevant” comments.

The amendments enable the director of the Press and Publications Department (PPD) to block any website for failing to obtain a licence. Historically, the PPD constituted the principal tool used by successive Jordanian governments to control the old media and control the content of new media as well. The PPD instructed internet service providers to block over 200 websites last year. The blocked websites were mostly critical of the government. Conversely, websites that are friendly to the government are tolerated.

Many national and international organisations condemned the decision.¹⁰ Under international best

practices, states should refrain from adopting separate rules limiting internet content.¹¹

In May 2011 the United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, submitted a report to the UN Human Rights Council.¹² The Special Rapporteur considers cutting off users from internet access, regardless of the justification provided, including on the grounds of violating intellectual property rights law, to be disproportionate and thus a violation of Article 19, paragraph 3, of the International Covenant on Civil and Political Rights (ICCPR). The ICCPR is an international binding treaty for almost 167 state parties, including Jordan.

Jafranews publisher Nidhal al-Faraneh and editor Amjad Muala were arrested for more than three months in 2013, accused of harming relations with a foreign country for publishing the link to a YouTube video which showed a man – purportedly a member of the Qatari royal family – lounging, dancing and showering with several women.¹³

Many Jordanians do not have home internet. They depend on internet cafés to communicate with each other. The Jordanian government has passed regulations to monitor internet cafés. The Regulations Governing Internet Cafés¹⁴ stipulate that internet café owners must be “Jordanians of good repute”, who have never been charged with immoral crimes or fraud. Internet café owners are obliged to monitor users by CCTV, register the names and identity numbers of users, allocate an IP address to each computer, and keep a monthly record of the websites browsed by visitors.

Article 29 g of Telecommunications Law No. 13 of 1995 and its amendments states that the licensees have a “commitment to offer the necessary facilities to the competent parties to implement the judicial and administrative orders related to tracing the telecommunications specified in those orders.”

Such regulations and practices clearly violate IPAHRCS, especially principle 13.

⁷ www.ammonnews.net/article.aspx?articleno=131313

⁸ Human Rights Watch. (2012, February 26). Jordan: Advocate of a republic jailed. *Human Rights Watch*. www.hrw.org/news/2012/02/26/jordan-advocate-republic-jailed

⁹ www.jordanzad.com/print.php?id=93318

¹⁰ Jordan Open Source Association. (2013). The Jordan Open Source Association deplores censorship of news websites. jordanopensource.org/article/jordan-open-source-organisation-deplores-censorship-news-websites; Greenslade, R. (2013, June 4). Jordan blocks 200 news websites. *The Guardian*. www.theguardian.com/media/greenslade/2013/jun/04/freedom-of-speech-jordan

¹¹ Joint London Declaration, 2001, UN Special Rapporteur, OAS, OSCE. www.osce.org/fom/99558?download=true

¹² Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, Human Rights Council, Seventeenth session Agenda item 3, United Nations General Assembly, 16 May 2011. www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf

¹³ www.jfranews.net

¹⁴ Published in Official Gazette No. 5034 on 1 June 2010. www.pm.gov.jo/arabic/index.php?page_type=gov_paper&part=3&id=5034

Conclusions

The media are often described as the public “watch-dog” or even as the “fourth estate”. The power of the media to influence public opinion makes them an attractive target for illegitimate control. Governments often seek to transform the media from watchdog to lapdog. New media are part of the information society and offer a huge opportunity to consolidate democracy and to promote development. The government should not consider new media a challenge but rather an opportunity.

Despite *de jure* and Jordanian constitutional guarantees of freedom of expression and protecting citizens’ privacy, several *de facto* laws remain on the books. It seems that what the constitution gives with one hand, the government takes with the other, contrary to the positive obligations placed on the state to guarantee freedom of opinion and of the media.

Jordan reacted to the potential of new technology, especially seen during the Arab Spring, by using technology to trace the online activities of citizens and control the flow of information. Collecting data is not limited to those suspected of criminal wrongdoing, but extends to all citizens.

The government also uses laws to punish activists when they criticise it or top officials. Physical harassment and cyber attacks against bloggers and staff of online news websites hamper activists from expressing their views freely. Excessive sanctions exert a chilling effect on freedom of expression, which violates the principle of proportionality.

Action steps

In emerging democracies, introducing good laws is the first step to promote independent, pluralistic and professional media as a fundamental infrastructure of good governance. It is time to take into consideration the following steps in Jordan:

- Jordan should respect its international obligations, especially Article 19 of the ICCPR and its interpretation.
- Government interference may be legitimate in exceptional cases if a “pressing social need” overrides others’ privacy to protect national security or prevent a crime. The government has to prove the legality of interference before a designated court to get permission to collect private information.
- Jordanian media laws need major surgery and comprehensive review; criminal law rules affecting freedom of expression, including laws protecting national security, should be clearly defined.
- The Regulations Governing Internet Cafés need to be abolished, as they broadly limit access to information without pressing social need.
- The Cyber Crimes Law must be amended to meet international standards in striking a fair balance between respecting freedom of information and penalties for abuse.
- Jordan should withdraw the need to license websites with the government, as it is unreasonable and restricts an individual’s access to the internet.
- Jordan should pass a data protection act to fill the existing gap in protecting citizens’ privacy.

KENYA

In surveillance a panacea to Kenya’s security threats?



Kenya ICT Action Network (KICTANet)
Victor Kapiyo and Grace Githaiga
www.kictanet.or.ke

Introduction

Kenya is located in East Africa and has an estimated population of over 43 million people.¹ The country has, according to recent estimates, 31.3 million mobile subscribers and 19.1 million internet users.²

Despite the country’s relative peace, Kenya has since 1975 fallen victim to a number of sporadic terrorist attacks. And, since the 2011 Kenya Defence Forces (KDF) incursion in Somalia,³ terrorist attacks in retaliation by groups such as Al Shabaab have increased, taking the form of grenade attacks or indiscriminate shooting, with the most recent incidents being the Westgate Mall siege,⁴ the Gikomba grenade attack,⁵ and the Mpeketoni massacre.⁶ These incidents have raised public concern over Kenya’s preparedness to combat terrorism.

In 2010, the country adopted a new constitution, which provides an expansive bill of rights, including, among others, privacy rights. However, the country still lacks dedicated privacy legislation following the state’s repeated failure to adopt the Data Protection Bill 2013.⁷ In 2012, parliament passed the much-criticised Prevention of Terrorism Act,⁸ which provides the legal framework for counter-terrorism activities.

This report seeks to assess the implications of the government’s response to terrorism through its proposal to introduce and adopt surveillance technology in major towns as a measure to avert future terror attacks.

Policy and political background

In its manifesto,⁹ the Jubilee Government, elected in March 2013, proposed the use of CCTV cameras in fighting crime and a “buy Kenyan” procurement policy as solutions to Kenya’s security problems. In this regard, in May 2014 it contracted Safaricom Limited¹⁰ to build the Integrated Public Safety Communication and Surveillance System (IPSCSS) to help security forces fight crime.¹¹

Opinion is divided – including in discussions on KICTANet¹² – on the appropriate ICT solutions to deal with the country’s rising security problems. Some support the introduction of a Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) system, such as has been implemented in the US and Israel.¹³

However, some feel that technology alone is insufficient to counter terrorism.¹⁴ They argue that the government should sort out the basics and invest in police reforms, attitude and behaviour change, police communication, police coordination and response to crime, anti-corruption measures, forensics, and effective prosecution of cases.

The project proposed by the Jubilee Government has been criticised as a continuation of the now well-established government approach of unsuccessfully throwing technology at problems without a corresponding re-organisation of bureau-

1 data.worldbank.org/country/kenya
2 The Kenya National ICT Masterplan 2013-2017, p. 16. <https://www.kenet.or.ke/sites/default/files/Final%20ICT%20Masterplan%20Apr%202014.pdf>
3 The Kenya Defence Forces incursion into Somalia sought to quell the Al Qaeda-linked Al Shabaab militant group under Operation “Linda Nchi” (Protect Country).
4 This occurred in September 2013, resulting in the death of 67 people and the wounding of 175 people. Westgate Shopping Mall attack. en.wikipedia.org/wiki/Westgate_shopping_mall_attack
5 May 2014, resulting in the death of 10 people and the wounding of 70 people. Samwel, O. (2014, May 17). 10 killed and 71 injured in Gikomba terror attack. *The People*. www.mediamaxnetwork.co.ke/thepeople/76951/ten-killed-71-injured-gikomba-terror-attack
6 June 2014, resulting in the death of 60 people. Ongiri, I., & Namunane, B. (2014, June 17). Uhuru blames massacre on tribalism, hate politics. *Daily Nation*. www.nation.co.ke/news/Uhuru-blames-massacre-on-tribalism--hate-politics/-/1056/2352306/-/www11az/-/index.html
7 www.cickkenya.org/index.php/component/k2/item/download/299_b3de9506b20338b03674eacd497a6f3a
8 kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/PreventionofTerrorism_No30of2012_.doc

9 Jubilee Coalition. (2013). *Transforming Kenya: Securing Kenya’s Prosperity, 2013-2017*. issuu.com/jubileemanifesto/docs/jubilee_manifesto/3
10 The leading mobile telecommunication network operator in Kenya. www.safaricom.co.ke
11 PCSU. (2014, May 14). Integrated communication, surveillance system to boost security. *Capital FM*. www.capitalfm.co.ke/business/2014/05/integrated-communication-surveillance-system-to-boost-security
12 Online discussion on Security Situation in Kenya. www.kictanet.or.ke/?p=20030
13 Ibid., Gichuki John Chuksjonja via KICTANet.
14 Ibid., John Walubengo via KICTANet.

cratic procedures.¹⁵ Similar projects include the primary school laptop project, so-called “digital speed governors”,¹⁶ cashless payment for public transport, speeding cameras, biometric voter registration, electronic voting, and the electronic transmission of election results.

The proposed surveillance project

The IPSCSS¹⁷ will result in the installation of 1,800 CCTV cameras with face and motor vehicle number plate recognition capabilities in strategic locations in Kenya’s two big cities of Mombasa and Nairobi; setting up a command and control centre where footage from the CCTV cameras and handheld devices will be relayed in real time; a video conferencing system connecting 195 police stations; with high-speed internet; the development of a 4G LTE¹⁸ network for the police with 80 base stations; supplying the police with 7,600 radio communication devices with SIM cards and photo and video capability; and linking 600 police vehicles to the command and control centre.

The goal of the project is to, among other things, enable security agents to communicate better and boost their capacity to fight terrorism.¹⁹ The government has also put in place a National Cyber Security Strategy²⁰ to counter the ever-evolving cyber threats.

Safaricom Limited was single-sourced to develop the project, expected to cost 14.9 billion shillings (USD 169.6 million),²¹ which will go up to 18.8 billion shillings (USD 214 million) after taxes.²² Safaricom is expected to provide maintenance and support

over a five-year period at a cost of 440 million shillings (USD 5 million) annually.²³

The project has caused a lot of controversy. It has emerged that it is similar to a previous controversial tender, which was cancelled, pitting Chinese firms Huawei and ZTE against each other. These firms are currently embroiled in litigation over the issue.²⁴ Further, the decision to single-source the tender and award it to the mobile provider Safaricom has resulted in the suspension of the project by the Kenyan National Assembly’s Committee on Administration and National Security. This is due to queries over the project cost, the choice of Safaricom as the supplier, its technical capacity, and its foreign ownership. Other queries relate to the opaqueness of the procurement and possible violation of procurement law, corruption allegations, and the secrecy, speed and purported urgency of the procurement.²⁵

Implications of the proposed surveillance project

This section focuses on the implications of the proposed surveillance project, and, more particularly, the impact that the use of CCTV with facial recognition technology has on privacy rights guaranteed in the Constitution of Kenya.

Facial recognition technology enables the identification or authentication of individuals by comparing their face against a database of known faces and searching for a match.²⁶ The process requires a computer to find a face in the image, and then create a numeric representation of the face based on the relative position, size and shape of facial features. Thereafter, the numeric “map” of the face in the image is compared to a database of images of faces, such as a national identification database.

The use of such technologies is on the increase, and there is now widespread use and application in law enforcement, border control, the military, casinos, on mobile phones, and on social media sites such as Facebook. However, there are still concerns over the introduction of CCTV cameras with facial recognition capacity in fighting crime in Kenya.

Article 31 of the Constitution of Kenya provides for the right to privacy, which includes the right for a person not to have their person, home or property searched; their possessions seized; information relating to their family or private affairs unnecessarily acquired or revealed; or the privacy of their communications infringed on. Further, Article 24 provides for the limitation by law of a right or fundamental freedom, but only to the extent that it is reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom, taking into account all relevant factors.²⁷

Section 35 of the Prevention of Terrorism Act limits the constitutional right to privacy, but only for purposes of investigating acts of terrorism; the detection and prevention of a terrorist act; and ensuring that the enjoyment of rights and fundamental freedoms by an individual does not prejudice the rights and fundamental freedom of others.

The proposed Data Protection Bill, 2013, does not recognise images or video recordings of an individual as personal data. However, the bill reinforces the right to privacy and provides best practices and principles in data protection compliance, and regulates the collection, retrieval, processing, storage, use and disclosure of personal data. In these circumstances, the introduction and use of facial recognition technology in the absence of clear regulation means there is hardly any protection from the abuse of collected images.

The government has maintained that the legitimate aim of the project is to enable law enforcement to identify terrorists. However, this goal presupposes the knowledge of the identity of the terrorists, which is debatable. As a result, the use of the technology opens the system up for abuse and application in a manner that is discriminatory. Even before the introduction of CCTVs, Kenyan police conducted raids targeting persons of either Somali heritage, Muslim faith or both. The unregulated use of CCTV cameras will only catalyse such profiling.

While the use of facial recognition technology has its benefits, its unregulated use may infringe

upon human rights. It has been reported that the government does not have a database of photos to use to compare their results with, as the current photos on IDs are unintelligible to computers.²⁸ As such, without such a database, it is not meaningful to implement such a system, especially in light of the other security needs and priorities.

The use of facial recognition technology will allow the identification of any person by name and in secret from a photo taken on the street, from the internet or other sources such as social media sites like Facebook. In addition, it will allow the police to capture images *en masse*, and maintain a photo and video database of the political and non-criminal activities of anyone. This poses threats to freedom of expression and association. Moreover, there is no limitation on the scale of surveillance that the CCTV system will cover.

The use of the technology also poses challenges to due process, as neither judicial authorisation nor the consent of the individual is required for the surveillance, opening up the system to illegitimate access. This means that law enforcement, in the absence of clear guidelines and safeguards, can abuse the system, and without any legitimate reason or cause, covertly use facial recognition on anyone without their permission, without any meaningful transparency or accountability, and for unjustified purposes for which the system was not originally intended.

Additionally, the technology will allow the state to tap into the existing databases and use facial recognition to identify people using their national identification records or the Independent Electoral and Boundaries Commission biometric voter register.

It should be noted that there is no independent public oversight body to regulate how the information collected will be managed. While the Independent Policing Oversight Authority²⁹ has been established, it has a limited mandate that focuses on investigation of complaints related to disciplinary or criminal offences committed by members of the National Police Service, and can only make recommendations based on its findings. Further, while the Data Protection Bill proposes to confer to the Commission on Administrative Justice the mandate and responsibility to enforce its provisions, the bill is yet to be passed and the Commission cannot therefore assume such functions.

15 Walubengo, J. (2014, June 17). Without changes to policing, Safaricom’s cameras may struggle to deliver. *Daily Nation*. www.nation.co.ke/oped/blogs/dot9/walubengo/-/2274560/2351214/-/11w8ih4z/-/index.html

16 Gerald Andae, G. (2014, January 1). Agency orders matatus to install new speed governors. *Business Daily Africa*. 1 January 2014, accessed 19 July 14, www.businessdailyafrica.com/Agency-orders-matatus-to-install-new-speed-governors/-/539546/2131568/-/ccfie9/-/index.html

17 The National Police Integrated Public Safety Communication and Surveillance Project; see also: Wokabi, C. (2014, June 14). Safaricom to face MPs over Sh15bn security contract. *Daily Nation*. www.nation.co.ke/news/Safaricom-to-face-MPs-over-Sh15bn-security-contract/-/1056/2349044/-/mx7va5/-/index.html

18 <https://sites.google.com/site/ltencyclopedia/home>

19 Daily Nation. (2014, May 13). Why State House made a call to Safaricom chief over insecurity. *Daily Nation*. www.nation.co.ke/news/Why-State-House-made-a-call-to-Safaricom-chief-over-insecurity/-/1056/2313756/-/ybd3dt/-/index.html

20 www.icta.go.ke/wp-content/uploads/2014/03/GOK-national-cybersecurity-strategy.pdf

21 Calculated at a rate of 87.94 Kenyan shillings (KES) per 1 USD.

22 Ngirachu, J. (2014, July 1). Safaricom security tender to be audited, says Rotich. *Daily Nation*. www.nation.co.ke/business/Safaricom-security-tender-to-be-audited-says-Henry-Rotich/-/996/2368428/-/wyzsp2/-/index.html

23 Kiplangat, J. (2014, June 18). Safaricom to be paid Sh440m every year. *Daily Nation*. www.nation.co.ke/news/Safaricom-to-be-paid-Sh440m-every-year/-/1056/2353672/-/b1ff14z/-/index.html

24 Wokabi, C. (2014, May 13). Sh14bn Safaricom deal to boost war on terror. *Daily Nation*. www.nation.co.ke/news/Sh14bn-Safaricom-deal-to-boost-war-on-terror/-/1056/2313684/-/afydehz/-/index.html; see also: Teyie, A. (2014, July 5). Intrigues of lucrative government tenders. *Daily Nation*. mobile.nation.co.ke/news/Intrigues-of-lucrative-government-tenders/-/1950946/2373320/-/format/xhtml/-/sgsya3/-/index.html

25 Wafula, C. (2014, June 5). Safaricom security deal placed on hold. *Daily Nation*. www.nation.co.ke/news/politics/Safaricom-security-deal-placed-on-hold/-/1064/2338948/-/eqcohoz/-/index.html; Ngirachu, J. (2014, June 4). Three MPs question Safaricom security deal. *Daily Nation*. www.nation.co.ke/news/politics/Three-MPs-question-Safaricom-security-deal/-/1064/2336670/-/2t3x1vz/-/index.html

26 Office of the Privacy Commissioner of Canada. (2013). *Automated Facial Recognition in the Public and Private Sectors*. www.priv.gc.ca/information/research-recherche/2013/fr_201303_e.asp

27 The relevant factors include, among others: the nature of the right, purpose and extent of limitation; the existence of less restrictive means to achieve the purpose; and the need to ensure the enjoyment of rights does not prejudice the rights of others.

28 Odongo, W. (2014, June 8). Cameras will not save us. *Daily Nation*. www.nation.co.ke/lifestyle/Cameras-will-not-save-us/-/1190/2341040/-/b7190pz/-/index.html

29 ipoa.go.ke/index.php/functions-of-authority

Lastly, the fact that Safaricom, which is Kenya's largest telecommunications service provider, is building the system raises doubt about the integrity of the system, the company's independence, and the apparent conflict of interest. The company has over 20 million subscribers³⁰ whose personal information it keeps pursuant to laws requiring SIM card registration. There are fears that its role in the development of the system may compromise its independence, including that of its network. There are also worries that Safaricom will enable law enforcement to easily access its database of users to match with the facial recognition data. The company in recent times came under sharp criticism for disclosing personal information to third parties as part of its bulk SMS services, despite clear provisions to the contrary in its terms and conditions.³¹

Conclusions

It is important to note that despite the presence of constitutional guarantees on the right to privacy, the absence of a proper policy and legislative regime for privacy protection means that the use of facial recognition technology in surveillance will result in serious implications for privacy and personal safety and lead to the violation of fundamental rights and freedoms. Therefore, it is time for laws that limit the use of facial recognition data collection.

A report³² by the US National Academy of Sciences has concluded that biometric recognition technologies are inherently probabilistic and fallible. In addition, according to the Surveillance Studies Centre at Queen's University in Ontario, Canada, urban surveillance systems have not been proven to have any effect on deterring criminals.³³

Whereas fears over insecurity have led to different sectors of society welcoming the introduction of the project, it must be stated that

technology alone is insufficient to deal with crime. It can only be used to complement other initiatives by law enforcement to fight crime. Facial recognition technologies are not always foolproof or accurate. And as such, they ought to be designed and implemented with not only this in mind, but also with consideration to the social, legal and cultural factors that can affect the effectiveness and acceptance of the systems.

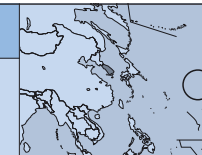
Action steps

Moving forward, the following are recommended:

- The Data Protection Bill 2013 should be amended to take cognisance of facial recognition technologies, and its adoption fast-tracked.
- There is a need for clear regulations and safeguards on the collection, access, retrieval, processing, storage, use and disclosure of personal data, including biometric information. This includes legislation that governs intermediaries.
- The proposed surveillance project should not start before the adoption of proper privacy safeguards, including the Data Protection Bill.
- A comprehensive privacy impact assessment should be conducted before developing and purchasing new technologies that will collect personal information including biometric data.
- The CCTV cameras should be located only in public spaces.
- Mechanisms should be put in place to regulate all state security, intelligence, policing, and other law enforcement agencies, to ensure they observe the rule of law and are transparent and democratically accountable.

KOREA, REPUBLIC OF

Communications surveillance in South Korea



Jinbonet

Chang, Yeo-Kyung

<http://act.jinbo.net/drupal/english>

Introduction

The Korean Railway Worker's Union (KRWU) went on strike on 9 December 2013 opposing the privatisation of the railroad. The Korean government's response was hard-line, and the police imposed widespread surveillance on the striking workers and their families.

Firstly, the police acquired all the mobile communication records of union members and their families, including schoolchildren, and tracked the real-time location of their mobile phones – the mobile service providers had offered to provide this information at 10-minute intervals for several months. The police also asked popular websites, such as game sites and internet shopping malls, to provide the real-time access IP addresses of the workers and their families. The mobile service providers also handed over the identities of about 300 to 400 people who talked on the phone with the strikers to the police, who used this information to interview the subscribers about details of their relationship with the strikers. Railway workers and human rights NGOs, including Jinbonet, filed a petition to the Constitutional Court against the real-time location tracking on May 2014.

Policy and political background

The NGOs argued that the lack of adequate legal requirements for police to access communication metadata in an investigation is unconstitutional. The authorities conduct surveillance on workers exercising their right to strike as if they were criminals – they have been maintaining a DNA database of criminals, which includes striking workers, since 2010.¹ Communications surveillance in particular, which has insufficient legal control given the rapid development of the internet and mobile technologies, has significantly extended the power of the police and the intelligence agency beyond the law.

Communications surveillance in South Korea is regulated by the Protection of Communications

Secrets Act (PCSA). The previous military dictatorship in South Korea had conducted communications surveillance for a long time without any legal regulation. The PCSA, passed in 1993 in the aftermath of a wiretapping controversy among presidential candidates, allows the intelligence agency and investigation agencies to intercept the content of communications in real time with prior court approval. The content of communications such as stored email or SMS messages is provided to agencies with a prior warrant for search and seizure under the Criminal Procedure Act. However real-time wiretapping on foreign groups and nationals can be conducted merely with the approval of the president. The intelligence agency and the investigation agencies can wiretap in real time by making use of intermediaries, including telecommunication service providers, or by using their own technologies. They can also wiretap without any permission for 36 hours if it is considered an emergency.

Since 2002 the PCSA has begun to regulate communication metadata: the record of the date and the time of communications, the IP address, the internet logs, the location of the base station or the communication device, etc. Although court permission has been required to collect communication metadata since 2005, when it is “necessary to conduct any investigation,” the permission is given without any specific restrictions. According to the Telecommunications Business Act, personal information to identify the subscriber or user such as name, residential registration number (which is the national ID number in South Korea), address, etc. is separately provided to the agencies without any permission from external supervisory agencies such as the courts.

Ex-post notification² has been implemented regarding undercover communications surveillance: users have been notified of wiretapping since 2001, of the handing over of communication metadata to agencies since 2005, and of the search and seizure of stored communications content since 2009.³ The personal information of the subscriber or the user is not included in this notification. The government

³⁰ About Safaricom, Safaricom, www.safaricom.co.ke/about-us/about-safaricom

³¹ Terms and Conditions, Safaricom. www.safaricom.co.ke/about-us/about-safaricom/terms-conditions

³² National Research Council. (2010). *Biometric Recognition: Challenges and Opportunities*. Washington, DC: The National Academies Press. https://download.nap.edu/login.php?record_id=12720&page=%2Fdownload.php%3Frecord_id%3D12720; see also: National Academy of Sciences. (2010, September 24). Automated biometric recognition technologies ‘inherently fallible,’ better science base needed. *The National Academies*. www8.nationalacademies.org/onpinews/newsitem.aspx?RecordID=12720

³³ Kelly, H. (2013, April 26). After Boston: The pros and cons of surveillance cameras. *CNN.com*. edition.cnn.com/2013/04/26/tech/innovation/security-cameras-boston-bombings

² Police notify persons of the fact that they became a target of wiretapping within 30 days after the decision is made.

³ However, in the last two cases the violator was not punished.

¹ act.jinbo.net/drupal/node/7631

TABLE 1.		
Base-station data provided to investigators		
	Base-station data	All communications metadata
Second half of 2009	15,440,864	15,778,887
2010	38,706,986	39,391,220
2011	36,800,375	37,304,882
2012	24,831,080	25,402,617
2013	15,245,487	16,114,668
SOURCE: Government of the Republic of Korea (Korea Communications Commission, the Ministry of Future Creation and Science)		

then releases statistics about the number of these cases twice a year.

Besides the above, telecommunications service providers, including intermediaries, should keep communication metadata depending on the service they offer:

- Twelve months for mobile service providers
- Six months for landline service providers
- Three months for internet service providers.

Communications surveillance:
Cases and civil society reaction

Although the PCSA was an attempt to legally regulate communications surveillance, the rapid development of the internet and mobile technologies, and the prompt adoption of them by the agencies, makes it overwhelming. A popular example is real-time location tracking of telecommunication devices.

Real-time location tracking

When the PCSA created the framework for the regulation of communication metadata in 2002, it referred to *historical* communication records. Without any external request, telecommunications service providers have kept the historical communication metadata related to billing, and they were to some extent expected to and asked to by their customers. However, agencies then started to require the “future” location information of their targets. The telecommunications service providers accepted the request, not only because collecting real-time location information and providing this was technically possible, but also because the related regulatory clause was not clearly defined on that matter.

For example, in the case of a mobile phone location, the telecommunications service provider informs a police officer of the location of the base station capturing the signal from the specified

mobile phone by text message every 10 minutes. In the case of IP addresses, the internet service provider informs the police officer when the specified ID logs in.⁴ Because telecommunications service providers in South Korea confirm their subscribers’ or users’ identities before activating mobile phone or internet services including online games, this kind of location information helps the agencies to accurately track the subject.

Real-time tracking was illustrated when a woman worker had been staging a sit-in protest at the top of a 35-metre-high crane for more than 150 days to oppose a huge lay-off of workers. “Buses of hope” had been organised to support her struggle, carrying thousands of supporters to the place of protest. To arrest those who organised the buses, the police and the prosecutors traced the real-time location of the mobile phones of the activists and their families for months. Human rights NGOs challenged this in the Constitutional Court in 2012, filing a second petition against tracing the mobile phones and internet IDs of the leaders of the KRWU and their families in 2014. Both Constitutional Court reviews are still underway.

The use of data from base stations

Another constitutional controversy surrounding communication metadata concerns the use of data from mobile base stations. The PCSA does not clearly define whether or not agencies should specify the technical scope of the request when they require a telecommunications service provider to hand over communication metadata. Consequentially, agencies are offered mobile phone numbers captured by base stations around the areas where assemblies and demonstrations take place to identify people who participate in these protests. In the case of

4 Some online game companies have subsidiaries to deal with these requests as they receive too many from the police. newsmaker. khan.co.kr/khnm.html?mode=view&code=115&artid=201112061719361&pt=nv

TABLE 2.						
Requests for telecommunications interception						
Year	Prosecution	Police	NIS	Military investigative unit or others	Total	NIS requests as % of total
2010	4	227	8,391	48	8,670	96.8%
2011	3	263	6,840	61	7,167	95.4%
2012	0	139	5,928	20	6,087	97.4%
2013	1	96	5,927	8	6,032	98.3%
SOURCE: Government of the Republic of Korea						

highly populated areas, the agency could be provided with over 10,000 mobile phone numbers from just one base station.

In 2012, a phone number of a journalist who covered an opposition party event was included in the base-station data offered to investigators. Jinbonet and the victim submitted a constitutional petition and the review is now underway.

Table 1 shows statistics on the amount of base-station data offered to investigators, compared to all the metadata handed over to authorities.

Internet packet inspection

Because the Korean intelligence agency, the National Intelligence Service (NIS), not only has the right to collect secret information but also the power to investigate, it now conducts the largest number of telecommunications interceptions among the agencies, according to official government statistics. The statistics are aggregated using the data from telecommunications service providers who have offered data to the agencies. However, the statistics on interception conducted by the NIS using its own equipment have never been open to public scrutiny and are cloaked in secrecy.⁵

Table 2 shows the overall statistics for telecommunications interceptions in South Korea compared to NIS requests.

It was first known that the NIS had been monitoring the internet network and intercepting content by using deep packet inspection (DPI) in 2009. Monitoring the internet network in this way infringes basic human rights such as the right to privacy and freedom of expression and communication, as

it allows the agency to monitor not only emails but all other interests of an internet user, including relationships and the financial life of a subject. Human rights NGOs, including Jinbonet, revealed the presence of internet packet inspection by the NIS at a media conference, held together with its victims. They also submitted a petition to the Constitutional Court when the NIS again conducted internet packet inspection in 2011 while investigating a person suspected of being in violation of the country’s national security laws.

The NIS insists that it is impossible to investigate foreign-based emails such as Gmail without packet inspection, while it can investigate domestic internet usage by approaching service providers. The constitutional review is now underway.

Provision of personal information

It is a massive infringement of human rights that internet service providers (ISPs) provide personal information of subscribers or users such as name, ID, resident registration number, address, etc. to the agencies, without any restriction. This provision has faced severe criticisms, with allegations that it is abused by authorities who deliberately target internet users who criticise the government. The fact that there have been 9,574,659 cases of personal information provided in 2013 means that the personal information of 26,232 people was provided every day, and that the details of around 19% of the total national population have already been provided in South Korea. Table 3 shows statistics on the provision of personal information.

Conclusions

The reason why stored communication metadata is offered to law enforcement agencies is because the data is needed as evidence in investigations, and these requests by authorities are allowed. However, when a crime has not yet happened, the “reserved” location data of someone is not necessary

5 In 2005, the fact that the intelligence agency had monitored CDMA mobile phones was revealed by the government. The agency had officially denied all queries from NGOs, media and the national assembly for a long time. The intelligence agency had developed tapping equipment that could be attached to the wirelines of mobile communication service providers as well as the equipment for intercepting radio frequencies. See Jinbonet. (2009). *Mobile Surveillance and the Protection of Communications Secrets Act of Korea*. act.jinbo.net/drupal/node/6306

TABLE 3.					
Provision of personal information by ISPs					
Year	Prosecution	Police	NIS	Military investigative unit or others	Total
2010	1,323,176	5,419,365	76,018	326,233	7,144,792
2011	1,295,968	3,958,055	102,979	491,989	5,848,991
2012	2,241,812	5,115,131	110,923	411,722	7,879,588
2013	2,858,991	6,230,617	113,305	371,746	9,574,659
SOURCE: Government of the Republic of Korea					

information which telecommunications service providers have to generate or keep in order to provide it to the authorities. The data is processed only to make it convenient for the agencies to electronically trace their subjects in real time. This practice goes against data protection norms which require that collecting and using any personal information should be the minimum necessary.

The data protection norms, including the country's Data Protection Act, grant many exceptions to the intelligence and investigation agencies. The data generated under these exceptions might also be used for the financial benefit of the service providers. Considering that the purpose of the constitution and international human rights law is to protect private life, personal information, and the privacy and freedom of communication from any governmental surveillance, the present legal system in South Korea, such as PCSA and the Data Protection Act, means that the government is infringing on these human rights.

Action steps

There is a serious communication surveillance crisis, not only in South Korea but throughout the whole world. As a UN resolution⁶ pointed out in November 2013, it is necessary to improve domestic laws related

6 UN General Assembly Resolution A/C.3/68/L.45/Rev.1 on "The right to privacy in the digital age", 20 November 2013. www.un.org/ga/search/view_doc.asp?symbol=A/C.3/68/L.45/Rev.1

to the protection of privacy, communication privacy and personal information in the digital age. It is essential to establish an independent body that supervises communications surveillance conducted by the intelligence agency and the investigation agencies. Neither the Personal Information Protection Commission and the National Assembly in South Korea have performed this supervisory role well enough.

Additionally, an international norm to regulate secret surveillance by intelligence agencies is needed in each country. As Edward Snowden revealed, as long as intelligence agencies across the world collect information by cooperating with or competing with each other, no citizen of any nation can be guaranteed privacy.

To achieve this, lawmakers in South Korea have to recognise the seriousness of communications surveillance and improve domestic laws. They also need to cooperate internationally to build proper international norms on the issue. Human rights NGOs will continue taking vigorous action to demand that these steps are implemented.⁷

7 Joint Statement by NGOs in the Republic of Korea on Intelligence Agencies' Internet Surveillance, 21 August 2013. act.jinbo.net/drupal/node/7636

KOSOVO

Kosovo's experience with data retention:
A case of adopting negative EU standards



FLOSSK
Arianit Dobroshti
www.flossk.org

Introduction

The Kosovo government, through the Ministry of European Integration, was in the first part of 2014 considering the third draft of a problematic drag-net electronic interception and data retention law. The adoption of the law was thwarted in large part thanks to the reaction of civil society, a European Union Court of Justice ruling that came just in time, and ultimately the disbanding of the Kosovo Parliament for early elections. It will come back.

The process highlights a case of imposing dubious standards from the European Union (EU) on a country, which often results in weak democracies and breaches of the rule of law.

Attempts to pass the law

A draft law on electronic interception and data retention was previously considered in 2012-2013, with the latest attempt being in 2014. In 2013 the second attempt was turned down by the Intelligence Agency Oversight and Security Parliamentary Committee.

The bill returned with similar problems in 2014. This time it came alongside the dialogue on visa liberalisation which the EU has been having with Kosovo for years with meagre success.¹

Currently, electronic surveillance in Kosovo is permitted through the Penal Code and the Code of Penal Procedure, provided a warrant is secured, although some have argued that more detailed rules are lacking. Kosovo has enshrined privacy in its quite modern constitution and has implemented a

1 The requirement is framed in this way: "Ensure that future legislation on interception distinguishes clearly between judicial interception and interception for intelligence services, in line with European best practices, while the provisions on data retention for law enforcement purposes comply with the EU acquis on data retention." See the Report from the Commission to the European Parliament and the Council on Progress by Kosovo in Fulfilling the Requirements of the Visa Liberalisation Roadmap, 8 February 2013. ec.europa.eu/dgs/home-affairs/e-library/documents/policies/international-affairs/general/docs/report_on_progress_on_kosovo_visa_liberalisation_en.pdf

data protection law and established a data protection agency based on EU legislation.²

As reintroduced, the bill would have given the Kosovo Intelligence Agency the ability to tap into communications networks for the purpose of recording internet and telephone metadata and content. A court warrant was not mandatory; instead, only lawful authorisation was mentioned.

The Minister of European Integration stated that the draft law had been endorsed by the EU. Emails to the EU Mission in Kosovo were not returned. Directive 2006/24/EC³ on data retention was already considered highly problematic, even in the EU countries. Article 5 on the types of data to be retained is exhaustive. They are, of course, metadata, but metadata can reveal a lot.⁴ The implementation of the Directive had been thrown out by high courts in Germany, the Czech Republic and Romania and was being contested in Austria, Ireland and Slovenia. Sweden was threatened for years with heavy fines by the European Commission to implement it, as was Romania.⁵

On 7 April, just a day before the Court of Justice of the EU (CJEU) was due to hand down its verdict on the matter of data retention, the Ministry sent a new draft to a selected number of civil society organisations. This again was in violation of consultation procedures mandated by law which stipulate publication for general public access.⁶ This draft was much more precise in language and with noticeable improvements, limiting, for example, the number of institutions that would have access to the data. Two points giving rise to concern, however, remained:

2 Kosovo has transposed EU's Directive 95/46/EC on Data Protection via Law No.03/L-172 on the protection of personal data.

3 Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

4 Leber, J. (2013, June 18). Mobile Call Logs Can Reveal a Lot to the NSA. *MIT Technology Review*. www.technologyreview.com/news/516181/mobile-call-logs-can-reveal-a-lot-to-the-nsa

5 EDRI. (2013, June 5). EC goes after governments for not implementing data retention. *EDRI*. history.edri.org/edriagram/number11.11/ec-fines-sweden-data-retention

6 Art. 32 of Regulation No. 09/2011 on Rules and Procedure of the Government of the Republic of Kosovo foresees the publication of draft normative acts for consultation.

data retention and the ability of the Kosovo Intelligence Agency to surveil without a warrant.

On 8 April, the CJEU ruled Directive 2006/24/EC on data retention invalid.⁷ The Directive was key to the data retention portion of the Kosovan draft law.

In its ruling, referring to the Directive, CJEU notes that it covers “in a generalised manner, all persons and all means of electronic communication as well as all traffic data without any differentiation, limitation or exception being made in the light of the objective of fighting against serious crime” (paragraph 57). Furthermore, “the access by the competent national authorities to the data retained is not made dependent on a prior review carried out by a court or by an independent administrative body whose decision seeks to limit access to the data and their use to what is strictly necessary for the purpose of attaining the objective pursued and which intervenes following a reasoned request of those authorities submitted within the framework of procedures of prevention, detection or criminal prosecutions. Nor does it lay down a specific obligation on Member States designed to establish such limits” (paragraph 62).

The Court cites the opinion of the Advocate General of the CJEU: “The fact that data are retained and subsequently used without the subscriber or registered user being informed is likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance” (paragraph 37). Have in mind that the Court is only addressing metadata here, unlike Kosovo’s draft law. The Court deems that by adopting the Directive, “the EU legislature has exceeded the limits imposed by compliance with the principle of proportionality in the light of Articles 7, 8 and 52(1) of the Charter [of Fundamental Rights of the European Union]” (paragraph 69). It can be concluded from the above that in the CJEU’s view, general surveillance of citizens not suspected of committing serious crimes without the authorisation of a court is neither necessary nor proportionate.

On 29 April, the Kosovo government announced that it would be sending a revised Draft Law on Interception of Electronic Communication to parliament.⁸ The draft underwent some positive changes

in light of the CJEU decision, but still had noticeable problems. Below are the significant issues.

Interception interfaces: The first major problem is the separate *interception interface* it provides to the Kosovo Intelligence Agency (KIA). While the draft requires court warrants also for the KIA, in practice the KIA would be assigned its own interface. The law calls for two types of electronic solutions: *monitoring facilities* placed at the authorised institutions that would get the feed that they have been authorised to receive upon showing the warrant, and *interception interfaces* placed at communications companies that do the actual feeding of the data. But the KIA also gets one of these interfaces at its own facility. This provides no means of control against abuse and practically gives the Agency *carte blanche* to intercept.

Data retention: This is the second major problem. Despite promises by the sponsoring Minister Vlora Çitaku⁹ and the CJEU ruling annulling the EU Directive, data retention was still present in the draft, albeit in a somewhat lighter version. Data to be retained for 12 months included a long list of metadata.¹⁰ The minister has stated that the draft has been approved by the European Commission, and EU Special Representative/Head of EU Office in Kosovo, Samuel Žbogar, stated that the law, while not perfect, meets minimum standards. It was clear that the European Commission was suggesting to Kosovo what the interpretation of the CJEU ruling was, although a public formal interpretation of the ruling by the Commission was not available.

Authorised institutions: The draft law did not limit the “special laws” that could be used for issuing warrants. This means that if passed in this form, attention would be required to make sure that other institutions do not get access using other less onerous laws through the back door.

Purpose (Art. 1 and 12.7): The EU Directive was specifically directed at fighting serious crime, although when implemented it became subject to much abuse. In the draft the reference to the Directive was expunged, but a limitation of the scope to “serious crime” was at this point introduced. This was an advance.

Notification: This draft referred to the Criminal Code and the KIA Law as two of the legal bases for getting warrants. While the Criminal Code has the concept of notification of citizens upon surveillance built in, the KIA Law does not. Therefore no citizen would be allowed to know that they had

been surveilled by the KIA, since unless otherwise expressly allowed by another law, notification is prohibited by this one. As ruled by the European Court of Human Rights,¹¹ notification is a right, hence the draft is in violation of the European Convention on Human Rights, which Kosovo has unilaterally embraced – but its citizens still cannot seek redress from the European Court of Human Rights because Kosovo is not formally a party to the Convention.

Interception assistance (Art. 9): As the draft law states, “Based on a lawful inquiry, in full compliance with the Criminal Procedure Code of Kosovo” it allows for the violation of citizens’ anonymity by requesting the identity of a suspect in preparation for a warrant. Indirectly, this article states that no warrant would be required for this procedure. Furthermore, the notification principle is once again violated in this article, as notification is expressly prohibited.

Records of interception (Art. 11 and 13): The need to keep records and provide data on the number of interception requests was a positive change in this draft. Yet this point becomes somewhat moot when considering that the KIA would have its own interface. In the reporting requirements, there are no criteria about the effectiveness and indispensability of data retained to combat crime, only on the effectiveness of the ability to provide data, which privacy advocates in Europe have argued against with regard to the Data Retention Directive.

Penalties (Art. 15): For non-compliance violations, a network operator or service provider could be fined at least EUR 86,000 and up to 7% of the annual income from their economic activity in electronic communications. There were no penalties foreseen for violations that harm the privacy of citizens, clearly erring in favour of sharing citizens’ data with the authorities.

Data transmission security standards (Art. 5.5): The draft law refers to the data security standards used by the operator and says this will be dealt with in secondary legislation.

Looking at how well written the relevant parts of the Criminal Code¹² and the Criminal Procedure

Code¹³ are, there could be only two reasons to push this new law: data retention and the extension of the KIA’s ability to tap.

Kosovo context

The power of the EU in Kosovo is immense; as a result, the new attempt to pass this law was given to the Ministry of European Integration. There was another strong reason for having this ministry sponsor the draft law: the government had twice before failed to take the draft law beyond the Intelligence Agency Oversight and Security Parliamentary Committee. Bypassing the specialists at the public security and intelligence committee was apparently part of the agenda.

Kosovo has good laws, but implementation is lacking. Since 2008 Kosovo has been unique in having a European Union Rule of Law Mission (EU-LEx) to address the shortcomings of public security institutions and the legal system. It is for this very reason that the various reports issued by the European Commission on Kosovo find faults which hamper Kosovo’s progress towards visa liberalisation with the Schengen area, as well as overall European integration.

Action steps

For new surveillance powers to be granted, all the necessary legal safeguards within a state would have to function in order to control the additional authority being provided. This situation does not currently exist in Kosovo and any move in this direction should be made with increased caution above and beyond that found in the EU member states.

The EU also has a heightened responsibility to monitor the surveillance practices of the states where it has political influence to ensure that they do not further undermine human rights, instead of merely exporting its own standards as fit-for-purpose. In the case of Kosovo, the EU should not only come out loud and clear against any sort of mass surveillance, but should also insist that the KIA abide by the same rules as other security institutions.

7 See Para. 71, Joined Cases C-293/12 and C-594/12, Requests for a preliminary ruling under Article 267 TFEU from the High Court (Ireland) and the Verfassungsgerichtshof (Austria).

8 Versions of the draft law have been distributed only via email to several non-governmental organisations and there was no official publication. The author’s copy is available here: <https://www.dropbox.com/s/9rcswy6a8bsozkv/Draft%20law%20on%20interception%20as%20sent%20to%20parliament%20-%202029%20April.doc>

9 Vlora Citaku, <https://twitter.com/vloracitaku/status/461093395017236480>

10 See note 8, Article 12.

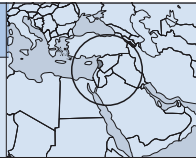
11 Boehm, F., & de Hert, P. (2012). Notification, an important safeguard against the improper use of surveillance – finally recognized in case law and EU law. *European Journal of Law and Technology*, 3(3). jlt.org/article/view/155/264

12 Republic of Kosovo. (2012). Criminal Code of the Republic Of Kosovo No. 04/L-082. *Official Gazette of the Republic of Kosovo*, No. 19.

13 Republic of Kosovo. (2012). Code Nr. 04/L-123 of Penal Procedure. *Official Gazette of the Republic of Kosovo*, No. 37.

LEBANON

Surveilling the banking sector in Lebanon



Mireille Raad

Introduction

Many argue that online privacy is a human right, while others insist that it is a negotiated contract between the state and its citizens – a contract in which citizens exchange some of their data in return for national security. So in theory – and in an “ideal state” – citizens could rely on the protection of their home governments to ensure their physical safety while also preserving their online privacy of communications, transactions, identities and speech. But to what extent can states really uphold this contract?

In Lebanon, there is an odd “ideal law” on banking secrecy dating back to 1956. This law did not create secrecy as a privilege to be enjoyed by banks, but as a duty that banks operating in the country must observe. Violation of banking secrecy is a criminal offence. However, in June 2012, Kaspersky Lab announced the discovery of “Gauss”, a complex state-sponsored cyber-espionage toolkit targeting major banks in Lebanon and parts of the Middle East. Gauss is designed to steal sensitive data, with a specific focus on browser passwords and online banking account credentials.

This cyber violation violates the Lebanese banking secrecy law and is a direct attack on a nation’s sensitive financial transactions and a critical economic organ: the banking sector is one of the few stable sectors in Lebanon and, as many argue, one of the sectors stabilising the economy. If the banking sector collapsed, the country might fall into chaos, experts say.¹

Due to the complexity and similarities between Gauss and malware like Stuxnet, Flame, Duqu and others, fingers pointed at the United States (US) and Israel, accusing them of being behind Gauss.

Background

*Lebanon is a very small country. [...] Not much you can do. It is up to major international bodies, like the UN [United Nations], Human Rights Commission or the EU [European Union] or the American people themselves to ask for a change in this behavior.*² –Lebanese Telecom Minister Nicolas Sehnaoui commenting on the Edward Snowden/National Security Agency (NSA) leaks in June 2013.

This blunt quote illustrates the simple reality that many developing countries face in a digital age when large-scale mass surveillance and spying on detailed data and sensitive transactions become an act of daily nation bullying. This problem is only accentuated by a digital divide, where most services and servers reside in developed countries; not to mention that only rich countries can actually “afford” to own and operate systems that allow them to perform such acts of mass privacy violation from the comfort of their “homeland”.

Sehnaoui’s quote comes as no surprise since Lebanon, like much of the Middle East, has a difficult recent history – it is a small diverse country amid big regional powers. Frequent invasions of this country date back to the Assyrians, Persians, Greeks, Romans, Arabs, Fatimids, Crusaders, Ottoman Turks and most recently the French and Israelis.

Recently, Lebanon has also been a focal point of larger geopolitical rivalries in the region between Iran, Saudi Arabia, Syria, Palestine, the Gulf States and of course Israel and the US. So it stands to reason that there is a long history of struggling against external spying on telecommunications and internet servers, with more than a hundred people arrested for collaborating with and spying for foreign states since April 2009.³

Tracking the malware

In June 2012, Kaspersky Lab⁴ announced the discovery of a malware toolkit spreading in Lebanon and

parts of the Middle East. This discovery was made possible only after knowledge gained by in-depth analysis and research conducted on the Flame⁵ malware.

The toolkit had different modules named after famous mathematicians and philosophers like Godel, Lagrange and Gauss. The module named “Gauss” implements the data-stealing capabilities. The Kaspersky investigation estimated that Gauss began operations in mid-2011. Its infiltration into systems is conducted in a controlled and targeted fashion, ensuring stealth and secrecy.

The main functionality of the malware includes:

- Intercepting browser history, cookies and passwords.
- Harvesting and sending detailed system configurations of infected machines, including specifics of network interfaces, computer drives and BIOS.⁶
- Infecting USB sticks (flashdrives) with a data-stealing module using the same LNK vulnerability that was previously used in Stuxnet and Flame, but in a more “intelligent” way that under certain circumstances is capable of “disinfecting” the drive.
- Listing the content of the system drives and folders.
- Stealing credentials for various banking systems in the Middle East (Bank of Beirut, EBLF, BLOM Bank, Byblos Bank, Fransabank and Credit Libanais). It also targets users of Citibank and PayPal. The online banking Trojan functionality found in Gauss is a unique characteristic that was not found in any previously known cyber weapons.
- Hijacking account information for social networks, email and instant messaging accounts.
- Installing a font called “Palida” with an unknown objective, but speculations suggest it is used to remotely detect infected machines.
- Using advanced techniques for handling high traffic load balancing, load distribution and fault tolerance known as Round-robin DNS⁷ – which suggests that the makers of the malware were expecting high traffic volumes.

- An encrypted code with an unknown objective.
- Communication with command and control servers.

The above technical specifications clearly connect Gauss to Flame – Flame is connected to Stuxnet – which prompted Kaspersky Lab to call it a “nation-state sponsored cyber-espionage toolkit”⁸ rather than a tool for criminal theft – something that gives Gauss a geopolitical dimension.

Once the news of the malware broke, the Lebanese Central Bank⁹ issued a note to all commercial banks to take the necessary measures to protect computer systems. Some bankers confidently said that they are not concerned about any virus, insisting that they had nothing to hide. “Let them [the Americans] browse our accounts. They won’t find anything suspicious because all our clients are well-known,” one banker told *The Daily Star*,¹⁰ while another denied the existence of the virus altogether.

The head of the IT department in the Central Bank of Lebanon said that the Lebanese banks had upgraded their software security systems to block any virus designed to spy on transactions and operations: “The anti-virus program blocks all known viruses and this has been going on for a long time. But the Gauss virus did not have time to inflict harm on the systems,” he said.¹¹

However, a group of independent security professionals who claim having first-hand experience dealing with the Gauss malware in Lebanese banks issued a statement¹² that was published on several Lebanese blogs. It stated that banks are still vulnerable, and raised the concern that by conveying simplistic views about Gauss, the banking sector is not truly willing to fight back.

Conclusion

Technology trumps all. In a borderless interconnected cyberspace, states – even the most tech-savvy ones – are seldom able to uphold contracts they make with their citizens on digital rights, even if they want to. This claim is backed by stories from across the globe,

¹ Dockery, S. (2012, August 11). Virus plunges Lebanon into cyber war. *The Daily Star*. www.dailystar.com.lb/News/Local-News/2012/Aug-11/184234-virus-plunges-lebanon-into-cyber-war.ashx#ixzz33c7Yh200

² Al Saadi, Y. (2013, June 13). The NSA Global Surveillance and Lebanon: ‘Not Much We Can Do’. *Al-Akhbar*. english.al-akhbar.com/node/16107

³ Ibid.

⁴ Kaspersky Lab is a Russian multinational computer security company and the world’s largest privately held vendor of software security products. https://en.wikipedia.org/wiki/Kaspersky_Lab

⁵ Flame is arguably the most complex malware ever found, and is used for targeted cyber espionage in Middle Eastern countries. [https://en.wikipedia.org/wiki/Flame_\(malware\)](https://en.wikipedia.org/wiki/Flame_(malware))

⁶ The fundamental purposes of the BIOS are to initialise and test the system hardware components and to load the operating system. <https://en.wikipedia.org/wiki/BIOS>

⁷ https://en.wikipedia.org/wiki/Round-robin_DNS

⁸ Kaspersky Lab. (2012, August 9). Kaspersky Lab discovers ‘Gauss’ – a new complex cyber threat designed to monitor online banking accounts. *Kaspersky Lab*. www.kaspersky.com/about/news/virus/2012/Kaspersky_Lab_and_ITU_Discover_Gauss_A_New_Complex_Cyber_Threat_Designed_to_Monitor_Online_Banking_Accounts

⁹ https://en.wikipedia.org/wiki/Banque_du_Liban

¹⁰ Habib, O. (2012, September 14). Lebanese banks develop anti-virus system. *The Daily Star*. www.dailystar.com.lb/Business/Lebanon/2012/Sep-14/187818-lebanese-banks-develop-anti-virus-system.ashx#axzz3AFd4RS4h

¹¹ Ibid.

¹² www.plus961.com/2012/10/no-our-banks-are-still-vulnerable-to-cyber-attacks


```
<body onload='javascript:var detective = new Detector();
if(detective.detect("Palida
Narrow"))|detective.detect("Palida"))
{window.location="PortalSecurityAlert.aspx"}'>
```

Screenshot from BLOM Bank current online banking portal (<https://eblom.blombank.com>)

stories that are similar to the Lebanese one. Many of these we have learned from the Snowden revelations.

Those revelations changed the conversation on privacy and surveillance from a government-citizen debate into an international debate between states. “Spying”, which traditionally was a “targeted” operation on specific political actors in foreign states, turned into mass surveillance and catch-all, detailed monitoring and wiretapping of terabytes of data per second.

This mass surveillance is enabled by technology and can exist only because of it. Huge amounts of data on our social interactions and economic transactions simply exist “online”. Technology, with its algorithms, cheap storage and processing cycles is able to store and “make sense” of data that is almost humanly “un-crunchable”. This data needs to be captured only once – it can be copied and can never really be “returned”.

However, technology comes with costs, ranging from research and development to the day-to-day operating costs of large systems. This only adds insult to injury by increasing the digital divide between poor and rich and enabling rich countries to have the “advantage” of big data over many other nations.

Privacy protection measures also come at a high cost for governments and the private sector. They also come with a hit on user-friendly interfaces and interactions. Security and usability have always been at odds.

The digital divide is already raising concerns and plays a major role in surveillance, since most of the services and infrastructure like internet exchange data centres are hosted in “rich” countries or owned by companies who follow the legal jurisdictions of those countries. This gives those countries easier access to large amounts of data being routed through their territories or legal reason to demand disclosure of data from companies who have to comply with their laws, not the laws its clients are subject to.

The best option that countries have to uphold their contract with their citizens and protect privacy is to try to keep as much of the data as possible within their own territories – for example, Germany and France are leading efforts to secure EU traffic by keeping it within borders. German Chancellor Angela

Merkel has called for creating a “European communications network” – something that poses a new risk of “fragmenting” the internet. In response to that call, US President Barack Obama announced the extension of US citizen privacy protections to EU citizens.¹³

This announcement shows how much power dynamics and politics are at play in international surveillance and how different people using the “open internet” – our biggest common shared resource – are not treated equally, while equality is paraded as an international human right that everyone must uphold.

Action steps

There is no direct action point with immediate outcome that can be taken to tackle extraterritorial surveillance. But here are some of the ideas that can be helpful:

- The internet is a global, open and shared resource that everyone helped build and everybody uses. The benefits of accessing the internet have been demonstrated in many studies. Data is what we share on the internet – without data and meta-data, the internet is an expensive set of cables. We should lobby to include privacy of data on the internet as a global human right, and offer easy and solid safeguards for all countries to abide by, with clear punishments for those who refuse to.
- Inform local policy makers of different research being done, especially of the International Principles on the Application of Human Rights to Communications Surveillance.¹⁴
- Localise and strengthen the ability of activists to debate these issues in each country.
- Have media discussions with the general public, especially inside the US or countries more likely to conduct surveillance.
- Increase awareness and the technical abilities to counter surveillance.

¹³ MacAskill, E. (2014, June 25). US to extend privacy protection rights to EU citizens. *The Guardian*. www.theguardian.com/world/2014/jun/25/us-privacy-protection-rights-europe

¹⁴ <https://en.necessaryandproportionate.org/text>

MEXICO

The FinFisher case



SonTusDatos

Cédric Laurant and Monserrat Laguna Osorio
sontusdatos.org

Introduction

The right to privacy is protected by the Mexican Constitution, which establishes that the privacy of one’s person, family, residence, documents or possessions cannot be violated. In addition, the constitution recognises the human rights established in it, and those included in international treaties that Mexico has signed. However, it was not until 2007 that Mexico started to regulate the area of data protection: the constitution was amended in order to guarantee the right to data protection and established that any interference in communications must be approved by a judge. In July 2010, Congress enacted the Federal Law on Protection of Personal Data Held by Private Parties (LFPDPPP). The scope of this law only applies to individuals and companies, not government and other public entities.

Policy and political background

The Federal Institute of Access to Information and Data Protection (IFAI) is the autonomous institution mandated to safeguard individual rights to data protection. In the beginning, IFAI only existed to guarantee the right of citizens to access government public information. However, since 2010 its mandate has been extended in order to guarantee the right to the protection of personal data.

In March 2013, Privacy International’s report, *The Right to Privacy in Mexico*, Stakeholder Report Universal Periodic Review 17th Session,¹ pointed to concerns over surveillance practices. It highlighted that between 2011 and 2012, the Department of Defence bought USD 350 million worth of surveillance software to be used by the Mexican Army. Of concern here is the lack of transparency on the purchase and use of this software. Recent news also revealed that

federal agencies had purchased software that might place individuals’ right to privacy at risk.

Today there is doubt about whether Mexico has adequate laws and institutions to deal with any violation of their citizens’ rights in terms of privacy and data protection, considering that the responsible party might be its own government.

FinFisher in Mexico

In March 2013, the Citizen Lab,² an interdisciplinary research centre at the University of Toronto, published an investigation about a spyware programme called FinFisher, marketed by the company Gamma International.

FinFisher is malicious software that requires the user to download fake updates from apparently reliable sources such as Adobe Flash, iTunes and BlackBerry. Once it is installed on a computer system, a third party can remotely control the user’s computer and access it as soon as the device is connected to the internet. As soon as the device becomes infected by FinFisher, the hacker who used it is able to see the user’s emails and social messaging conversations, take screenshots, obtain passwords, and switch on microphones and cameras. FinFisher cannot be easily detected by an antivirus or antispyware.

The Citizen Lab detected 25 countries with servers that host the programme.³ In Mexico, an infected server was detected at the provider UNINET S.A. de C.V., while another was detected at IUSACELL S.A. de C.V., but in Malaysia where the company has some of its servers.⁴

Previously, reports had revealed that activists and members of political opposition around the world had their phones and computers tapped because they had been infected by FinFisher. For example, in February 2013, the European Centre for

² The Citizen Lab’s areas of investigation include human rights violations in the digital environment, censorship and surveillance. <https://citizenlab.org>

³ Marquis-Boire, M., Marczak, B., Guarnieri, C., & Scott-Railton, J. (2013). *You Only Click Twice: FinFisher’s Global Proliferation*. Canada: The Citizen Lab. <https://citizenlab.org/wp-content/uploads/2013/07/15-2013-youonlyclicktwice.pdf>

⁴ Sánchez, J. (2013, July 17). Fijan plazo a UniNet y Iusacell para informar sobre FinFisher. *El Universal*. eleconomista.com.mx/tecnociencia/2013/07/17/fijan-plazo-uninet-iusacell-informar-sobre-finfisher

Constitutional and Human Rights (ECCHR), Reporters Without Borders, Privacy International, Bahrain Watch and the Bahrain Centre for Human Rights filed a complaint before the Organisation for Economic Co-operation and Development (OECD) against Gamma International with respect to it exporting espionage technology to Bahrain.⁵ The software has been used to spy on activists in Bahrain. When asked about this, Gamma International declared that they only sell FinFisher to governments. However, they admitted to having found copies of their products and stolen demos that have been used in repressive regimes.⁶

On 20 June 2013, Mexican civil associations ContingenteMX, Propuesta Cívica and Al Consumidor filed a complaint with the IFAI that resulted in the authority investigating both IUSACELL and UNINET with the aim of learning about the use of FinFisher on their servers, and to protect the personal data that might be at risk. Academics, journalists, activists and members of civil society organisations joined the complaint.⁷ A month later, Privacy International sent a letter to the IFAI supporting the investigation. The letter makes it clear that “the presence of a FinFisher Command and Control server in a country does not necessarily imply that this product is being used by Mexican intelligence or law enforcement authorities.”⁸ The ECCHR also supported the complaint by asking the IFAI to investigate the case.

At first, UNINET declared that they have no responsibility concerning the allocation of IP addresses assigned to clients, while IUSACELL claimed FinFisher was not installed on their servers.

On 3 July 2013, the Permanent Commission of the Mexican Congress exhorted the IFAI to begin the investigation, as requested by ContingenteMX, Propuesta Cívica and Al Consumidor.⁹ Seven days later,

Congress asked the Secretariat of the Interior for a detailed report on the state’s strategy for monitoring cyberspace and how it avoids infringing on user privacy rights.¹⁰ Congress also asked the Secretariat whether they had acquired the FinFisher software, and asked the Office of the Mexican Attorney General whether there had been any complaint about the wiretapping of individual communications. Neither has answered the questions.

On 11 July 2013, human rights activists from the group Civil Disobedience reported that they had found trails of the FinFisher programme on their mobile phones and computers and had received various, but undefined, threats.¹¹ The newspaper also reported that the Office of the Mexican Attorney General had spent nearly MXN 109 million (approximately USD 8 million) for the FinFisher software and about MXN 93 million (around USD 7 million) for a satellite tracking system called Hunter Punta Tracking/Locsys. Both purchases were made from the Mexican company Obses and, according to the newspaper *Reforma*, the contract was overpriced.

José Luis Ramírez Becerril, Obses’s representative, declared that the company had sold the same espionage equipment to other Mexican government agencies. But if Gamma International only sells to governments and does not have resellers, how could Obses make the deal? Due to the initial legal procedure of verification that ContingenteMX, Propuesta Cívica and Al Consumidor filed against IUSACELL and UNINET to learn about the operation of FinFisher, the IFAI also decided to investigate Obses.

In its verification of Obses, which started in May 2013, the IFAI asked the company if it had sold the FinFisher software and had provided services to the government. The information it gave was insufficient as it argued that the information was protected by rules of confidentiality. The IFAI therefore imposed a fine of MXN 1,295,200 (approximately USD 100,200) on the company for obstructing the IFAI’s investigation by not providing the full information it requested.¹²

There are records that show that, in August and September 2013, two citizens made two requests for information from the Secretariat of the Interior through the internet system INFOMEX, which is designed precisely for citizens to ask for

public information about the government. The first request asked for information about the use of the FinFisher software in government agencies.¹³ The second request asked which strategies among those that entail eavesdropping on cyberspace had been implemented and, if this were the case, what the scope of the strategies were, including the protocols and rules that were used to avoid violating users’ privacy.¹⁴ The answer to both petitions was that the information requested did not exist and it was recommended that the specific agencies involved (the Army and the Attorney General) be asked.

On 4 September 2013, WikiLeaks revealed that executives from Gamma International visited Mexico in February and April 2013.¹⁵ Carlos Gandini, high executive from that company, was in Mexico from 14 to 17 February, while Martin Muench, FinFisher developer, was in the country around 23 to 26 April. There is no information about what offices they visited. In September 2013, the Citizen Lab reported that the FinFisher command and control centres in the IP addresses that Citizen Lab had previously detected were still active: FinFisher was still installed and operating on the Mexican servers that Citizen Lab had reported on back in March 2013.¹⁶ Since September 2013, there has been no new information about the presence of FinFisher on Mexican servers. On 4 August 2014, a hacker with the nickname of PhineasFisher announced that he had hacked FinFisher¹⁷ and posted on the internet various confidential documents. Among these were what seem to be authentic client records, manuals, brochures, price lists and source code. According to a description of the leaked information,¹⁸ it is interesting to note that, in the list of customers, the username “Cobham” appears, probably referring to the Cobham Group, whose division “Cobham

Defence Electronics” builds products for defence, medical, industrial and commercial applications in Mexico.¹⁹

Analysis of the situation

Mexico has one single federal law regulating the area of privacy and data protection, the LFP-DPPP. This law could be used against UNINET and IUSACELL because both are private parties that might be collecting and processing personal data illegally.²⁰ UNINET and IUSACELL must adhere to the principles of legality, consent, information, quality, purpose, fairness, proportionality and accountability under the LFPDPPP. This implies that both companies should have implemented adequate operational processes and information security measures in order to ensure the protection of those principles. In any transfer of personal data, the data owner²¹ needs to be notified beforehand, unless the transfer is necessary or legally required to safeguard the public interest, or when required for a judicial proceeding.

In this regard, the constitution guarantees the individual’s right to privacy and data protection, subject to a few exceptions, such as in the case of military invasion, serious breach of the peace, or any other event which may place society in severe danger or conflict. According to the constitution, only the federal judicial authority can authorise telephone wiretapping and the interception of private communications, at the request of the appropriate federal authority or the State Public Prosecution Service.

The IFAI’s investigation is still in progress and it has not revealed any of its findings yet. The investigation addresses several issues: the cases in which FinFisher has been used, the purposes for which it has been used, and whether there has been due process. If FinFisher has been used by state entities to violate the communications of activists or the general population’s human rights, with purposes different from the ones established under law, and the espionage has been carried out without any authorisation by the competent authorities, a serious violation of those constitutionally protected human rights is at stake.

In order to legally fight against this violation, one could initiate a judicial process called constitutional adjudication (*juicio de amparo*). This

5 ECCHR, Reporters without Borders, Privacy International, Bahrain Watch, & Bahrain Center for Human Rights. (2013). *OECD Complaint against Gamma International for possible Violations of the OECD Guidelines for Multinational Enterprises*. United Kingdom: Privacy International. https://www.privacyinternational.org/sites/privacyinternational.org/files/downloads/press-releases/jr_bundle_part_2_of_2.pdf

6 Vermer, A. (2013, July 22). Corruption scandal reveals use of FinFisher by Mexican authorities. *Privacy International*. www.privacyinternational.org/blog/corruption-scandal-reveals-use-of-finfisher-by-mexican-authorities

7 Ricaurte, P. (2013, June 28). IFAI: inicio investigación sobre FinFisher en México. *ContingenteMX*. contingentemx.net/2013/07/03/ifai-inicio-investigacion-sobre-finfisher-en-mexico

8 Ricaurte, P. (2013, July 3). Privacy International solicita al IFAI que inicie investigación sobre FinFisher. *ContingenteMX*. contingentemx.net/2013/07/03/privacy-international-solicita-al-ifai-que-inicie-investigacion-sobre-finfisher

9 Deputies Chamber. (2013). *Proposiciones con punto de acuerdo presentadas por diputado en la LXII Legislatura turnadas a comisión*. sitl.diputados.gob.mx/LXII_leg/proposiciones_por_pernplxii.php?iddpt=421&pert=4

10 *Ibid*.

11 Jiménez, B. (2013, July 11). Denuncian activistas cacería cibernética. *Reforma*. (Link only available for subscribers but available also at www.criteriohidalgo.com/notas.asp?id=180404)

12 IFAI. (2014). *Verification Process exp. PS.0025/13*. sontusdatos.org/biblioteca/decisiones-judiciales-y-administrativas

13 INFOMEX. (2013). *No. application 0000400188713*. The application only can be seen as a result of a search in the Infomex system at <https://www.infomex.org.mx/gobiernofederal/moduloPublico/moduloPublico.action>

14 INFOMEX. (2013). *No. application 0000400230813*. The application only can be seen as a result of a search in the Infomex system at <https://www.infomex.org.mx/gobiernofederal/moduloPublico/moduloPublico.action>

15 Ramírez, P., & Molina, T. (2013, September 4). Desarrollador de FinFisher y otros ejecutivos del espionaje cibernético, activos en México, revela Wikileaks. *La Jornada*. wikileaks.jornada.com.mx/notas/desarrollador-de-finfisher-y-otros-ejecutivos-del-espionaje-cibernetico-activos-en-mexico-revela-wikileaks

16 Molina, T. (2013, October 7). Sigue activo el programa de espionaje cibernético FinFisher en México: Citizen Lab. *La Jornada*. wikileaks.jornada.com.mx/notas/sigue-activo-el-programa-de-espionaje-finfisher-en-mexico-citizen-lab

17 www.reddit.com/r/Anarchism/comments/zcjl0p/gamma_international_leaked

18 pastebin.com/KZQ5jojs

19 www.cobham.com/about-cobham/defence-systems/about-us/defence-electronics/san-diego/services/cobham-defence-electronics-mexico.aspx

20 By “processing” we mean the retrieval, use, disclosure or storage of personal data by any means.

21 The data owner is the individual to whom personal data relate.

process is mentioned in the constitution under a section entitled “Laws or acts issued by the authority, or omissions committed by the authority, which infringe the fundamental rights recognised and protected by this Constitution”.²² As the constitution protects the right to privacy, the legal basis upon which to file a constitutional adjudication would precisely be the violation of this human right and the absence of due process of law: the lack of a warrant by a judge authorising the interception of communications. A constitutional adjudication can also be founded on the rights protected under the international human rights treaties that Mexico has ratified. The jurisdiction that issues the decision of the constitutional adjudication is a federal court. Appeal of the ruling (*recurso de revisión*) is possible before an appeals court. As a last resort, it is the Supreme Court of Justice of the Nation (SCJN), Mexico’s highest federal court, that is competent to hear the case, but only on a discretionary basis and if the matter is significant (“*asunto de importancia y trascendencia*”). In case the complaint is granted, whether at a federal court or before the SCJN, the court would restore the right claimed by the plaintiff, but not issue any sanction to the agency responsible for violating the right.

Another, completely different recourse would be to reclaim the patrimonial accountability (*responsabilidad patrimonial*) of the state. This is an administrative procedure, not a judicial one, which is designed for those individuals whose rights and property have been infringed on as a result of illegal or unconstitutional state administrative activity.²³ The judicial, legislative and executive branches of the federation, constitutional autonomous agencies, units, entities of the Federal Public Administration, the Office of the Mexican Attorney General, federal courts, administrative and any other public federal entity, are subject to this administrative procedure. A lawsuit of patrimonial accountability is presented before the offending agency and is aimed at determining if there was a fault – in this case, the violation of a human right. It is possible to appeal the agency’s decision before the Federal Tax and Administrative Court. If the fault can be demonstrated and expressed in monetary terms, the plaintiff obtains relief through financial compensation.

The IFAI is responsible for guaranteeing the data owner’s right to the protection of his or her personal data. In this case, however, its role is unclear. It can investigate, as it has already done, and issue fines. But there is no established procedure for a case of government surveillance. Also, as the matter at stake is a violation of human rights, another institution could play a role: the National Human Rights Commission (CNDH). Nevertheless, that institution may only make recommendations that are not binding: it can determine whether there was a violation of human rights and who was responsible, but can only issue recommendations to prevent it from happening again.

Conclusions

Mexico is facing a situation that is testing the strength of its legal framework and the effectiveness of its administrative and judicial institutions. The petition by ContingenteMX, Propuesta Cívica and AI Consumidor could prove to be a factor that triggers more complaints aimed at ensuring transparency and respect of human rights by the Mexican government – in particular with respect to the right to privacy.

No matter whether, one day or another, someone will demonstrate that the government used FinFisher and did it illegally, Mexico does have a legal framework in place that enables it to address the FinFisher case as a privacy violation and a breach of human rights. However, the country does not have the legal and institutional framework that enables it to tackle government surveillance cases effectively. Government espionage is a delicate issue because it is not always clear whether government authorities are acting to protect national security interests and whether they are going beyond their obligations and start infringing on citizens’ human rights. It is precisely because limits are not always clear and institutions are fallible that there should be specific rules and procedures to safeguard individual human rights, as well as accountability and oversight rules that the government must comply with.

Action steps

There should be a minimum number of principles, the goal of which should be to protect the right to privacy and data protection, and to address government surveillance. Analysing the FinFisher case in light of existing legislation shows that the government is violating human rights, but is not revealing that it is spying on individuals, nor its seriousness. The International Principles on the Application of Human Rights to Communications Surveillance (“the Principles”) are a good starting point to

analyse other aspects of similar cases. These principles are the outcome of a global consultation with civil society groups, industry and international experts in communications surveillance law, policy and technology, and apply to surveillance conducted within a state or extraterritorially, regardless of the purpose of the surveillance.²⁴

In order to guarantee privacy and data protection, ContingenteMX, Propuesta Cívica and AI Consumidor have also proposed that competent authorities reconcile their legal framework with the Principles.²⁵ However, the first seven of the 13 principles (legality, legitimate aim, necessity, adequacy, proportionality, competent judicial authority and due process) are in fact safeguards that can be found in the Mexican Constitution, which deals with human rights and the cases and circumstances in which the state is able to interfere with them. Then, it would be more important that the government commit to comply with the other six principles (user notification, transparency, public oversight, integrity of communications and systems, safeguards for international cooperation, safeguards against illegitimate access and right to effective remedy) because they provide propositions specifically focused on wiretapping communications in the surveillance ambit.

Aside from covering the legal aspect, it is also necessary to foresee the operative needs that the law requires to be enforced: there should be operative rules and procedures derived from the Principles that let the same principles work in practice. Then, once the government’s commitment is verified, the state should determine the institutions and federal agencies that have to abide by those operative rules and procedures in order to protect individuals against surveillance. The compliance by the Federal Institute of Telecommunications (*Instituto Federal de Telecomunicaciones*) with the above-mentioned operative norms and procedures would, for instance, be necessary to guarantee the principles of user notification, but also the integrity of communications and systems. The Attorney General’s Office (*Procuraduría General de la República*), on the other hand, would help implement the principles of legality, legitimate aim, necessity, adequacy, proportionality, competent judicial authority and due process. In fact, since all the principles are related to each other, every institution and federal agency that would commit to the objective of protecting

individuals against surveillance would contribute to compliance with each of the 13 principles to various degrees. The state should also decide which specialised institution could guarantee the compliance with the applicable operative rules and procedures. In this sense, the IFAI is a good starting point because it is an autonomous institution that has a high level of public confidence. In this way, the principles of transparency and public oversight would be reinforced at the same time.

It is important to underline that the Principles would be worthless without an engaged society that demands respect of its rights. We recommend that from the Principles, we use the ones that can be promoted and exercised by Mexican civil society and non-profit organisations. As an example, the principle of legality suggests that, due to the rate of technological changes, limits to the right to privacy should be subject to periodic review by means of a participatory legislative or regulatory process. We recommend giving a role to civil society in these reviews. Regarding the principle of user notification, which establishes that individuals should be notified of communications surveillance, and the principle of transparency, which establishes that states should be transparent about communications surveillance, both of them can be achieved if civil society is vigilant and continuously informed about what the government is doing.

As a result, the action steps we recommend are the following:

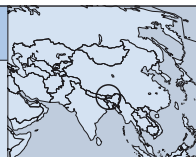
- Establish a clear legal framework for using espionage software and other similar tools. There should be specific rules for when the government wishes to use software like FinFisher. The rules would indicate the cases in which it is allowed and how the privacy of all the individuals who are not being investigated is safeguarded.
- Ratify the United Nations Guidelines for the Regulation of Computerized Personal Data because, by doing so, individuals would be assured of obtaining a basic threshold of protection for their privacy and personal data. Mexico would also show its commitment towards better protecting individuals’ communications and internet privacy.
- Encourage Congress to discuss the topic of government surveillance, as well as protect the privacy of communications.
- Organise campaigns to make civil society aware of the importance of privacy and how surveillance puts freedom of expression and association at risk.

22 Trife. (2013). *Mexican Constitution*. www.trife.gob.mx/sites/default/files/consultas/2012/04/cpeum_ingles_act_o8_octubre_2013_pdf_19955.pdf

23 Cámara de Diputados. (2014). *Ley Federal de Responsabilidad Patrimonial del Estado*. www.diputados.gob.mx/LeyesBiblio/pdf/LFRPE.pdf

24 <https://en.necessaryandproportionate.org/text>

25 Robles, J. (2013, October 7). Comunicado de prensa sobre los avances en las investigaciones sobre #FinFisher en Mexico. *ContingenteMX*. contingentemx.net/2013/10/07/comunicado-de-prensa-sobre-los-avances-en-las-investigaciones-sobre-finfisher-en-mexico



Development Knowledge Management and Innovation Services Pvt. Ltd.
Kishor Pradhan
www.dekmis.com

Introduction

Located in South Asia, Nepal is a relative latecomer as a republic in democratic circles. After more than a decade of insurgency, the interim constitution promulgated in 2007, which is still in force, paved the way for the first constituent assembly election (CAE) in 2008. The constituent assembly formed from this abolished the more than century-old monarchy. Nepal has been in the process of writing a new constitution since 2008. After the second CAE in 2013 and the formation of the second assembly, it is hoped that in a year or two the people of Nepal will finally have the pleasure of a new constitution and a stabilisation of the envisioned federal republic of Nepal.

According to the latest Nepal Telecommunication Authority (NTA) Management Information System Report published in February 2014, Nepal, with its population of 26,494,504,¹ has an 84.77% telephone penetration rate. The data shows there is a 74.97% mobile penetration rate among telephone users. At the moment, Nepal has an internet penetration rate of 28.63%, with 7,585,761 users.²

The OpenNet Initiative (ONI) reported that Nepal had little or no internet censorship in 2007. ONI conducted testing from October 2006 through January 2007 on six Nepali ISPs,³ and the tests revealed no evidence of filtering.⁴

However, four years ago, September 2010 was a dark period for netizens⁵ in Nepal who until then had enjoyed a free internet to its fullest extent. The authorities, out of the blue and citing the reasons that there had been an increase in crime and anti-

social activities using the internet, formed a special central investigation bureau that started clamping down on internet service providers (ISPs) to track the misuse of the internet by their subscribers.⁶

In 2011 the ISPs were told by the authorities to monitor their subscribers' activities and those who failed to do so were jailed. Since then the government has been monitoring the browsing details of high-bandwidth subscribers. The NTA has directed ISPs to provide information on all subscribers who use a bandwidth of 1 Mbps or more.⁷ The Nepal police work closely with NTA technicians now in a joint task force to scan web details of users so that they can identify voice over internet protocol (VoIP)⁸ racketeers.

The NTA further made it mandatory for ISPs to install filtering software to block websites that are "obscene, seductive and corrupt social morals". Any content that threatens "religious harmony, national security, and goes against values and beliefs of the state" was deemed objectionable enough to be blocked.⁹ Under pressure, the ISPs have been providing the police with Multi Router Traffic Grapher (MRTG)¹⁰ data of subscribers for network traffic monitoring since 2011.

Of late Nepali netizens cannot help feeling that "somebody's watching me"¹¹ while using the internet or communicating by some other technological means.

Policy perspectives

In order to assess the policy perspectives regarding privacy rights and mass communications

surveillance in Nepal, primarily three legal or policy provisions need to be considered.

In Article 22 of the Constitution of the Kingdom of Nepal 1990, the right to privacy was addressed as a fundamental right for the first time. The right to information was also included in the constitution. Later, the right to privacy was retained in the 2007 interim constitution, which remains in force today. Article 28 of the interim constitution states: "Except in circumstances as provided by law, the privacy of the person, residence, property, document, statistics, correspondence, and character of anyone is inviolable." However, there is no government authority to receive complaints regarding violations of privacy rights, although people may submit applications and reports concerning violations of their privacy rights to the National Human Rights Commission (NHRC). It is also possible to file a case in the Nepalese courts regarding violation of the right to privacy.¹²

In Chapter 2 of The Right to Information Act of 2007 (RTI Act 2007), entitled "Right to Information and Provisions Regarding the Flow of Information", Article 3 deals with the right to information and states: "Every citizen shall, subject to this Act have the right to information and every citizen shall have access to the information held in the public Bodies."¹³ The right to information is however stipulated by defining the parameters of the information that can be accessed; notwithstanding anything provided for in Sections (1) and (2) of the RTI Act 2007, the information held by a public body on certain subject matters cannot be disseminated.¹⁴

The Nepal Electronic Transaction Act of 2008¹⁵ serves as the cyber law in Nepal. In general it establishes legal provisions on the "dos and don'ts" for using ICTs such as computers and the internet, and on the nature of content circulated online. It provides for the official and legal application of electronic transactions such as digital signature and certification, but is silent about how privacy

will be protected. Nevertheless, the cyber law has critically empowered the authorities more when it comes to protecting the privacy rights of people.

Somebody's watching me?

When the authorities clamped down on ISPs in 2010, they said that VoIP is illegal in Nepal but that many of the public communications service providers were and still are rampantly using the internet to provide relatively low-cost calls. The authorities argued that, due to the illegal use of the internet for online calls which bypassed the NTA, it was losing billions of rupees every year.¹⁶ Who was responsible for this was not clear, however, as the ISPs countered that they provide the internet bandwidth to their subscribers – who *could* be public communications service providers – but they cannot really monitor or regulate what the internet bandwidth gets used for.

Further, the authorities claimed that the internet was used for criminal activities, as no record can be traced of internet calls. At the same time there were increasing cases of "objectionable" content being posted on websites from Nepal.

Rubeena Mahato, reporting on the tougher controls imposed by the NTA in 2010, emphasised that "MRTG data only allows monitoring the browsing patterns of users, but could be a stepping stone for the government to introduce censorship and intrude on private correspondence in the future."¹⁷

Measures taken by the authorities in Nepal for specific communications surveillance of criminal and objectionable activities are reasonable. But the monitoring of MRTG data entails mass communications surveillance. Mass communications surveillance entails surveillance of personal data and metadata, or what the International Principles on the Application of Human Rights to Communications Surveillance (IPAHRCS) – adopted through a global consultation with civil society groups, industry and international experts in communications surveillance law, policy and regulation in July 2013 – defines as "protected information". Information that includes, reflects, arises from or is about a person's communications and that is not readily available and easily accessible to the general public should be considered to be "protected information", and should accordingly be given the highest protection in law.¹⁸

1 www.cbs.gov.np

2 www.nta.gov.np/en/mis-reports-en

3 According to the Internet Service Provider Association of Nepal there are currently 43 internet service providers and nine VSAT network service providers in Nepal. www.ispan.net.np/registered-isp-list

4 https://opennet.net/research/profiles/nepal

5 The term netizen is a portmanteau of the English words internet and citizen. It is defined as an entity or person actively involved in online communities and a user of the internet, especially an avid one. en.wikipedia.org/wiki/Netizen

6 Pradhan, K. (2010, September 20). Can internet be muzzled in Nepal? *Nepalnews.com*. www.nepalnews.com/index.php/guest-column/9294-can-internet-be-muzzled-in-nepal

7 Mahato, R. (2011, July 22). Surfing under surveillance. *Nepali Times*. nepalitimes.com/news.php?id=18395

8 VoIP is illegal in Nepal, although netizens use Viber, Skype, Tango and other internet-based voice communication services.

9 Mahato, R. (2011, July 22). Op. cit.

10 The Multi Router Traffic Grapher (MRTG) is a tool to monitor the traffic load on network links. MRTG generates HTML pages containing PNG images that provide a live visual representation of this traffic. oss.oetiker.ch/mrtg/doc/mrtg.en.html

11 Somebody's Watching Me was the title of a song by R&B artist Rockwell, released on the Motown label in 1984. The song's lyrics relate the narrator's paranoid fear of being followed and watched. en.wikipedia.org/wiki/Somebody's_Watching_Me

12 Privacy International. (2012). *Nepal*. https://www.privacyinternational.org/reports/nepal

13 www.moic.gov.np/acts-regulations/right-to-information-act.pdf

14 As per the RTI Act 2007, the subject matters on which information cannot be disseminated by a public body include information which seriously jeopardises the sovereignty, integrity, national security, public peace, stability and international relations of Nepal; which directly affects the investigation, inquiry and prosecution of a crime; which seriously affects the protection of economic, trade or monetary interest or intellectual property or banking or trade privacy; which directly jeopardises the harmonious relationship among various castes or communities; and which interferes with the individual privacy and security of body, life, property or health of a person.

15 www.tepc.gov.np/uploads/files/12the-electronic-transaction-act55.pdf

16 In July 2014, the exchange rate was approx. 96 Nepali rupees per 1 USD.

17 Mahato, R. (2011, July 22). Op. cit.

18 https://en.necessaryandproportionate.org/text

Communications surveillance and violation of privacy rights are said to be increasing in Nepal. This perspective is corroborated by a recent incident on 18 April 2014, when Vinaya Kasaju, former chief commissioner of the National Information Commission (NIC), updated his Facebook status:

Dear FB friends, I cannot write this message in Nepali, because police personnel from Aparadh Anusandhan Mahasakha,¹⁹ Hanumandhoka, have taken away my desktop computer. They came at about 3:30 p.m. They showed me their identity card. I asked for letter. They said we have come with an order of boss. If you don't come with us, we must force you. I followed them to their van. On half way they talked with their chief and stopped the van. Waited for about half an hour in front of Radiant Academy, Sanepa, then they brought me back home. They also got a written receipt from us that Ganga, my wife, received. They took our photos. Ganga took photos of them and of their receipt. They mentioned that they have taken my computer. But we do not have hard copy of receipt, only photo which I'm trying to put here. Don't I have right to know why I was arrested, even for an hour? I am deprived of my communication tool. Who will save our RTI?

The next day Vinaya posted the following:

Hegemony of some big media house is increasing in our country too. Dil Sobha was reported as criminal running sex trade. Yesterday one big media covered Kanak Dixit as if he has done a big scandal. They don't wait for investigation report or court decision. I came to know unofficially, that a big media boss complained against my website www.cmr.org.np charging that he is losing the money from Google Ads. What a shame. There is no ad in my website. It is not difficult to find where Google Ads money is going. Has the media boss ever paid tax of that income to the government? I want my computer back as soon as possible safely, without loss or manipulation or theft of any data/file. As the former chief information commissioner, as a media consultant and as an author there are files of national importance and my resources for study and writing. There are many such files about which I can tell only to concerned authority. I hope and request to return my computer safely.²⁰

In all this Vinaya concludes that the cyber crime authorities in Nepal took action against him wrongly, which was the result of the lack of capacity of the authorities in tracking or locating the actual culprit. He concluded, "The capacity of the authorities to deal with and investigate cyber crimes is lacking in Nepal. Their capacity needs to be built to handle cyber crime issues, so that the real criminals are caught and innocent people are left alone."²¹

The ordeal Vinaya went through was a gross violation of his privacy rights. The authorities, without any warrant and on the basis of an informal complaint to a senior police authority by a powerful media mogul, violated his privacy rights.

It is not that the authorities or any other citizen in Nepal do not have rights to information. As established by the Right to Information Act, an institution or an individual is entitled to have access or the right to information, but by following a proper procedure. The NIC, formed under the Act, manages right-to-information cases. After receiving a request for information and verifying the authenticity, the NIC decides on the ensuing action. And this is applicable to government authorities, such as police departments, too.

The issue is the juxtaposition and limitation of the right to privacy, right to information and communications surveillance. As the legality principle of the IPAHRCS states:

Any limitation to the right to privacy must be prescribed by law. The State must not adopt or implement a measure that interferes with the right to privacy in the absence of an existing publicly available legislative act, which means a standard of clarity and precision that is sufficient to ensure that individuals have advance notice of and can foresee its application. Given the rate of technology changes, laws that limit the right of privacy should be subject to periodic review by means of a participatory legislative or regulatory process.²²

Given the rapid changes in the communications landscape, it is about time that the authorities in Nepal revisit the current right-to-privacy legal provisions, those that deal with the right to information, as well as mass communications surveillance policies and practices. The authorities should be able to reassure citizens and netizens alike that their privacy is not intruded on when communicating, and

make them not feel that "somebody's watching me" when communicating privately, socially, professionally or officially.

Conclusions and action steps

The conclusions that can be drawn from the Nepal experience so far are two-fold. On the one hand it can be asked, how is the right to privacy going to be protected by the authorities in a changed communication landscape? On the other hand, given the imperative of communications surveillance for national security and crime control, how is it not going to be intrusive?

These juxtaposed perspectives urgently call for the authorities to revisit the issues of the right to privacy and the imperative of communications surveillance and find a balanced middle path that can uphold both. In this context, the following action steps can be suggested.

- The authorities need to revisit the policies or laws related to the right to privacy and reformulate them in the changed context of the ways people communicate or access information or process and maintain personal data.

- Regarding the laws or policies for communications surveillance, the authorities should formulate regulations which distinctly address the issues of internet censorship and communications surveillance.
- Communications surveillance, whether mass communications surveillance or specific communications surveillance, needs to be distinguished by law or policy and regulated accordingly, following a standard legal procedure.
- Civil society, especially rights-based organisations, should be more engaged in Nepal on lobbying the authorities to recognise and protect the right to privacy and the right to communication, without being under surveillance.
- International rights organisations and donors working on the right to privacy related to communications surveillance should provide technical assistance to the government and civil society (including the media) in developing countries like Nepal, in order to build their capacity for addressing and managing the issues of privacy and communications surveillance in line with international principles or conventions.

¹⁹ In English, Crime Investigation Department.

²⁰ <https://www.facebook.com/vinaya.kasaju/?fref=ts>

²¹ Personal conversation with Vinaya Kasaju.

²² International Principles on the Application of Human Rights to Communications Surveillance. <https://en.necessaryandproportionate.org/text>

NEW ZEALAND

Eyes on New Zealand



Association for Progressive Communications (APC) and Tech Liberty

Joy Liddicoat and Tech Liberty¹
www.apc.org, www.techliberty.org.nz

Introduction

New Zealand is a small country, with a population of less than five million, situated in the far reaches of the southern hemisphere. But its physical remoteness belies a critical role in the powerful international intelligence alliance known as the “Five Eyes”,² which has been at the heart of global controversy about mass surveillance. This report outlines the remarkable story of how an international police raid for alleged copyright infringement activities ultimately became a story of illegal spying on New Zealanders, and political deals on revised surveillance laws, while precipitating proposals for a Digital Rights and Freedoms Bill and resulting in the creation of a new political party. We outline how civil society has tried to respond, and suggest action points for the future, bearing in mind that this incredible story is not yet over.

Background: New Zealand’s role in the Five Eyes

The impact of the revelations of mass surveillance and New Zealand’s role must be seen against the backdrop of the country’s role in the Five Eyes alliance. Nicky Hager, New Zealand’s most prominent investigative journalist, says “for the most part [New Zealand’s role in the Five Eyes] was an accident of history.”³ Arising from intelligence-sharing agreements among five countries during and after World War II, the main agency responsible for its day-to-day operations in New Zealand is the

Government Communications Security Bureau (GCSB).⁴

A key aspect of this intelligence-sharing regime is a legal framework that provides differing levels of protections for internal (national) versus external (extraterritorial) communications, or those relating to national citizens versus non-nationals. This framework discriminates on grounds of national origin, and in doing so purports to step around human rights protections from interferences with the right to privacy of communications by the governments of the Five Eyes, claiming that such protections apply only to nationals or those within their territorial jurisdiction.⁵

Historically, the main purpose of the GCSB under this legal framework has been to spy on our neighbours in Asia and the South Pacific on behalf of the Five Eyes. This enabled the GCSB to claim that it did not spy on New Zealand citizens or permanent residents. Public assurances to this effect were given on a number of occasions by both the GCSB and the New Zealand government.⁶

Case study: Mega Upload – the move to domestic surveillance

In 2012 the New Zealand Police assisted the United States of America’s Federal Bureau of Intelligence (FBI) to carry out a raid on the house of Mr Kim Dotcom, founder of Mega Upload, an online file-sharing platform. Mr Dotcom had migrated to New Zealand from Hong Kong and was living in New Zealand legally as a permanent resident. The extraordinary raid of the house (replete with a helicopter bringing armed police officers into the house grounds to seize computers and other property), the seizure of the Mega Upload online service, and Mr Dotcom’s subsequent arrest and criminal prosecution, received huge media attention both in New Zealand and overseas.⁷

Mr Dotcom is an enigmatic figure, who has maintained a vigorous defence of all charges and high and consistent media presence through public en-

gagement against leading politicians, including the prime minister. There are many factors to the case which remain outstanding – extradition issues, validity of search warrants, and many other legal matters outside the scope of this report. However, in relation to surveillance issues, the case against Mr Dotcom revealed that the GCSB had been spying on him and sharing information from its activities with New Zealand law enforcement officers who were also dealing with the FBI in the investigation of Mega Upload. Public outrage followed the discovery that the GCSB were in fact spying on New Zealanders and resulted in the prime minister establishing an independent investigation by Rebecca Kitteridge.

The Kitteridge Report⁸ revealed that the GCSB activity was not an isolated case: in fact 88 unnamed New Zealanders had been spied on over many years.⁹ The report concluded that the GCSB based their operations on a faulty interpretation of the relevant New Zealand law (for example, they believed the prohibition on spying did not apply where there was a warrant and did not apply to “metadata” because metadata was not a “communication”), and that the law was unclear and therefore the GCSB were not at fault.¹⁰ Various recommendations were made for changing GCSB operations and law.

Prime Minister John Key immediately responded that the report made “sobering reading” and further: “I am embarrassed to say that I heard the unequivocal assurances and read the clear prohibition in the GCSB legislation, and I believed that they did not spy on New Zealanders. But it turns out they have been regularly spying on New Zealanders from before 2003 and since. They have seriously let down the public.”¹¹ Signalling a need for law reform, the prime minister also said: “In addition, the Act governing the GCSB is not fit for purpose and probably never has been.”¹²

The Kitteridge Report had been leaked, much to the fury of government ministers, and a parliamentary inquiry was launched. The prime suspect was Peter Dunne, a parliamentarian holding a single vote supporting the coalition government. Data about both Dunne’s movements and those of journalists in the parliamentary precinct (from security card swipe records at various doors in different buildings) were handed to the investigation. Dunne and journalist Andrea Vance’s

private phone records and emails from a three-month period were also provided to the investigation, without their knowledge or consent. These actions were widely seen as an attack on privacy and press freedom, sparking intense commentary from local journalists and media outlets. Dunne denied he was the source of the leak and asserted his rights to privacy,¹³ but was forced to resign his ministerial portfolio.¹⁴

Throughout this time, the Snowden revelations also kept coming, contributing to ongoing media focus and providing a wider global backdrop to the GCSB scandal and the proposed law reforms.

It was in this context that two new laws were introduced. The first, the GCSB Bill, was designed to restructure the GCSB and establish its legal basis more clearly. But the new laws went much further, retrospectively validating the GCSB action and fundamentally shifting the permitted surveillance activities to include surveillance of New Zealand citizens. Rather than clarifying that the GCSB could not spy on New Zealanders, the new law simply extended the authority to do so and validated the previously unlawful activity, clearly violating privacy rights. There was widespread consternation and opposition from legal groups, the technical community, business, human rights organisations and community organisations. The New Zealand human rights commission also took the unusual step of preparing a separate report for the prime minister highlighting serious concerns with the proposals.

The second law, the Telecommunications Interception Capability and Security Act (TICS), gave sweeping new powers to the GCSB, making new network security measures by all network operators including telecommunications companies, such as submission of security measures to the newly constituted GCSB. Thomas Beagle from Tech Liberty noted:

The [TICS] bill codifies the government’s assertion that all digital communications (which is increasingly becoming equivalent to “all communications”) must be accessible by government agencies. The limits imposed are minimal and laws such as the GCSB Act override any limits included in TICS. Furthermore, to ensure that the government can do this, the GCSB will now have oversight of the design and operation of New Zealand’s communications networks. They will be able to veto any decision made by the network

1 TechLiberty is a New Zealand group advocating for civil liberties online: www.techliberty.org.nz

2 The “Five Eyes” countries are New Zealand, Australia, Canada, the United Kingdom and the United States of America. The alliance operates an integrated global surveillance arrangement that covers the majority of the world’s communications. For an overview of legal arrangements see: APC et al. (2014). Joint Submission in Connection with General Assembly Resolution 67/167, “The right to privacy in the digital age”. <https://www.apc.org/en/pubs/submission-office-high-commissioner-human-rights-r>

3 Hager, N. (1996). *Secret power: New Zealand’s Role in the International Spy Network*. Port Nelson: Craig Potton Publishing, p. 58.

4 The first law authorising its operations was in 1977, followed by the Government Communications Security Bureau Act 2003.

5 APC et al. (2014). Op. cit., Appendix 1.

6 See also Hager, N. (2013, April 10). Who is really responsible for the GCSB shenanigans? *Pundit*. www.pundit.co.nz/content/who-is-really-responsible-for-the-gcsb-shenanigans

7 For an overview of the case, see: https://en.wikipedia.org/wiki/Megaupload_legal_case

8 Kitteridge, R. (2013). *Review of Compliance at the GCSB*. www.gcsb.govt.nz/news/publications

9 Ibid.

10 Bennett, A. (2013, April 9). CSB report: 88 cases of possible illegal spying uncovered. *New Zealand Herald*. www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=10876424

11 Key, J. (2013, April 9). PM releases report into GCSB compliance. *Beehive.govt.nz*. www.beehive.govt.nz/release/pm-releases-report-gcsb-compliance

12 Ibid.

13 Shuttleworth, K. (2013, July 30). Reports phone records released. *New Zealand Herald*. www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=10905495

14 Burr, L. (2013, June 7). Peter Dunne resigns as minister. *3 News*. www.3news.co.nz/Peter-Dunne-resigns-as-minister/tabid/1607/articleID/300658/Default.aspx

operators that might impact on security or, more likely, limit their ability to spy as they see fit.¹⁵

Under the TICS, the GCSB now has the ability to approve or refuse to approve all significant changes to New Zealand's telecommunications infrastructure. This new power far exceeds any role of the GCSB in the Five Eyes, extending its oversight to business and other private sector activities.

At the same time as these two new laws were being passed, a new internet censorship law aimed at harmful online speech, the Harmful Digital Communications Bill, was also before parliament.¹⁶ The local internet community worked hard to respond to these new measures, including bringing national attention to concerns about the role of New Zealand in the Five Eyes, highlighting human rights concerns and the need for limitations on human rights only in exceptional and narrow circumstances, in line with the 13 International Principles on the Application of Human Rights to Communications Surveillance.¹⁷

The degree of public interest was enormous. Large public meetings and street rallies were held throughout the country, fuelled by the Snowden revelations and leaks of information about the role of New Zealand in the Five Eyes. Thousands of people rallied, started and joined online campaigns, with both online and offline media and journalists engaging.

Overall, it was an intense period of constant media coverage and political focus. At times developments happened daily, even hourly, making it difficult to maintain an overview of what was happening, how developments were related and to think strategically about how to respond. Views were also divided: some thought privacy issues were not relevant in an internet age; others considered it was legitimate for the government to carry out surveillance. Despite widespread public opposition to the GCSB Bill, the prime minister went so far as to claim that New Zealanders cared more about how many fish they were allowed to catch than they did about their online privacy.¹⁸

By the end of 2013 both the GCSB and TICS Bills were law and campaigns to counter them had proved ineffective. But the awareness of internet-related policy issues had grown enormously. In

March 2014 the main political opposition, the Labour Party, announced plans for a new Digital Bill of Rights.¹⁹ Within weeks Gareth Hughes, a Greens political party member of parliament, launched a new Digital Rights and Freedoms Bill,²⁰ drawing heavily on the global civil society Charter of Internet Rights and Principles,²¹ with protections for encryption, privacy and freedom from search, surveillance and interception of communications.

Implications

The GCSB and TICS laws were passed, while New Zealand continues to affirm its security stance with the United Kingdom²² and the Five Eyes alliance. Yet the political and legal fallout from the Kim Dotcom raid has extended far beyond anything that could ever possibly have been imagined.

What began as mutual assistance in law enforcement for alleged intellectual property rights violations (which sparked the original police raid and seizure of Mega Upload) has ended in multiple investigations, revelations of spying, new laws, and a sea change in regulation affecting the internet in New Zealand. We have even seen the birth of a new political party, the Internet Party, founded by Mr Dotcom, which has formed an alliance with the Mana Party and is contesting the general election in September 2014.²³

But the pace of regulatory intervention, its technical aspects, and the intensely political nature of the proposals make it very difficult for many New Zealanders to engage meaningfully. More major law reforms were announced in May 2014, with a wholesale review of the Privacy Act which will include new measures for data sharing by government agencies, mandatory reporting of data breaches, and a new offence of impersonation.

While this review is welcome, and there is a good Privacy Commissioner²⁴ who has knowledge of internet-related issues, the policy review will also require close scrutiny and engagement from civil society groups. Legal academics are still only beginning to focus on surveillance and privacy²⁵

and in general the legal community has been slow to grasp the human rights implications of internet-related policy and regulatory measures.

In some cases rights-affirming changes have been made to draft laws,²⁶ but change is often difficult once laws are drafted because of political issues. In the case of the GCSB Bill, for example, it quickly became apparent that the government was unlikely to make major changes. Dunne, the politician who had refused to disclose his own communications to parliamentary investigators, ultimately voted for the GCSB Bill in a political deal widely condemned as a cynical "trade off for privacy".²⁷ His ministerial portfolio was later reinstated.²⁸

In addition, the Kitteridge Report had found that the legal authority for collection of metadata was unclear and that it should be clarified. However, the government declined to do so in the GCSB and TICS laws and instead went further, extending the powers of the GCSB and the legal regime for spying on New Zealanders.

The 13 Principles are being used to support advocacy and were referenced in submissions on the Harmful Digital Communications Bill.²⁹ But while these have been helpful for civil society, it is difficult to see if these have had lasting impact in a country whose government's foreign policy is so closely aligned to the Five Eyes alliance. One encouraging sign is that the Principles have been cited in the Internet Party's policy on privacy and internet freedom.³⁰

New Zealand prides itself on its human rights reputation. But the reality is that our human rights online are more at risk. The result from these events is that threats to internet freedom have actually increased: instead of curtailing the GCSB's powers, new laws provide much stronger, direct state-sanctioned surveillance (including the use of metadata) by the GCSB, which it can use in domestic law enforcement. In the public mind, significant issues of trust remain, but it is unclear how this might affect the 2014 national elections.

New civil society voices have emerged in the last two years, but these groups need more support because the volume, speed and size of internet-related

policy is growing rapidly. In this environment, which is also highly politically charged, it is vital to have strong independent voices, and groups such as Tech Liberty are being increasingly called on to respond and help to inform public understanding and debate.

In a further development, in July 2014, the United Nations High Commissioner for Human Rights issued a damning report on issues of mass surveillance. The report concluded that the collection of metadata is a violation of the right to privacy and human rights obligations apply without discrimination.³¹ It is unfortunate that the report was not available during the Kitteridge inquiry, which concluded that the legality of metadata collection was unclear. But the clear and unequivocal UN report now needs to be followed up and actioned in New Zealand. Regular monitoring of New Zealand internet freedom is also needed so that it can be available quickly to support advocacy when needed.³²

Action steps

Tech Liberty is one of only a handful of New Zealand civil society groups and individuals working on internet-related human rights issues, including privacy and surveillance. Others include the New Zealand Council for Civil Liberties, New Zealand Law Society, and InternetNZ. As a voluntary group with limited resources, the task of monitoring and advocating is often difficult. More support and resources are needed if the network of voices that has the capacity to engage in these important debates and activities is to be grown and strengthened. This includes the legal and academic communities.

Specific actions that need to be taken include:

- Support civil society advocacy efforts, including capacity building for those groups for whom internet-related human rights issues are still new.
- Regularly update the NZ internet freedom index³³ to enable periodic monitoring of threats to internet freedom, and use these results in reporting on New Zealand's human rights performance.
- Review, and where necessary amend, the GCSB and TICS Acts in light of the United Nations High Commissioner for Human Rights report which finds, among other things, that collection of metadata is a violation of the right to privacy.
- Bring the New Zealand experience to the United Nations Human Rights Council session on the right to privacy in the digital age in September 2014.

15 Tech Liberty. (2013 November 5). TICS - Second spy law passes. *Tech Liberty*. techliberty.org.nz/tag/gcsb

16 The Harmful Digital Communications Bill 2012 deals with harmful online content and has been reported back from Select Committee. It is not expected to become law until 2015. See also Paton, L. and Liddicoat, J. (2013). New Zealand. In APC and Hivos, *Global Information Society Watch 2013: Women's rights, gender and ICTs*. www.giswatch.org/en/country-report/womens-rights-gender/new-zealand

17 www.necessaryandproportionate.org

18 John Key, press conference, 12 August 2013. www.3news.co.nz/Key-NZers-care-more-about-snapper-than-GCSB/tabid/817/articleID/308665/Default.aspx

19 Cunliffe, D. (2014, March 9). Digital Bill of Rights. *Labour*. <https://www.labour.org.nz/media/digital-bill-rights>

20 internetrightsbill.org.nz/ten-internet-rights-and-freedoms

21 internetrightsandprinciples.org/site/

22 McCully, M. (2013, January 13). NZ-UK joint statement on cyber security. *Beehive.govt.nz*. www.beehive.govt.nz/release/nz-uk-joint-statement-cyber-security

23 Bennett, A. (2014, May 27). Mana confirms election year deal with Internet Party. *New Zealand Herald*. www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=11262597

24 Privacy Commissioner John Edwards: privacy.org.nz

25 For example, the University of Otago held a symposium on Surveillance, Copyright and Privacy in January 2014: <https://blogs.otago.ac.nz/scpconf/programme-of-events/abstracts-of-talks>

26 Tech Liberty. (2014, May 27). HDC Bill reported back by Select Committee. *Tech Liberty*. techliberty.org.nz/hdc-bill-reported-back-by-the-select-committee

27 National Business Review. (2014, August 14). Swing vote Dunne supports GCSB Bill after changing tune on domestic spying. *National Business Review*. www.nbr.co.nz/article/swing-vote-dunne-supports-gcsb-bill-after-changing-tune-domestic-spying-peters-holds-out-ck

28 AAP. (2014, January 21). Leak forgotten, Dunne back as minister. *MSN.nz*. news.msn.co.nz/nationalnews/8787062/dunne-reinstated-as-minister

29 For example, by Tech Liberty: techliberty.org.nz/submission-harmful-digital-communications-bill/#more-1968

30 Internet Party, Privacy and Internet Freedom Policy, Clause 4.1.1. <https://internet.org.nz>

NIGERIA

Online surveillance: Public concerns ignored in Nigeria



Fantsuam Foundation

John Dada and Teresa Tafida
www.fantsuam.net

Introduction

Nigeria, a country of 170 million people, recently made global headlines when social activists, through the use of social media (#BringBackOurGirls), brought media attention to the kidnapping of over 300 girls by an armed gang of religious extremists.¹ This event and the related security concerns about Africa overshadowed the 24th World Economic Forum on Africa that was hosted by Nigeria in May 2014.² The global scrutiny caused by this event has put the Nigerian government on the back foot in its efforts to bring security in the country under control.

This report looks at the government's mass surveillance attacks on its citizens before and after it purchased USD 40 million of Israeli technology³ to be used for the monitoring and control of the internet. Various top government officials have called for the regulation of social media: the minister of information argued that even the United States (US) intercepts its citizens' communication. However, he omitted the fact that in the US there are legal and judicial processes to show its use and limits so that abuses will be checked. To further the government's surveillance agenda, additional legislation is already under consideration by the Nigerian Communications Commission.⁴

Policy and political background

Nigeria is in its third round of democratic governance since the ouster of the military regime. However, vestiges of autocratic leadership still abound. The recent awarding of the USD 40-million surveillance contract, without following due process and in spite of nationwide expression of opposition, suggests a governance system that is yet to function democratically.

Nigeria is ranked 112th out of 180 countries in the 2014 Reporters Without Borders press freedom index.⁵ Recently, government agents raided some media houses and seized their newspapers during what was called "routine security action".⁶ Such arbitrary action gets the support of several top government officials, including the president and agencies who have expressed the desire to clamp down on the use of social media and access to information.

Nigeria does not yet have any existing data privacy laws or legal provision for interception of communication. The current security challenges in the country are being used as the reason to take major security decisions and make national commitments without the necessary constitutional approvals.

The history of implementation of government projects in Nigeria is riddled with inefficiency and corruption. A recent example is the USD 470-million National Public Security Communication System⁷ that resulted in the installation of CCTV cameras ostensibly to curb crime and violent attacks in the capital city. However, since its inception the level of insecurity in the capital city has increased dramatically. The people's lack of endorsement of the Israeli Elbit Systems purchase is therefore based on popular perception of the capabilities and motives of the government when initiating projects, espe-

cially when such projects are deliberately shrouded in secrecy.

Exposing the Nigerian surveillance system

Nigeria has experienced widespread and growing incidences of kidnapping, blackmail, terrorist attacks and abduction. While these issues may be linked to governance challenges of mismanagement, corruption and unemployment, short-term measures to address these problems can be counterproductive.

In April 2013, an Abuja-based newspaper, *Premium Times*,⁸ broke the news that the Nigerian government had awarded the security tender to an Israeli firm for the procurement of the Elbit Systems technology.⁹ This would enable the Nigerian government to intercept all internet activity, and to invade users' privacy at will. The purchase is made more disturbing in that there is no enabling legislation for such an action by the government.

The paper also revealed that all Nigerian GSM service providers were intercepting all forms of communication.¹⁰ This action on its own is a violation of the International Principles on the Application of Human Rights to Communications Surveillance.¹¹ Without the benefit of judicial protection through any laws on privacy and data collection, Nigerians remain vulnerable to an infringement of their privacy from their government, and from foreign governments or organisations.

Another angle to the surveillance contract is the allegation by BDS Switzerland that the Elbit Systems technology has been developed and tested through the surveillance, repression and killing of Palestinians, including numerous civilians.¹² This issue, however, appears to have gone largely unnoticed in Nigeria.

The Nigeria Communications Commission (NCC) has released a draft policy on lawful interception that will empower security officers to intercept phone calls, text messages, chat messages, emails, etc.¹³ It is of concern that the NCC would opt for regulation rather than allow the National Assembly

to debate and decide on the issue. The NCC option would be open to abuse and violation of the fundamental right to privacy, a violation of Nigeria's 1999 constitution.

The recent arbitrary seizure of newspapers by the army and similar acts have raised concerns about security agents and law enforcement officials using the access and information at their disposal to their own advantage, or the government using regulations to crack down upon the opposition.

Conclusions

While it is difficult to fault the need for mass surveillance for the purpose of ensuring national security, and in the Nigerian situation, to track the terrorist activities of Boko Haram and online fraudsters, the peoples' concern is the normalising of surveillance in the guise of safety in a polity where legislative oversight and legal protection are missing. The history of governments all over the world, as documented by Snowden, is replete with abuse of their citizens' rights to privacy. It is significant that in spite of the outcry by citizens and attempt by the legislative arm of government to halt the Elbit contract, the government was not deterred. It is the fear of action with such impunity, not subject to the scrutiny of constitutional provision, that creates so much concern.

There is a need for more openness from the Nigerian government to allow a public debate on the spying programme to ensure better inclusion and buy-in. In its present form it does not meet the legislative requirements for procurements of that magnitude and national significance, and the government has not asked for the people's view – the views that have been expressed have been largely ignored. In its present form, the contract breaches the International Principles on the Application of Human Rights to Communications Surveillance,¹⁴ specifically on the issues of legality, legitimate aims, competent judicial authority, due process, user notification, transparency, integrity of communications and systems, and the need to safeguard against illegitimate access. Its illegality derives from its contravention of the 2007 Public Procurement Act. The Elbit contract did not meet the requirements for the awarding of such special contracts.

Action steps

In spite of loud protests by civil society organisations and individuals in Nigeria, and a feeble attempt by the House of Representatives to stop the contract, the government went ahead to purchase

1 Van Wagtendonk, A. (2014, May 2). Nigerians take to streets, social media to demand return of kidnapped girls. *PBS*. www.pbs.org/newshour/rundown/nigerians-take-streets-social-media-demand-safe-return-kidnapped-girls

2 Mosch, T. (2014, May 9). Africa's future overshadowed by Nigeria's present. *DW*. www.dw.de/africas-future-overshadowed-by-nigerias-present-at-wef/a-17625665

3 Emmanuel, O. (2013, April 25). Jonathan awards \$40million contract to Israeli company to monitor computer, Internet communication by Nigerians. *Premium Times*. www.premiumtimesng.com/news/131249-exclusive-jonathan-awards-40million-contract-to-israeli-company-to-monitor-computer-internet-communication-by-nigerians.html

4 Draft Lawful Interception of Communications Regulations. media.premiumtimesng.com/wp-content/files/2014/05/Legal-Regulations_Lawful_Interception_of_Communications-o80113.pdf

5 rsf.org/index2014/en-index2014.php

6 Reporters Without Borders. (2014, June 11). Army seizes newspaper issues day after day on "security" grounds. *Reporters Without Borders*. en.rsf.org/nigeria-army-seizes-newspaper-issues-day-11-06-2014_46418.html

7 Isine, I. (2014, June 27). High-level corruption rocks \$470million CCTV project that could secure Abuja. *Premium Times*. www.premiumtimesng.com/news/163975-high-level-corruption-rocks-470million-cctv-project-secure-abuja.html

8 Emmanuel, O. (2013, April 25). Op. cit.

9 Johnson, J. (2013, July 2). Scandal in Nigeria over Israeli arms firm's Internet spying contract. *Electronic Intifada*. electronicintifada.net/blogs/jimmy-johnson/scandal-nigeria-over-israeli-arms-firms-internet-spying-contract

10 Emmanuel, O. (2014, February 10). U.S. spy program reforms spotlight Nigeria's expanding surveillance program. *Premium Times*. www.premiumtimesng.com/news/154931-u-s-spy-program-reforms-spotlight-nigerias-expanding-surveillance-program.html

11 <https://en.necessaryandproportionate.org/text>

12 www.bds-info.ch

13 Collins, K. (2013, September 4). Nigeria embarks on mobile phone surveillance project. *Wired.co.uk*. <http://www.wired.co.uk/news/archive/2013-09/04/nigeria-phone-bugging>

14 <https://en.necessaryandproportionate.org/text>

the very expensive Elbit surveillance equipment from Israel. The ignoring of peoples' views by the government is a worrying trend.

A second disturbing trend that clearly violates the principle of integrity of communications and systems is compelling telecommunications service providers to provide their customers' records to security agencies. This is under the Bill for an Act to Provide for the Interception, Development and Protection of Communications Networks and Facilities for Public Interest and Other Related Matters, 2013.¹⁵

At the same time, the impact of social networking on the government's actions and activities has been rather limited in scope: it was useful in mobilising people for the 2012 fuel protests, and recently it was used to force the government to finally acknowledge the abducted girls (#chibokgirls), although this is beginning to lose traction and three months later, the girls have yet to be rescued.

An issue that may work in favour of the government is access. This was suggested during the recent elections in Ekiti state in which the incumbent governor, whose track record of governance was widely held as a model, lost to a rival who is under criminal investigations arising from his earlier tenure.¹⁶ Social networking sites were overwhelming in their support for the incumbent, but the results showed that the reality was far from that.

Could it be that social networking in Nigeria's most educationally advanced state is still not accessible to the bulk of the population?

If this trend continues, the government may soft pedal on its crackdown on internet freedoms. With the cost of internet access in Nigeria at about ten times what it costs in a country like the United Kingdom, affordable access remains a challenge to the people's access to relevant information. If it is the government's intention to operate clandestinely and without consideration for public opinion, a deliberate effort NOT to create an enabling environment to facilitate affordable internet access may just be all the government needs to do. Advocating for increased citizen access to the internet therefore remains a priority for civil society.

With increasing pressure on the government as the national elections draw closer, it can be expected that the views of the people will be ignored and decisions taken to curtail their freedom, and they will have no recourse to the law for redress. There will therefore be a need to campaign legislators, policy makers and other stakeholders to raise the concerns. The new programme being developed by the Fantsuam Academy on electronic surveillance as part of its Computer Diploma curriculum is a small effort towards raising more public awareness of the gravity of the issue of mass surveillance.

PAKISTAN

Pakistan dominates the surveillance hall of shame



Bytes for All, Pakistan

Furhan Hussain and Gul Bukhari
bytesforall.pk

Introduction

Nestled in the heart of South Asia, the Islamic Republic of Pakistan has had an intense history involving multiple wars, the splitting away of its eastern wing, military coups, political insurgency, ethnic cleansing and separatist movements; all in less than seven decades of existence.

Many of these afflictions have paved the way for the strengthening of institutions such as the military, resulting in the civilian system of checks and balances or oversight of these institutions becoming non-existent, while human rights violations by these powerhouses remain as rampant as before. Their reach has now also fully extended to information and communications technologies (ICTs).

Policy and political background

In 2013, for the first time in its 66-year history, Pakistan saw a democratic government complete its legitimate tenure of five years, before handing over the reins to another democratically elected government. This change came after a pattern of short bursts of democracy, followed by military dictatorships, spanning decades. Be that as it may, the military is widely understood to maintain control of certain key areas, in particular foreign policy and security. Civilian governments may not trespass on these areas. Compounding this is the non-accountability of the military establishment, with grave implications for fundamental rights, and a direct impact on communications surveillance. Civilian subordination and helplessness is epitomised by the National Commission for Human Rights Act 2012, which excludes the armed forces and the intelligence agencies from the purview of the planned commission.¹

A parliamentarian, upon condition of anonymity, commented that today Pakistan is a security state, where a number of authorities, ambitious for control, have thrived unchecked by law. "Some intelligence agencies in Pakistan are without and beyond any law," he said, referring to the Inter-Services Intelligence agency (ISI), the military's premier spy agency believed to be highly active in illegal surveillance.² These sentiments are reflected in the fact that out of an ever-increasing military budget, no breakdown of portions allocated for intelligence and surveillance agencies is ever made available.³

Today, Pakistan is ranked as one of the most dangerous countries in the world for human rights defenders (HRDs), journalists and minorities,⁴ who are threatened by acts of discrimination and violence with impunity by both state and non-state actors. According to some experts, the actions of the state suggest that it is strategically complicit in crimes committed by non-state actors, rather than being a silent onlooker.⁵ Meanwhile, the massive surveillance in place – both online and off – is increasingly seen as a tool for repression, rather than meeting the government's narrative of protecting citizens from terrorism.

Surveillance in Pakistan is not just limited to the local authorities. Last year's data leaks by whistleblower Edward Snowden revealed that Pakistan is the second most spied-on country in the world.⁶ The government of Pakistan determined that the country's sensitive data was at risk of being stolen by the United States (US) and decided to address the

¹⁵ Nigeria Communications Week. (2013, October 24). FG presses forward with controversial wire-tap programme. *Nigeria Communications Week*. www.nigeriacommunicationsweek.com.ng/telecom/fg-presses-forward-with-controversial-wire-tap-programme#sthash.zLPYJ7jY.dpuf

¹⁶ Channels Television. (2014, June 22). Ekiti election: Fayemi concedes defeat, congratulates Fayose. *Channels Television*. www.channelstv.com/2014/06/22/fayemi-concedes-defeat-congratulates-fayose

¹ FORUM-ASIA. (2013). Pakistan: Delay and uncertainty in establishing the National Commission for Human Rights. In B. Skanthakumar (Ed.), *2013 ANNI Report on the Performance and Establishment of National Human Rights Institutions of Asia*, p. 180. www.forum-asia.org/?p=16848

² Interviewed by the authors in June 2014.

³ Sheikh, I., & Yousaf, K. (2014, June 3). Budget 2014: Govt announces 700bn defence budget. *The Express Tribune*. tribune.com.pk/story/716913/budget-2014-defence-budget-increasing-at-diminishing-rate

⁴ Pathak, A. (2014, May 14). PAKISTAN: Human rights defenders in Pakistan in need of defence. *Asian Human Rights Commission*. www.humanrights.asia/news/ahrc-news/AHRC-ART-036-2014; Haider, M. (2014, May 4). Pakistan most dangerous country for journalists: UN. *DAWN.com*. www.dawn.com/news/1104120; Hassan, S. (2014, May 5). Pakistan's Hindus, other minorities face surge of violence. *Reuters*. www.reuters.com/article/2014/05/05/us-pakistan-minorities-idUSBREA4405U20140505

⁵ Bukhari, G. (2014, May 12). Silent onlooker? No, Sir. *The Nation*. www.nation.com.pk/columns/12-May-2014/silent-onlooker-no-sir

⁶ CIOL. (2013, June 13). India fifth most snooped country by US, Pakistan second. *CIOL*. www.ciol.com/ciol/news/190000/india-fifth-snooped-country-us-pakistan

crisis.⁷ Most recently, the Pakistani Foreign Office officially protested against the US National Security Agency's (NSA) surveillance of its left-leaning political party, the Pakistan People's Party (PPP),⁸ after recent revelations about the NSA having special permission from the US government to do so.⁹

Ironically, certain Pakistani laws also permit the execution of surveillance warrants in foreign jurisdictions¹⁰ and the state has a history tainted with instances of collaboration with foreign intelligence agencies (including the NSA)¹¹ as well as corporations when it comes to information surveillance and controls.¹²

The state of surveillance/surveillance state: An analysis

The constitution of Pakistan largely supports fundamental rights to privacy and freedom of expression, assembly and information, meaning mass communications surveillance is essentially illegal. Pakistan is also a signatory to the United Nations Declaration of Human Rights (UDHR), the International Covenant on Economic, Social and Cultural Rights (ICESCR), and the International Covenant on Civil and Political Rights (ICCPR), each of which focuses extensively on the rights of people to privacy, assembly and free speech, without fear of judgment or persecution. Yet some legislation and extra-legislative practices put in place by various arms of the

executive contravene the letter and spirit of human rights protections as laid out in the country's own constitution, as well as of those in its international obligations.

Extra-legislative surveillance

The case of murdered journalist Saleem Shahzad, who was tortured and killed after being abducted from the heart of the country's capital, demonstrates the role of secret agencies that exist without any legislative underpinnings, and their almost absolute control over surveillance. Physical surveillance (security checkpoints and CCTV) of Shahzad's route to the television studios where he was headed did not help solve his case. It was made evident in subsequent reports and analysis, including that of Amnesty International,¹³ that only those who controlled these surveillance tools and apparatuses could have avoided detection. The ISI, though a prime suspect in the case, was only partially investigated by the judicial commission formed to investigate the case. Conversely, it was claimed by human rights defenders and groups that Shahzad's mobile phone records went missing for up to 15 days before his murder, although the ISI has denied it. The independent judicial commission recommendations subtly hinted for the need to make "important intelligence agencies (ISI) more law abiding through a statutory framework carefully outlining their respective mandates and roles."¹⁴

These recommendations led to the draft Inter-Services Intelligence Agency (Functions, Powers and Regulation) Act of 2012 being proposed in parliament, in an attempt to give the spy agency a legal status and subject it to judicial and parliamentary oversight. However, the bill, which among other things would have laid the foundations against illegal surveillance by the ISI, was withdrawn¹⁵ – the military remains all-powerful and continues to operate the ISI in a fashion after the Orwellian secret force in Animal Farm.

7 Mirza, J. (2013, September 26). Pakistan takes steps to protect itself from NSA style cyber attacks. *The News International*. www.thenews.com.pk/Todays-News-6-204384-Pakistan-takes-steps-to-protect-itself-from

8 Haider, M. (2014, July 6). Pakistan lodges formal protest with US against PPP surveillance. *Dawn.com*. www.dawn.com/news/1116802

9 Mail Today Bureau. (2014, July 2). America gave NSA permission to spy on BJP, claims whistleblower Snowden. *Mail Online India*. www.dailymail.co.uk/indiahome/indianews/article-2677247/America-gave-NSA-permission-spy-BJP-claims-whistleblower-Snowden.html

10 La Rue, F. (2013). Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (A/HRC/23/40). United Nations Office of the High Commissioner for Human Rights. www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf

11 Gallagher, R. (2014, June 14). How Secret Partners Expand NSA's Surveillance Dragnet. *The Intercept*. <https://firstlook.org/theintercept/article/2014/06/18/nsa-surveillance-secret-cable-partners-revealed-rampart-a/>

12 Bytes for All, Pakistan. (2012, June 17). Dr. Eric Schmidt, please don't advertise surveillance to Pakistan government. *Bytes for All*. content.bytesforall.pk/node/56; The Express Tribune. (2012, June 15). Gilani seeks Google's help in tracking cross-border movement. *The Express Tribune*. tribune.com.pk/story/394128/gilani-seeks-googles-help-in-tracking-cross-border-movement; Davies, S. (2013, July 18). Pakistan government admits secret "censorship arrangement" with Facebook. *The Privacy Surgeon*. www.privacysurgeon.org/blog/incision/pakistan-government-admits-secret-censorship-arrangement-with-facebook

13 Amnesty International. (2014). "A Bullet has been chosen for you": *Attacks on journalists in Pakistan*. London: Amnesty International, International Secretariat, United Kingdom.

14 ANI. (2011, June 19). 'Prime suspect' ISI to probe Pak journalist murder case. *Yahoo News*. <https://sg.news.yahoo.com/prime-suspect-isi-probe-pak-journalist-murder-case-071918521.html>; Abbasi, A. (2011, June 19). ISI to probe Saleem Shahzad murder. *The News International*. www.thenews.com.pk/TodaysPrintDetail.aspx?ID=6829&Cat=13; Nisar, M., Khan, A. A., Iqbal, J., Khan, B. A., & Shaukat, P. (2012). *Judicial Inquiry Report on Saleem Shahzad's Murder*. Islamabad.

15 Zaafir, M. S. (2012, July 13). Farhatullah withdraws bill in Senate about ISI control. *The News International*. www.thenews.com.pk/Todays-News-6-120149-Farhatullah-withdraws-bill-in-Senate-about-ISI-control

Legalised surveillance?

According to the Pakistan Telecommunication (Re-organization) (Amendments) Act, 2006, the government can authorise any person(s) to intercept calls and messages, or trace location or movement through any telecommunication medium, giving the authorities a free hand to conduct communications surveillance, and with no mention of any governance parameters ensuring a due process. The ordinance also states that no cyphering hardware or software used within the country may be considered "approved" unless authorisation has been granted by the Electronic Certification Accreditation Council established under the Electronic Transaction Ordinance, 2002.¹⁶ This suggests that the fundamental right to online privacy through encryption is subject to the approval of the authorities. According to the Pakistan Telecommunications Authority's (PTA) policy on the use of virtual private network (VPN) tunnels, use of all "non-standard modes of communication like VPNs [...] by which communication becomes hidden or modified to the extent that it cannot be monitored, is a violation," as per the Monitoring and Reconciliation of International Telephone Traffic (MRITT) Regulations 2010.¹⁷ An interesting intersection between legal vs illegal surveillance can be observed by noting that while the PTA has legal authority to conduct communications surveillance, it denies doing so by itself.¹⁸ Instead, it has confirmed that the ISI monitors "grey traffic" over the internet,¹⁹ despite the fact that it has no legal mandate to do so.

Similarly, another act called the Investigation for Fair Trial Act, 2013, can be criticised for being worse than US's "Patriot Act" because it bypasses requirements for surveillance to be necessary and proportionate. The law encompasses and permits collection of all imaginable forms of data,²⁰

16 Pakistan Telecommunication (Re-organization) (Amendments) Act, 2006.

17 Pakistan Telecommunication Authority (PTA). (2010, December 2). No.17-1/2010/Enf/PTA (VPN) I Use Of VPNs/Tunnels and/or Non-Standard SS7/VoIP Protocols. Retrieved from Internet Service Providers Association of Pakistan (ISPAK): www.ispak.pk/Downloads/PTA_VPN_Policy.pdf

18 Pakistan Telecommunication Authority. (2014). PTA response. bolobhi.org/wp-content/uploads/2014/05/PTA-response.jpg

19 Abbasi, A. (2014, December 5). Grey phone traffic: IT authorities passing the buck to ISI. *The News International*. www.thenews.com.pk/Todays-News-13-27079-Grey-phone-traffic-IT-authorities-passing-the-buck-to-ISI

20 "[D]ata, information or material in any documented form, whether written, through audio-visual device, CCTV, still photography, observation or any other mode of modern devices or techniques, [...] e-mails, SMS, IPDR (internet protocol detail record) or CDR (call detail record) and any form of computer based or cellphone based communication and voice analysis. It also includes any means of communication using wired or wireless or IP (internet protocol) based media or gadgetry." Investigation for Fair Trial Act, 2013. www.na.gov.pk/uploads/documents/1361943916_947.pdf

taking state surveillance of communications to previously unheard of levels. The act obviates the need to serve a warrant permitting the authorised surveillance body to collect data when the nature of the surveillance or interception "is such that it is not necessary to serve the warrant on anyone," which is vague and unspecific.²¹ Further, the law takes away the option of service providers refusing to provide user data to spy agencies. Failure to cooperate by allowing backdoors into private user data, or by disclosing information about such co-operation, carries the punishment of imprisonment of one year and/or a fine of up to 10 million rupees (roughly USD 101,000). The secrecy implicit here has obvious implications for any user-notification mechanisms pertaining to the issuing of any surveillance warrant.²²

While the Act provides for some public and judicial oversight, these are feared to remain theoretical as most operations undertaken by intelligence agencies remain beyond the reach of law and oversight as pointed out earlier. Also, the level of well-documented intimidation tactics and influence that impact on court decisions in Pakistan²³ would bear negatively on the efficacy of such oversight.

Jahanzaib Haque, editor of Dawn.com, says of the recent pro-surveillance legislation: "Due to a mixture of both fear and ignorance, parliament has passed extremely regressive legislation that leaves the public, and especially journalists, exposed to the threat of state surveillance that will inevitably result in misuse in the current form."²⁴

Indeed, most known instances of harassment of civilians through surveillance, especially women politicians²⁵ and HRDs, have taken place without the expression of any legitimate aim and without appropriate measures. Indicative of an absolute lack of transparency, there still are few or no official records available pertaining to the procurement of advanced surveillance technologies such as FinFisher, the presence of which (in the country's cyberspace) was revealed by a detailed report published by the Citizen Lab at the University of

21 Ibid.

22 Ibid.

23 Deutsche Welle. (2014, March 11). Pakistan postpones Musharraf trial amid threats from al Qaeda, Taliban. *Deutsche Welle*. www.dw.de/pakistan-postpones-musharraf-trial-amid-threats-from-al-qaeda-taliban/a-17487157; Sattar, B. (2014, April 12). Lawyer Babar Sattar critiques Pakistan Protection Ordinance. *Siyasat aur Qanoon*. (M. Pirzada, interviewer). tune.pk/video/2592131

24 Interview with Jahanzaib Haque, July 2014.

25 Dawn.com. (2011, August 5). No end to phone tapping of women MNAs. *Dawn.com*. www.dawn.com/news/649648/no-end-to-phone-tapping-of-women-mnas

Toronto.²⁶ A court case by Bytes for All, Pakistan attempting to resolve the questions pertaining to the elusive usage of this Trojan technology has been pending in the Lahore High Court since 2013. The Pakistani government is also known to be a client of Narus, a company that sells internet monitoring solutions.²⁷ Further, in an attempt to “eradicate crimes”, the government has also purchased a state-of-the-art monitoring and surveillance system from a company known as GCS.²⁸

According to Gulalai Ismail, a women’s rights defender and chairperson of Aware Girls who is based in the conflict-affected province of Khyber Pakhtunkhwa, “Last December, when I was launching an intensive peace programme in the Malakand Division, the state agencies came to inquire about the programme. I was shocked when I was told that I and my social media communications had been under surveillance for the last three years... In my communication with the agencies it was clear that my work for peace and human rights was seen as ‘anti-state’, and I was seen as an enemy rather than an activist.”²⁹

The most recent reinforcement for conducting communications surveillance has come in the form of the Pakistan Protection Bill (PPB) 2014. Apart from legitimising a number of violations, it is essential to note that the bill discusses “crimes against computers including cybercrimes, internet offences and other offences related to information technology, etc.” as scheduled offences, despite that fact that no form of cyber/electronic crimes ordinance exists in the country that could comprehensively define the nature and scope of these offences. Existing individual protection mechanisms and safeguards against illegitimate access also need re-examining in light of the current possibilities of misuse.³⁰

Conclusion

The residents of Pakistan are subject to mass surveillance by local and international governments. Recent laws that focus on dealing with terrorism,

such as the Fair Trial Act 2013 and Pakistan Protection Bill 2014, are feared to legitimise pernicious and wide-ranging communications surveillance.

While apparently intended to address issues arising from the war against terror and national security, surveillance has been and is being used for political reasons, leading to invasions of privacy, intimidation and blackmail, often targeted at civil society actors such as journalists and HRDs, as well as political activists and elected politicians.

Communications surveillance by intelligence agencies such as the ISI – the existence of which itself is not covered by any act of parliament and is therefore without any legal basis – is entirely extra-legal. Attempts at bringing such agencies within the purview of law have failed so far. This has grave implications for transparency and the rule of law, and has paved the way for continuing human rights violations with impunity.

Owais Aslam Ali, secretary general of the Pakistan Press Foundation (PPF), sums it up by calling the scale of surveillance in Pakistan “breathtaking”. Highlighting the lack of awareness of this issue amongst the public, he says, “Right now, there’s some awareness about mobile phones being risky. The awareness of the internet and email being equally dangerous has not yet permeated the journalist community... [It needs to be understood that] nothing is private [anymore]. [Without] confidentiality of sources [...] all you’ll be left with are different forms of press releases.”³¹

Action steps

The following advocacy steps are recommended in Pakistan:

- An overarching framework needs to be developed for issues of free expression, privacy, data protection, security, surveillance, etc. Civil society should advocate for the alignment of existing fragmented pieces of ICT policies, and the drafting of a comprehensive policy through a multi-stakeholder process. Such a policy should replace the current non-transparent inter-ministerial committees that function in lieu of transparent policy.³² The policy should ensure independent public oversight of any acquisition of surveillance technologies. Such oversight should be designed to take into account the

potential for human rights violations inherent in these technologies.

- Certain surveillance-focused provisions in laws such as the Investigation for Fair Trial Act 2013 that are considered predatory to human rights need to be examined against international human rights benchmarks, such as the International Principles on the Application of Human Rights to Communications Surveillance,³³ and challenged in courts of law.³⁴
- With regard to international surveillance, Pakistani civil society must become active in relevant international forums to pressure foreign governments to cease mass surveillance of Pakistani citizens.³⁵
- Public awareness needs to be raised regarding the risks of communications surveillance and ways to counter it through digital security tools and skills.

- Public awareness about how communications surveillance violates fundamental human rights standards needs to be raised in order to pressure the government and influence policy change.
- Civil society must lobby to bring extra-legal intelligence agencies within the purview of law.
- The link between various forms of electronic communications surveillance and offline methods of surveillance needs to be highlighted for traditional HRD organisations not necessarily well-versed in the latest issues on internet governance, online privacy, modern technology and human rights.

26 Bytes for All, Pakistan. (2013, May 1). Notorious spy technology found in Pakistan. Bytes for All. content.bytesforall.pk/node/99; Khan, A. Z. (2013, May 22). Big fish. *The News International*. www.thenews.com.pk/Todays-News-9-178951-Big-fish

27 Privacy International. (n.d.). Narus sells Internet Monitoring technology. *Privacy International*. <https://www.privacyinternational.org/sii/narus/#action>

28 P@SHA. (2014, April 17). GCS delivers Pakistan’s largest citywide surveillance center. P@SHA. pasha.org.pk/2014/04/17/news/gcs-delivers-pakistans-largest-citywide-surveillance-center

29 Interview with Gulalai Ismail, July 2014.

30 Protection of Pakistan Ordinance, 2014. www.dhrpk.org/wp-content/uploads/2014/02/PPO-with-amendments.pdf

31 Interview with Owais Aslam Ali, 26 May 2014.

32 Bajwa, F. (2009, June 29). National Security and Surveillance - Implications for an ICT Policy. *ProPakistani*. propakistani.pk/2009/06/29/national-security-and-surveillance-implications-for-an-ict-policy

33 <https://en.necessaryandproportionate.org/text>

34 Bytes for All’s petition challenging the FTA 2013 is currently under review in the Lahore High Court, Pakistan.

35 Bytes for All in collaboration with Privacy International and other international human rights groups challenged the GCHQ on mass surveillance of Pakistani citizens at the Investigatory Powers Tribunal in February 2014. See: Clark, L. (2014, January 19). Pakistani human rights group sues UK government for discriminatory GCHQ surveillance. *Wired.co.uk*. www.wired.co.uk/news/archive/2014-01/09/pakistan-human-rights-sues-uk

PERU

Rights versus crime: Twenty years of wiretapping and digital surveillance in Peru



Red Científica Peruana and Universidad Peruana de Ciencias Aplicadas

Fabiola Gutiérrez and Jorge Bossio
www.rcp.pe, www.upc.edu.pe

Introduction

The systematic monitoring of citizens by the state in Peru was revealed in 2000, after the collapse of the second administration of ex-president Alberto Fujimori (1995-2000). Fujimori resigned in his last year in office, after a network of government espionage and corruption was revealed. This included video recordings of secret meetings and alleged communications surveillance conducted and managed by presidential advisor Vladimiro Montesinos, working with the National Intelligence Service (SIN). This systematic surveillance by the state resulted in the dissemination of private information, recordings and videos of public officials, journalists and many other influential people.

These events sparked the beginning of the debate around the purpose of surveillance in Peru, and the violation of the right to private communications by state agencies and private entities – and what legislation could be developed to regulate this. This discussion is ongoing, with more cases of communications interception being revealed.

From state surveillance to industrial espionage and hacking

The Constitution of Peru establishes the privacy of communications as an individual right and does not differentiate between digital or non-digital communications. Nevertheless, respect for freedom of expression and association and non-discrimination, which are basic rights, have been violated many times due to the government's interest in tracking opposing opinions, the actions of political opponents, industrial competition or even religious tendencies and sexual preferences.

It is generally recognised that the state has the tools for monitoring, and can do so within a legal framework, with judicial approval, including in cases of suspected terrorism and crime. But, for instance, Peruvian legislation on cyber crime has also included a modification on what is permissible

when it comes to tapping telephones, a change that has been met with criticism.

Over the past 15 years there have, as a result, been several cases of communications violations, both by the state and individuals. Among the most notorious cases: the surveillance by the Fujimori government; industrial espionage that revealed the corruption of officials in influence peddling and lobbying; the dissemination of private telephone conversations of electoral candidates; and the publication of the email communications of government ministers by journalists.

The Fujimori government, the intelligence services, and the use of the military for surveillance (2000)

The history of the regime of Alberto Fujimori, president of Peru during two consecutive terms (between 1990 and 2000), is stained by the corruption that led to his resignation. His presidential adviser Vladimiro Montesinos had a starring role in this story full of espionage and extortion, and even kidnapping and murder.

Montesinos effectively became the chief of intelligence services, where he allegedly created a giant spy network using army personnel and monitoring equipment, intercepting communications and recording videos of public officials, journalists, media entrepreneurs and other influential people.

Industrial espionage: The case of Business Track (2008)

Authorities found some 60,000 intercepted emails by journalists and politicians opposed to the government in the computer systems of the general manager of the private security firm Business Track, Manuel Ponce Feijoo, a retired Navy officer. Evidence of the wiretapping of officials and business executives was also discovered. The most relevant case was called *Petroaudios* (the so-called “oil recordings”), in which telephone conversations about illegal negotiations involving state oil concessions that would benefit a foreign company (Norway's Discover Petroleum Company) were recorded and disseminated. Following this discovery, the illegal

practices of a private company engaged in systematic espionage came to light.¹

Communications violation: Monitoring a candidate for the mayoralty of Lima (2010)

On September 2010, during the election campaign for the mayoralty of Lima, a television programme broadcast an audio clip of a private telephone conversation between Christian People's Party candidate Lourdes Flores Nano and a former congressman from her party, Xavier Barron. In the conversation, Flores said that she no longer cared about the election, after the results of a preliminary voter poll in which her opponent, Susana Villarán, took the lead for the first time. “I am not interested in this election crap,” she said in the extracts that were released, prompting her precipitous decline in voter preferences. This audio recording was a determining factor in her loss of the election.

National Security: Violation of a minister's official emails by LulzSec/Anonymous Peru (2013)

The hacker group LulzSec Peru, collaborators of Anonymous, obtained and shared emails from the Ministry of Interior, including the minister, Walter Alban. Digital communications about issues such as the tracking of regional opposition leaders, the security of officials and prosecutors' investigations were intercepted. The hackers said their intention was to prove the vulnerability of state information systems.

The weak line: Private versus public

After the dismantling of the National Intelligence Service (SIN) following numerous cases of secret video recordings being made and communications monitored during the Fujimori regime, a new intelligence agency called the National Intelligence Directorate (DINI) was created. A couple of years ago, it came to light that the budget for the DINI was increased in order to monitor public network repositories like social networks, forums or general topic lists, arguing that the use of these online platforms meant that this was not a violation of private communications.

However, this surveillance is on the borders of what is considered private and public, and raises the problem of the legality of monitoring the public in general without any suspicion of a crime being committed.

The surveillance by the DINI sparked a debate about access to and protection of information, as it cannot be argued that it has been done with a legitimate interest in mind – if this were the case,

the law would have been followed and a court order would have been obtained. Although the increase in the budget allocated to the DINI is to monitor public networks, if they already do so illegally, the suspicion that they perform other types of communications surveillance looms with great force.²

The legal framework

Legislation relating to cyber crime in Peru is a relatively new category under the Penal Code. In 2000, provisions relating to espionage or computer hacking (Article 207-A) and computer sabotage (Art 207-B), that were within the scope of crimes against private property, were included. However, it became apparent over time that these did not respond to the needs of protection required when it came to information and communications technologies (ICTs).

In 2011, when the bill for the Cybercrime Law was presented to Congress, its original version meant that the police could access digital communications, and legislators felt that it did not respond properly to the right to privacy of communications. They argued that this right extends to all types of communication, and the bill had to be corrected.

The state filed a new version of the draft law, which was finally approved. However, the approved law was also questioned, because it prohibits, on the one hand, the creation of databases using any public information (which contradicts the law on access to information), and, on the other hand, leaves legislative gaps regarding telephone interceptions.

Cybercrime Law

On 22 October 2013 the new Cybercrime Law³ was approved. This law was inspired by the Budapest Convention on Cybercrime⁴ – although Peru is not a signatory to this international convention.

The new law punishes those who, using ICTs, “introduce, delete, copy, spoil, alter or suppress data, or render data inaccessible” for criminal purposes; those who engage in digital espionage, including telephone interceptions; engage in sexual harassment; and distribute child pornography.

Regarding telephone interceptions, the penalty for this offence has been increased to a maximum of eight years when it comes to classified or “secret and confidential” information. It also includes aggravating circumstances when the offence compromises national security, or when it is performed by public officials or those linked to these officials.

1 Romero, C., & Véliz, A. (2010, April 26). Tenía 53 mil emails hackeados. *La República*. www.larepublica.pe/26-04-2010/tenia-53-mil-emails-hackeados-o

2 Interview with Erick Iriarte A., lawyer and founding partner of Iriarte & Asociados (www.iriartelaw.com), 24 May 2014.

3 Law No. 30096 of 2013.

4 conventions.coe.int/Treaty/EN/Treaties/Html/185.htm

But the Cybercrime Law violates at least two other rights:

Access to information

The law establishes a sentence of three to six years for persons found guilty of capturing digital information from a public institution, such as what is spent on social programmes, and complements this with new data to analyse the information (such as when a journalist analyses public data from different sources, creating a new data set). Critics of this legislation understand that at this point it contradicts the Law on Transparency and Access to Public Information.⁵

Article 6 of the law on access to information makes it a criminal offence to use data without permission, which means that anyone who accesses public information without authorisation and creates a database where this information could be disseminated would be guilty of a crime. In this way, access to public information and the right to freedom of information are limited.⁶

This observation sparked the debate among politicians, civil society and experts and prompted a review. Article 6 was repealed in March 2014.

Information freedom

The amended article regarding telephone interceptions included in the Cybercrime Law goes as far as to punish any kind of monitoring, regardless of the purpose. This makes the privacy of communications so strict that the monitoring of public officials in order to secure transparency is also prohibited, affecting citizens' freedom of information and their ability to conduct research in the public interest. The exemption that applies to the media, and which refers to an exemption of the penalty when investigating or monitoring issues of public interest, was not included in the amendments of the law passed.

Conclusions

Mass surveillance by the Peruvian state has not been proven in recent years; however, it is known that the national intelligence services are treading a thin line of legality through their use of surveillance tools to monitor citizens' publicly shared information, which according to the norm is a crime too. The increase in the budget for the DINI suggests that they could be doing more than that. Ideally, these resources should be directed to using surveillance as a tool for protection and security – but we do not know yet know if that is the case.

Regarding the legal framework for surveillance, the biggest problem is not the law itself, but its interpretation and application. This creates the need for specialised training for legal practitioners, prosecutors and law enforcement authorities in technical terms and standards and technological methods related to the violation of communications in all aspects.

The Cybercrime Law appears to affect freedom of information legislation, which guarantees transparency in the public sector. The Cybercrime Law also impacts negatively on other genuine rights that allow society and individuals to exercise democratic control and play an oversight role. The fact is that what one law defends, the other blocks.

Undeniably, the many cases of interception pushed the approval of the Cybercrime Law, in the pursuit of legal mechanisms to curb such crimes. However, the result reflects little analysis on the topic, poor legal specifications, little precision in the application of the law, and the lack of a conscious review of comparative international laws that could have contributed to making it more efficient and appropriate.

Action steps

The debate on how to improve the Cybercrime Law should continue. Specifically, it should include the clause on media exemption in order to keep track of what is considered in the public interest. In this sense, it is also crucial to protect the right to freedom of information and investigation, which serves as a mechanism for citizen control in governmental affairs.

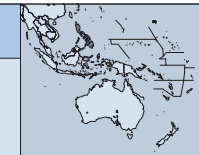
Given the uniqueness of the environment in which it must be applied, the Cybercrime Law could be reviewed by legal practitioners and compared to similar laws in other countries. It would also be advisable to add some kind of standard glossary of terms as an interpretive guide.

Civil society organisations that are frequently monitored should place more importance on the need to encrypt information and have reliable security mechanisms for their communications. Security protocols and devices can be used to prevent communications being violated. Internet service providers (ISPs) must guarantee their users reliable and safe communications, since it is very likely that intermediaries are used in surveillance.

Finally it is clear that the opposition, civil society and the media cannot give up fighting for their rights to privacy and to exercise their oversight of public affairs. The state will always try to find ways to control its citizens, and Peruvians already know that surveillance is just one of these ways.

PHILIPPINES

Communications surveillance in the Philippines: Laws and the struggle for the right to privacy



Computer Professionals' Union

Rick Bahague
www.cp-union.com

Introduction

The Philippines has been crowned the “texting capital of the world”¹ the “social networking capital of the world”,² and its financial district is ranked as the “selfiest city of the world”.³ Data is voluntarily uploaded and shared by its “netizens” on social media networks through mobile and landline networks and is a gold mine for any state surveillance activities. Its 106.5 million mobile subscribers sent two billion text messages daily last year. Fixed telephone subscription is almost non-existent, with a telephone density of four subscribers for every 100 inhabitants, and mobile subscriptions serve as the main communications tool. The digital divide has, however, plagued the country even after the deregulation of the telecommunications industry. The Philippines is ranked 98th in the world on the Information and Communications Technology Development Index (IDI),⁴ with the lowest score compared to its Asian neighbours.

There are two monopolies controlling the telecommunications industry in the country: Globe Telecoms and Philippine Long Distance Telephone (PLDT). Telecommunications infrastructure is under the control of corporations. Government communications and transactions have to pass through this private network infrastructure, which is a concern for sensitive information. Because of this, most state surveillance activities would require some cooperation from any of the telecoms monopolies. In fact, the controversial “Hello Garci” wiretapping

incident, which will be the focus of this report, was accomplished with the facilitation of one of their personnel.

Furthermore, the Philippines has been a long-time ally of the United States (US), being a former colony. Various agreements are in place which allow the US Armed Forces to use local resources for military exercises, to strategically position their weapons, and for mass surveillance activities. Edward Snowden revealed in March that the MYSTIC surveillance programme run by the US National Security Agency (NSA) monitors local telcos⁵ and “scrapes mobile networks for so-called metadata – information that reveals the time, source, and destination of calls.”⁶

While other governments in countries like Brazil and Germany protested the unlawful surveillance by the NSA, Philippine President Benigno Simeon “Noynoy” Aquino is not even familiar with the incident and has approved another agreement with the US on enhanced defence cooperation, which will open up more surveillance activities. In a statement, the Computer Professionals' Union (CPU) warned that the Enhanced Defense Cooperation Agreement (EDCA) “is an invitation for surveillance, drones and establishment of new listening posts violating rights to privacy and sovereignty.”⁷

In this report, we look at the state of communications surveillance in the Philippines, focusing on government policies and how they were applied in a wiretapping incident. It remains to be seen if these policies can be used against the growing US military presence in the country.

⁵ Law No. 27806 of 2002.

⁶ Interview with Roberto Pereira C., lawyer and legal consultant at the Press and Society Institute (IPYS) (www.ipys.org), 14 May 2014.

¹ Tuazon, J. M. (2012, December 4). 20 years on, SMS remains king in the ‘texting capital of the world’. *Interaksyon*. Accessed July 17, 2014. www.interaksyon.com/infotech/20-years-on-sms-remains-king-in-the-texting-capital-of-the-world (20 years on, SMS remains king in the ‘texting capital of the world’. *Interaksyon*)
² MST Lifestyle. (2013, May 21). PH is social networking capital of the world. *Manila Standard Today*. manilastandardtoday.com/2013/05/21/ph-is-social-networking-capital-of-the-world
³ Golangco, V. (2014, March 13). Sexy and social: why Manila is the selfiest city in the world. *The Guardian*. www.theguardian.com/cities/2014/mar/13/manila-selfiest-city-most-selfies
⁴ International Telecommunication Union. (2013). *Measuring the Information Society 2013*. www.itu.int/en/ITU-D/Statistics/Pages/publications/mis2013.aspx

⁵ Robinson, K. (2014, May 22). ‘NSA Gone Wild’ in the Bahamas, Mexico, Kenya, the Philippines and more. *AccessNow.org*. <https://www.accessnow.org/blog/2014/05/22/nsa-gone-wild-in-the-bahamas-mexico-kenya-the-philippines-and-more>
⁶ Devereaux, D., Greenwald, G., & Poitras, L. (2014, May 19). Data Pirates of the Caribbean: The NSA Is Recording Every Cell Phone Call in the Bahamas. *The Intercept*. <https://firstlook.org/theintercept/article/2014/05/19/data-pirates-caribbean-nsa-recording-every-cell-phone-call-bahamas>
⁷ Computer Professionals' Union. (2014, March 2). Enhanced defense cooperation: an invitation for surveillance, drones and unregulated communications. *Computer Professionals' Union*. www.cp-union.com/article/2014/05/02/enhanced-defense-cooperation-invitation-surveillance-drones-and-unregulated

Policies on communications surveillance

There are several policies governing surveillance, such as the Anti-Wiretapping Law, Cybercrime Law, Data Retention Law, Human Security Act, and E-Commerce Act. In addition, the National Telecommunications Commission has a standing Memorandum Circular for the retention of data by telecommunications companies.

The Anti-Wiretapping Act (AWA) enacted on 19 June 1969 is the first law regulating communications surveillance in the country. Section 1 of the AWA⁸ specifically states: “It shall be unlawful for any person, not being authorized by all the parties to any private communication or spoken word, to tap any wire or cable, or by using any other device or arrangement, to secretly overhear, intercept, or record such communication or spoken word by using a device...” However, “any peace officer, who is authorised by a written order of the Court” upon a “written application and the examination under oath or affirmation of the applicant and the witnesses” can do this.

Before being granted authorisation, the AWA enumerates particular strict conditions that have to be met: (1) “that there are reasonable grounds to believe that any of the crimes enumerated [...] has been committed or is being committed or is about to be committed,” (2) “that there are reasonable grounds to believe that evidence will be obtained essential to the conviction of any person for, or to the solution of, or to the prevention of, any of such crimes,” and (3) “that there are no other means readily available for obtaining such evidence.”

Furthermore, the AWA requires that authorisation should (1) identify the person or persons to be listened to, (2) identify the peace officer to overhear the communication, (3) identify the offence or offences committed or sought to be prevented, and (4) the period of authorisation. All conversations recorded are then to be submitted to the court within 48 hours after the expiration of the authorisation.

Section 3 of the Bill of Rights enshrined in the 1987 Philippine Constitution⁹ guarantees every Filipino citizen the right to privacy of communication. It states: “(1) The privacy of communication and correspondence shall be inviolable except upon lawful order of the court, or when public safety or order requires otherwise, as prescribed by law.” It specifically discourages authorities from conducting unlawful surveillance, otherwise: “(2) Any evidence obtained in violation of this or the preced-

ing section shall be inadmissible for any purpose in any proceeding.” As such, the current Revised Penal Code penalises any unlawful entry, search or seizure carried out in violation of the Bill of Rights.

Republic Act 8792 or the Electronic Commerce Act of 2000¹⁰ was the first law to govern electronic transactions in the age of internet in the country. It has a dedicated section (Section 31) on privacy or lawful access: “Access to an electronic file, or an electronic signature of an electronic data message or electronic document shall only be authorized and enforced in favor of the individual or entity having a legal right to the possession or the use of the plaintext, electronic signature or file and solely for the authorized purposes. The electronic key for identity or integrity shall not be made available to any person or party without the consent of the individual or entity in lawful possession of that electronic key.”

On 6 March 2007, the Human Security Act (HSA)¹¹ was signed into law by former President Gloria Macapagal-Arroyo. Section 7 of the HSA specifically allows law enforcement agencies to “listen to, intercept and record, with the use of any mode, form, kind or type of electronic or other surveillance equipment or intercepting and tracking devices, or with the use of any other suitable ways and means for that purpose, any communication, message, conversation, discussion, or spoken or written words” between people identified by the government as “terrorists” – or even on the slight suspicion of being terrorists.

Five years later, the Cybercrime Prevention Act of 2012 (CPA 2012)¹² was signed by current President Aquino. Section 12 of the law gave law enforcement agencies the power to “collect or record by technical or electronic means traffic data in real-time associated with specified communications transmitted by means of a computer system.” In February 2014, the Supreme Court struck down this section of the CPA 2012 and ruled that real-time collection of network traffic violates the constitution.

A month before CPA 2012 was put into law, Aquino signed the Data Privacy Act of 2012 (DPA 2012). This law defined the rights of a “data subject” as well as the responsibilities of “data processors” to ensure privacy while “ensuring free flow of information to promote innovation and growth.” It created the National Privacy Commission where all complaints on “unauthorised processing of personal

information and sensitive personal information”, “accessing personal information and sensitive personal information due to negligence”, “improper disposal of personal information and sensitive personal information”, among others, would be heard and processed. While there are no specific provisions on surveillance *per se*, the rights given to “data subjects” and prohibited acts are added safeguards against any kind of surveillance, in particular from the state.

As part of its regulatory function to protect users of telecommunications services, the National Telecommunications Commission also released a memorandum in 2007 on the data log retention of telecommunications traffic.¹³ This memorandum is unnecessary from a privacy perspective, but was otherwise implemented. It “aims to further strengthen the welfare and protection afforded to end-users and/or consumers” by directing telcos to record and store voice and non-voice traffic for at least two months. To date, even with this memorandum, no one has been reprimanded for SMS spamming. This phenomenon is a common problem now, where advertisers use personal data collected illegally.

The “Hello Garci” wiretapping incident

It would take an alleged taped conversation of former President Arroyo during the 2004 elections to demonstrate that communications surveillance is happening in this country.

After the ouster of President Joseph Estrada in 2011, Arroyo, then vice-president, assumed office. Arroyo is perceived to be the most corrupt president of the republic.¹⁴ IBON Foundation, a local think tank, estimated that PHP 7.3 billion (USD 181 million) of public funds were lost during her seven years in power.¹⁵ In 2011, she would be charged with electoral fraud and plunder.¹⁶ Among the popular evidence of her involvement in rigging the 2004 presidential election was a wiretapped conversation with an election commissioner which came to be known as the “Hello Garci Scandal”.

A complete transcript of the wiretapped conversation¹⁷ and a recording of the full conversation¹⁸ are available on the website of the Philippine Center for Investigative Journalism (PCIJ). In this transcript, Arroyo called Commission on Elections (COMELEC) Commissioner Virgilio Garcillano (Garci) several times to ensure a lead of no less than one million votes against the popular rival Fernando Poe Jr. in the presidential race. She also made sure that documents to support this lead were consistent. In one conversation, she asked for the statement of votes (individual summary of votes from towns and municipalities) to make them consistent with the certificate of canvass (consolidated votes in the province).

The Hello Garci operation brought a 12-0 win for Arroyo’s party in Lanao del Sur, a province in the southern island of Mindanao. In a Philippine election, voters select 12 senators in a ballot. It was an election manipulation operation which happened “with the complicity of the military, the COMELEC and even Malacanang,”¹⁹ according to Sheila Coronel of the PCIJ. (Malacanang or Malacanang Palace is the official residence and office of the Philippine president.)

The wiretapped conversations were released on 6 July 2005 by no less than Presidential Spokesperson Ignacio Bunye. Arroyo addressed the nation in a televised speech on 27 June 2005 to apologise for the “mistake” of calling Garci and assured the people that she did not cheat in the previous election.²⁰

The Hello Garci wiretapping incident was investigated by the Philippine Senate. It turns out that a military intelligence operation known as Project Lighthouse supervised the wiretapping of Garci and other individuals in the opposition. The Intelligence Services of the Armed Forces of the Philippines (ISAFP) working with personnel of a telco network made the wiretapping possible.²¹

The Hello Garci scandal exposed the manipulation of the most sacred right of the people in a democracy, elections. Furthermore, it also showed the current extent of communication surveillance performed by state forces.

8 www.lawphil.net/statutes/repacts/ra1965/ra_4200_1965.html

9 www.gov.ph/constitutions/the-1987-constitution-of-the-republic-of-the-philippines

10 www.ipophil.gov.ph/images%5Cipenforcement%5CRA8792-E-Commerce_Act.pdf

11 www.congress.gov.ph/download/ra_13/RA09372.pdf

12 www.gov.ph/2012/09/12/republic-act-no-10175

13 Data Retention of Telecommunications Traffic, Memorandum Circular 04-06-2007, National Telecommunications Commission, 8 June 2007.

14 Gopalakrishnan, R. (2007, December 11). Arroyo “most corrupt” Philippine leader: poll. *Reuters*. www.reuters.com/article/2007/12/12/us-philippines-arroyo-idUSSP30281220071212

15 GMA News.TV. (2008, March 4). IBON: Corruption scandals under Arroyo cost Filipinos P7.3B. *GMA News.TV*. www.gmanetwork.com/news/story/83278/news/nation/ibon-corruption-scandals-under-arroyo-cost-filipinos-p7-3b

16 Associated Press. (2011, November 18). Philippines charges Gloria Arroyo with corruption. *The Guardian*. www.theguardian.com/world/2011/nov/18/philippines-asia-pacific

17 pcij.org/blog/2005/06/25/downloadables-section/3

18 pcij.org/blog/2005/06/25/downloadables-section

19 Coronel, S. (2005, November 2). Lanao’s dirty secrets. *Philippine Center for Investigative Journalism*. pcij.org/stories/lanaos-dirty-secrets

20 A transcript of the president’s speech is available on the PCIJ website: pcij.org/blog/2005/06/28/the-president-says-i-am-sorry-i-want-to-close-this-chapter-2

21 GMA News.TV. (2007, August 22). Doble: ‘Hello Garci’ wiretap ops done through Smart mole. *GMA News*. www.gmanetwork.com/news/story/57157/news/nation/doble-hello-garci-wiretap-ops-done-through-smart-mole

Surveillance of social movements

The Philippines has a vibrant protest and social movement. In 2001, technology played an important role in the ouster of President Joseph Estrada over allegations of corruption. TXTPower, a group composed of mobile subscribers, was active in the use of text messaging during the “Oust Erap Campaign” of various sectors (“Erap” was Estrada’s nickname). It would also later launch a similar initiative against Arroyo.

Activists involved in social movements in the country are concerned with reports of electronic communication surveillance by state forces. The “Hello Garci” incident amplified these doubts. Moreover, the record of bringing justice to more than 1,206 victims of extrajudicial killings, 206 victims of forced disappearances, 2,059 victims of illegal arrests and 1,099 victims of torture during the Arroyo regime has been questioned in the second cycle of the Universal Periodic Review of the United Nations Human Rights Council.²² The Philippine government is a signatory to the International Covenant on Civil and Political Rights (ICCPR), International Covenant on Economic, Social and Cultural Rights (ICESCR) and the Universal Declaration of Human Rights.

If recent reports are to be believed, the current Aquino administration has purchased PHP 135 million (USD 3 million) worth of high-end surveillance equipment to spy on its critics.²³ This will be used by the ISAFP, which is alarming for social activists. ISAFP is the same agency that spearheaded the “Hello Garci” incident. It is now common activist practice that other than the usual personal security orientation, a discussion on information security is held so that they can take precautions.

Activists have also raised the alarm on the current regime’s EDCA. For them, “allowing US troops to position equipment which will definitely include surveillance equipment and drones with free access to the radio spectrum is the best recipe for mass surveillance.”²⁴

This year, the Supreme Court nullified the real-time collection of data provision in the Cybercrime Act. This was declared unconstitutional, heeding the campaigns of the CPU and other netizen groups. However, libel, the most contested provision of the

Act, which stifles freedom of expression, was upheld as within the frames of the constitution.

Violating the constitution and international norms

Wiretapping is a form of communications surveillance. The Philippines does not lack laws prohibiting and regulating it. The country’s AWA and HSA are both a starting point for defining legitimacy, adequacy and necessity of surveillance. Both laws also have strict requirements for enforcement officers, which include authorisation from a judicial authority in the conduct of surveillance, due process and user notification. Moreover, any unauthorised surveillance is penalised with 10 to 12 years of imprisonment in the HSA.

While the Hello Garci incident exposed the rotten and corrupt system of the Philippine elections, it also demonstrated blatant disregard of the right to privacy and the 13 International Principles on the Application of Human Rights to Communications Surveillance.²⁵ It was conducted without court permission, due process or user notification, and revealed that telco companies and state authorities were working together. Until now, the intention of the wiretapping of Commissioner Garcillano which caught former President Arroyo by chance is unclear.

Even with existing laws legitimising communications surveillance, the practice remains problematic. The HSA, AWA and Cybercrime Act are widely opposed to too much power being given to the state. While judicial authority is required by these laws, opposition is still strong due to the doubtful impartiality of courts in issuing surveillance permissions.

Public oversight has yet to be seen in the implementation of the HSA. The law prescribes a Grievance Committee composed of the Ombudsman, the Solicitor General, and the undersecretary of the Department of Justice. The Committee is tasked to receive, investigate and evaluate complaints against the police and other state forces regarding the implementation of the law. An Oversight Committee, composed of senators and members of congress, has also yet to publish reports on its oversight functions.

Lack of integrity of communications and systems

Hello Garci was the first proof that the state and monopoly telcos are working together to track citizens.

It has created awareness among the general public that telcos and the government are tracking calls and text messages without court permission and user notification.

In the case of the Hello Garci incident, a special model of phone was used to receive calls diverted to it by the telco for recording.

Furthermore, a memorandum circular from the National Telecommunication Commission (NTC), the regulatory body overseeing telco monopolies, allows storage of voice and non-voice data supposedly to serve as reference for consumer complaints.²⁶ While intended for prosecution of consumer complaints, a similar section on real-time traffic monitoring in the Cybercrime Act was ruled as unconstitutional by the Supreme Court.

The Philippines is part of the NSA’s MYSTIC and PRISM surveillance programmes

The country has more than a hundred years of being tied to the NSA in the US. In the early 1900s, in the great Philippine-American War, surveillance techniques were already employed. To defeat the Filipino guerrillas fighting for independence, the US army “created five integrated security agencies, a centralised telephone network, fingerprinting, photographic identification and index of police files of 200,000 alphabetised file cards with the means to collect, retrieve and analyse a vast amount of intelligence.”²⁷

Last March, Edward Snowden revealed that all text messages and calls passing through the two telco monopolies in the Philippines are captured by the NSA. With more than 100 million users of mobile telephones, and a vibrant protest movement which is demonised for its militancy, the US has all its reasons to implement mass surveillance in the country. In 2013, Snowden also said that the NSA has an established listening post in Manila to conduct mass surveillance against other Asian countries.

Recently, a new agreement with the US was signed by the Department of Foreign Affairs. The EDCA allows US weapons to be based in the country. The US has a rotating military presence through its frequent military exercises allowed by the Visiting Forces Agreement (VFA). The EDCA has been studied by a group of computer professionals and was found to be “an invitation for unregulated communication and surveillance” due to its provision of

allowing US troops to use the full radio spectrum, which is heavily regulated by the National Telecommunications Commission.

Conclusions

The Philippines has established laws on communications surveillance since 1969. Its constitution also regards privacy as a fundamental right of its citizens. In the Hello Garci scandal, where former President Arroyo was caught as she allegedly instructed Commissioner Garcillano – who was being wiretapped by the intelligence agency of the armed forces – to rig the 2004 presidential election in her favour, the right to privacy and the principles of judicial authority, due process and user notification were not applied. This also verified the fears of activists and privacy advocates on the possible connivance between telcos and state forces to track electronic communications.

Furthermore, the country has a long history of being part of NSA spy programmes. Its previous and present administrations have been subservient to US interests, which includes allowing the establishment of listening posts by the NSA to establish listening posts, the capture of massive amounts of metadata on mobile networks, and the importing of surveillance equipment through the EDCA and VFA.

However, Filipino netizens are also aware of their political strength, once mobilised. They were active in the ouster of two previous presidents and have shown their capacities again in the 2013 Million People March against the corrupt use of public funds by the current Aquino regime. It did not take long before they realised that the state and the US had been tracking their activities online and offline.

Action steps

The following recommendations can be made so that awareness of the 13 Principles and a stronger sense of the right to privacy are propagated:

- Through campaigns, create awareness of the Snowden revelations and how the state and telcos have cooperated with the NSA to conduct communications surveillance.
- Lobby for an Internet Bill of Rights similar to Brazil’s.
- Call for the strict implementation of the Data Privacy Act to protect citizens from the misuse of data for profit.
- Create forums on information security and privacy rights, similar to CPU’s briefing for social activists.

22 Olea, R. (2012, May 21). Groups score continuing rights abuses as The Philippines and the Universal Periodic Review undergoes review by UN body. *Bulatlat*. Accessed July 17, 2014. <http://bulatlat.com/main/2012/05/21/groups-score-continuing-rights-abuses-as-philippines-undergoes-review-by-un-body/>

23 Tan, K. J. (2014, April 8). Palace backs ISAFP, denies using spy gadgets vs. opposition. *GMA News*. www.gmanetwork.com/news/story/355967/news/nation/palace-backs-isafp-denies-using-spy-gadgets-vs-opposition

24 Computer Professionals’ Union. (2014, March 2). Op. cit.

25 <https://en.necessaryandproportionate.org/text>

26 Data Retention of Telecommunications Traffic, Memorandum Circular 04-06-2007, National Telecommunications Commission, 8 June 2007.

27 Morey, M. (2013, June 25). From Philippines to NSA: 111 years of the U.S. surveillance state. *Occupy.com*. www.occupy.com/article/philippines-nsa-111-years-us-surveillance-state

POLAND

Access to telecommunication data in Poland: Specific problems and general conclusions



Panoptikon Foundation

Katarzyna Szymielewicz and Anna Walkowiak
panoptikon.org

Introduction

Poland, as a member state of the European Union, was obliged to introduce mandatory telecommunication data retention as part of the implementation of the so-called Data Retention Directive.¹ As a result, all telecommunications service providers in Poland have to collect and store so-called *metadata* (i.e. data showing originator, destination, date and time) for at least 12 months. According to the directive, such data should be made available to the competent national authorities only in specific cases and in accordance with national law for the purpose of the investigation, detection and prosecution of serious crimes (as defined by relevant national law).² However, when implementing the directive, Poland failed to introduce these rules regarding the use of telecommunications data for law enforcement purposes. As a result, such information – collected about every person using telecommunication services in Poland – is used even in the prosecution of common crimes (like theft) and for the sake of crime prevention.

Moreover, Polish law does not provide for any safeguards that would prevent abuses, such as an external supervisory mechanism, court oversight, the obligation to inform the person concerned about the use of his or her data or the obligation to destroy data after the end of proceedings.³

Policy and political background

The distinction between security and freedom and the argument that it is not possible to have both are very powerful notions in Polish public debate. It also seems to be commonly accepted that if a certain activity is related to national security, it should be kept secret by default. The argument “because it is useful for law enforcement, it must be good for public security” is raised whenever the lack of accountability of intelligence agencies is mentioned. In addition, law enforcement and intelligence agencies have a strong influence in drafting the laws that are meant to regulate their powers.

This political climate has enabled what human rights advocates perceive as possibly the worst implementation of the Data Retention Directive: Poland opted for the longest possible data retention period (24 months) and, as mentioned, failed to introduce any legal safeguards. Therefore, Polish regulation providing for retention and use of telecommunications metadata has been heavily criticised by human rights advocates, the Ombudsman and the national Data Protection Authority.

As a result of persistent pressure exerted by both human rights organisations and public authorities, in 2011 this legal landscape gradually started to change. The Ombudsman and Prosecutor General filed six official complaints to the Constitutional Court, arguing that various powers attributed to intelligence and law enforcement (including the use of telecommunication data) should be limited. This case is still pending.⁴ In January 2013 the period of telecommunications data retention was shortened to 12 months, but other problems remained.⁵ Further changes, however, are expected because of two legislative proposals that are under discussion: (i) a draft law introducing a special commission to supervise intelligence agencies that investigate complaints from individuals; and (ii) a draft law lim-

iting the access to citizens’ telecommunication data by intelligence agencies.⁶

Surveilling the media: The case of Bogdan Wróblewski

In 2010 one of the most influential Polish daily newspapers, *Gazeta Wyborcza*, published an article claiming that several journalists who specialised in politics were under illegal surveillance. Polish intelligence agencies – namely the Internal Security Agency (*Agencja Bezpieczeństwa Wewnętrznego* or ABW) and the Central Anti-Corruption Bureau (*Centralne Biuro Antykorupcyjne* or CBA) – gained access to telecommunications data retained for public security purposes to spy on at least 10 journalists between 2005 and 2007. The intelligence agencies denied these allegations, but proof of their requests sent to telecommunications service providers proved otherwise. Bogdan Wróblewski, author of the abovementioned article, was among the alleged victims of illegal surveillance.

According to published information, the CBA spied on Wróblewski (back then a journalist specialised in court cases, now at the Supreme Audit Office, the highest public auditing body) by accessing and analysing his telephone accounts for six months – accounts which revealed a list of his contacts, including journalistic sources. This happened exactly when Wróblewski was working on critical articles dealing with special operations conducted by the CBA, which came under public scrutiny because of various irregularities. It seemed clear that the CBA tried to find out who Wróblewski’s sources of information were.

Because of these suspicions, the public prosecutor conducted an investigation to verify whether intelligence agencies acted against the law. Oddly enough, although there was evidence that the CBA and ABW asked telecommunications service providers for data related to journalistic activity, the investigation was closed due to “the failure to detect a crime”. Most of the records of the prosecutor’s proceedings were classified, which made it very difficult for individuals concerned to challenge the outcome.⁷

Due to a lack of other legal measures available to him, in 2011 Wróblewski decided to sue the CBA in civil proceedings, indicating that their actions violated his right to privacy, secrecy of correspondence, freedom of expression and freedom of the press. Wróblewski obtained additional support from civil society organisations that submitted their opinions to the court (*amicus curiae*), emphasising human rights violations. One of those organisations was the Panoptikon Foundation.⁸

In 2012, a district court in Warsaw ruled that the use of Wróblewski’s billing data by the CBA violated his right to privacy and constituted “typical surveillance for unknown purposes”. According to the judge, the CBA should be able to use billing data only for the purpose of anti-corruption proceedings (in accordance with the statutory duties of this agency). The court ordered the CBA to apologise to Wróblewski and to delete all data relating to him that the agency had obtained.⁹ The Court of Appeal dismissed the CBA’s appeal and upheld the ruling – finally, the CBA publicly apologised.¹⁰

Wróblewski’s case showed that imposing the obligation on telecommunications service providers to retain and give intelligence agencies access to their clients’ data without adequate safeguards inevitably leads to human rights violations. What turned out to be very problematic in this case is that Polish law does not require intelligence agencies to delete data once it is no longer necessary to retain it. As a result it may be possible to collect and retain data about a given person for years, even though he or she is not formally suspected of any crime. It is sufficient for intelligence agencies to prove that such person belongs to a “group under special scrutiny” for security purposes. Security purposes vary from allegations of belonging to a terrorist organisation to being part of a religious, political or sexual minority – and in many cases these groups do not justify surveillance.

Without introducing strict control over intelligence agencies’ powers to access citizens’ telecommunications data, and without further legal

1 European Union. (2006). Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC. eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF

2 European Union. (2006). Op. cit.

3 Panoptikon Foundation. (2012, April 3). How many times did the state authorities reach out for our private telecommunications data in 2011? We publish the latest research. *Panoptikon Foundation*. panoptikon.org/wiadomosc/how-many-times-did-state-authorities-reach-out-our-private-telecommunications-data-2011-we

4 Klicki, W. (2014, April 4). Służby przed Trybunałem. *Fundacja Panoptikon*. panoptikon.org/wiadomosc/sluzby-przed-trybunalem

5 Klicki, W., & Szymielewicz, K. (2012, October 15). Sejm jednomyślnie przyjął nowelizację Prawa telekomunikacyjnego. *Fundacja Panoptikon*. panoptikon.org/wiadomosc/sejm-jednomyslne-przyjal-nowelizacje-prawa-telekomunikacyjnego

6 Ministry of the Interior. (2013). Projekt ustawy o Komisji Kontroli Służb Specjalnych. legislacja.rcl.gov.pl/docs/12/181401/181409/181410/dokument87492.pdf; Senate of the Republic of Poland. (2014). Projekt ustawy o zmianie niektórych ustaw w zakresie przepisów dotyczących uzyskiwania i przetwarzania przez uprawnione podmioty danych gromadzonych przez przedsiębiorców telekomunikacyjnych. www.senat.gov.pl/gfx/senat/userfiles/_public/k8/komisje/2014/kpcpp/materiale/wniosek_nik_bilingio3120020140221095724.pdf

7 Czuchowski, W. (2010, October 8). Dziennikarze na celowniku służb specjalnych. *Gazeta Wyborcza*. wyborcza.pl/1,76842,8480752,Dziennikarze_na_celowniku_sluzb_specjalnych.html

8 Panoptikon Foundation. (2011). Opinia przyjaciela sądu (*amicus curiae*) Fundacji Panoptikon w postępowaniu Bogdan Wróblewski przeciwko CBA. panoptikon.org/sites/panoptikon.org/files/opinia_wroblewski.pdf

9 Klicki, W. (2012, April 26). Zwycięstwo dziennikarza w sporze z CBA – będą przeprosiny. *Panoptikon Foundation*. panoptikon.org/wiadomosc/zwyciestwo-dziennikarza-w-sporze-z-cba-beda-przeprosiny

10 *Gazeta Wyborcza*. (2013, April 26). CBA ma przeprosić dziennikarza „Gazety Wyborczej” Bogdana Wróblewskiego za to, że za rządów PiS kontrolowało jego billingi telefoniczne. *Gazeta Wyborcza*.

wyborcza.pl/1,76842,13815430,CBA_ma_przeprosic_dziennikarza_Gazety_Wyborczej_.html#ixzz32LVdHTpP

changes that would limit the legitimate purposes of surveillance, it is likely that cases like Wróblewski's will be repeated.

Conclusions

Telecommunications data retention, by definition, constitutes a serious violation of the right to privacy. Mobile phones are a part of our everyday life and therefore our telecommunications data reveals a lot about our life: from professional to intimate relationships to daily routines. With increasing amounts of data stored by private companies (not only telecommunications or internet service providers, but also shops, banks, insurance companies, health services or energy providers), the issue of legitimacy of data retention and access rules must be revisited. The trend towards retaining more data and broadening the catalogue of purposes that justify its further use should be reversed.

Any surveillance mechanism that targets innocent citizens and leads to the collection of data “just in case it may turn out to be useful” cannot be reconciled with a presumption of innocence. This position has been reinforced by the Court of Justice of the European Union in its recent judgement that declared the Data Retention Directive “invalid from the beginning” because of insufficient human rights safeguards.¹¹ This judgement should be implemented in all European countries.

Currently Polish law does not provide for any independent oversight over intelligence agencies. Only internal control mechanisms are in place, which cannot be treated as independent. As a result there is no way to verify whether Polish intelligence agencies observe at least existing legal safeguards, other than through journalistic investigation or whistleblowing. Wróblewski's case shows beyond doubt that strict control over intelligence agencies' powers to access citizens' telecommunications data is necessary. Such control mechanisms should cover not only the use of data retained for security purposes, but access to all types of data, the use of other surveillance technologies (SIGINT, CCTV, open source intelligence, predictive profiling, etc.) and international cooperation among intelligence agencies.

Institutional checks and balances with regard to surveillance carried out by the state cannot work without sufficient information. Therefore, the main obstacle that we face in demanding more accountability for illegitimate surveillance is secrecy and a

lack of transparency. Polish law does not provide for any reliable mechanism for verifying how many times and for what purposes public entities (law enforcement or any of the nine intelligence agencies) asked for citizens' personal data. This problem affects all types of data and all types of requests, whether telecommunications, electronic services, banking, or social security data.

Currently Polish public authorities are under no legal obligation to register their data requests, nor publish the number of requests or other details. Only telecommunications service providers are required to collect statistics showing how many times they were asked for their clients' personal information. However, research conducted by Panoptikon Foundation in Poland showed that even data that is collected by public authorities cannot be relied on. A simple comparison of statistics published by the Office for Electronic Communications (the supervisory body for telecommunications service providers) and data obtained directly from police and intelligence agencies via freedom of information requests, shows that there is a significant discrepancy. The law should provide for one methodology that would apply to collecting information about the scale and purpose of requests for citizens' data from various sources.

Action steps

Given the above, the following steps should be taken in Poland to secure a human rights framework for surveillance:

- Thanks to Edward Snowden's disclosures, European citizens learned that there is a link between mandatory retention of telecommunications data, introduced by the EU in 2006, and US programmes of mass surveillance. Measures which human rights advocates across Europe have been fighting for the last seven years turned out to be part of something much bigger and much more disturbing. This common context of international mass-surveillance operations should be further explored for advocacy purposes by civil society on both sides of the Atlantic.
- Following the recent ruling of the Court of Justice of the EU, Poland and other European countries should revise their laws that provide for telecommunications data retention without adequate safeguards. However, it will not be an automatic process resulting from the judgement. The judgement itself only affected the Data Retention Directive – not respective national laws. It might be necessary for citizens and the European Commission to take further legal

action. The possibility of bringing a complaint to the European Commission on the grounds that existing national laws are in violation of the European law is worth exploring.

- The need for more transparency in the area where law enforcement and intelligence agencies “meet” private companies and demand citizens' data has become evident, not only with regard to telecommunications data, but even more so with regard to all types of data that are stored by internet service providers. One way

of pursuing this goal is by drafting so-called transparency reports – reports that show not only the scale of surveillance but also explore its purposes and human rights impact. While companies focus on numbers, civil society and researchers should focus on problem analysis, asking pertinent questions on the basis of available data. Panoptikon Foundation drafted such a transparency report for Poland in 2013.¹² Other organisations could build further on this methodology.

¹¹ The Court of Justice declares the Data Retention Directive to be invalid. <http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf>

¹² Panoptikon Foundation. (2013). *Access of public authorities to the data of Internet service users: Seven issues and several hypotheses*. Warsaw: Panoptikon Foundation. panoptikon.org/sites/panoptikon.org/files/transparency_report_pl.pdf

ROMANIA

Back to the digital cage



StrawberryNet Foundation and Sapientia Hungarian University of Transylvania
Rozália Klára Bakó
www.sbn.net.ro, www.sapientia.ro/en

Introduction

Romania joined the European Union (EU) in 2007 – an important step towards integrating its policies into the EU framework, but with several gaps when it comes to information and communications technologies (ICTs).

While the European Court of Justice (ECJ) has rejected the EU Data Retention Directive¹ as invalid,² Romanian legislators were preparing two laws which, if adopted, would throw the country into a “digital cage”: Draft Law 263/2014 on cyber security, and Draft Law 277/2014 on the registration of prepaid mobile SIM cards and public Wi-Fi users.³ Back in 2011, Romania was at the forefront of rejecting the EU Data Retention Directive,⁴ risking sanction from the European authorities. In this context, adopting laws that violate users’ right to privacy in 2014 would be a step back for the ICT policy-making standards in the country.

“Romania is currently undergoing rapid and major technological development, but we have to make sure the new technology respects users’ rights. Under Ceausescu,⁵ Romanians were forced to register all typewriters with the Militia. Today, the government wants all Romanians to register all prepaid SIM cards and record all traffic going through free public Wi-Fi hotspots,” states an online petition launched on 8 June 2014.⁶ This report focuses on two civil society protests against data retention laws in Romania that occurred in June and July 2014.

Policy and political background: Romania in the European context

The process of ICT policy alignment started during Romania’s accession to the EU (2001-2004). Milestones of regulatory changes contributing to an ICT-enabled environment included the liberalisation of the telecommunications market (2003), and legislation dealing with universal access, e-commerce and online security, as detailed in the Romania country report in GISWatch 2007.⁷

While the EU regulatory framework acted as a pulling force, ICT businesses have also pushed Romanian governmental agencies to keep up with regional and global communication trends. Infrastructural development has enabled access to mobile telephony and internet across the country, with narrowing gaps between urban and rural areas, the young and the elderly, the rich and the poor. The mobile broadband penetration rate rose significantly between 2011 and 2013, with 47.6% of the population connected to the internet via mobile devices in December 2013, compared to 21% in December 2011.⁸

Digital literacy gap: Low or no skills

According to the Digital Agenda Scoreboard 2014 for Romania,⁹ which assesses the country’s digital performance based on data available for 2013, the widest gap between Romania and the EU average scores concerns rural fixed-broadband coverage (78% vs 90%), mobile broadband take-up (41% vs 62%), and 4G mobile broadband coverage (27% vs 59%). Partly due to this infrastructural gap,¹⁰ 42% of the Romanian population has never used the internet, compared to the 20% EU average, and only 45% is using the internet on a weekly basis, while the EU average is 72%. Meanwhile, individuals with low or no digital skills represent 85% of the population, significantly higher than

the 47% EU average.¹¹ An alarming ratio of 94% of “disadvantaged” people – individuals who are aged 55-74, have low levels of education and/or are unemployed, retired or inactive – have low or no digital skills, compared to the 64% EU average. Online safety and privacy issues are among the most critical digital skills gaps of Romanian internet users.

A report on EU digital skills issued in May 2014¹² placed Romania at the lowest end of the performance scale for every indicator: general ICT skills, safety, content creation and problem solving online. Even the so-called connected generation Z in Romania lags behind the digital literacy of youth in other countries, as shown in the EU Kids Online project findings,¹³ and the Net Children Go Mobile report.¹⁴ These alarming results show the heightened responsibility for policy makers and society at large, including businesses and civil society organisations, to protect the digital rights of a vulnerable, unskilled population.

Stop surveillance activities in Romania! A civil society campaign

ICT policy experts from Romania¹⁵ have warned of the threats to privacy if data retention laws¹⁶ are adopted. After draft laws were published in April 2014, civil society organisations have closely monitored the legislative process and informed the public, taking positions against both the content and the policy-making process.

“Invading people’s privacy is like rape”

When commenting on the draft laws on data retention, the head of the ICT committee for the Romanian Chamber of Deputies put it bluntly: intruding into people’s computers without their consent is like rape.¹⁷

Civil society and its partners¹⁸ began to mobilise in June 2014 at the Coliberator conference,¹⁹ organised by the Ceata Foundation. On 7-8 June 2014, a follow-up to this digital rights conference called Coliberator took place in Bucharest, featuring topics like “Reimagining the Digital Revolution after Snowden”, “A Free Digital Society”, and “Surveillance, capabilities, social consequences and responses”. Conference participants published an online petition, asking the Romanian authorities to withdraw the draft laws on data retention. The petition, called “Stop surveillance activities in Romania!”, received 1786 signatures²⁰ from people with various backgrounds: digital rights activists like Richard Stallman (the president of the Free Software Foundation), Jillian York (director at Electronic Frontier Foundation), Bardhyl Jashari (Metamorphosis Foundation),²¹ mainstream media representatives, bloggers, software developers and students.

Targeted protests against the “Big brother law”

At the same time, the Association for Technology and Internet, the Association for Defence of Human Rights in Romania, the Helsinki Committee, ActiveWatch, the Centre for Independent Journalism, the Romanian Centre for Investigative Journalism, Geo-spatial.org and the Ceata Foundation launched a joint statement²² expressing their strong disapproval of Law 277/2014 on registering prepaid SIM cards and monitoring public Wi-Fi users. This law was passed in the Romanian Senate on 2 June 2014, with only one day allowed for amendments and comments. The signatory organisations highlighted the disproportionate and unclear character of the law:

- All free Wi-Fi users will need to be identified.
- All prepaid mobile phone users will have to be registered within six months after the law comes into force, otherwise their services will be deactivated.
- Users’ registration will be done under uncertain conditions, with no clear provisions on who will be accessing their personal data.

On 2 July 2014, the law was rushed through parliament by the Chamber of Deputies. It was the

1 Directive 2006/24/CE of the European Parliament.

2 O’Brien, D. (2014, April 8). Data Retention Directive invalid, says EU’s highest court. Electronic Frontier Foundation. <https://www.eff.org/deeplinks/2014/04/data-retention-violates-human-rights-says-eus-highest-court>

3 www.apti.ro/noutati-cybersecurity-si-prepay-cdep

4 legi-internet.ro/blogs/index.php/legea-pastrarii-datelor-de-trafic-a-fost-respinsa-de-senat

5 Nicolae Ceausescu, Romanian dictator (1965-1989) under the Communist regime (1949-1989)

6 coliberator.ro/petition

7 giswatch.org/en/country-report/civil-society-participation/romania

8 Autoritatea Nationala pentru Administrare si Reglementare in Comunicatii (ANCOM). (2014). *Piata serviciilor de comunicatii electronice din Romania. Raport de date statistice pentru perioada 1 iulie – 31 decembrie 2013*, p. 39.

9 <https://ec.europa.eu/digital-agenda/en/scoreboard/romania>

10 And partly due to low ICT skills.

11 Data available for 2012.

12 European Commission. (2014). *Measuring Digital Skills across the EU: EU wide indicators of Digital Competence*. ec.europa.eu/digital-agenda/en/news/measuring-digital-skills-across-eu-eu-wide-indicators-digital-competence

13 Helsper, E. J., Kalmus, V., Hasebrink, U., Sagvari, B., & de Haan, J. (2013). *Country Classification: Opportunities, risks, harm and parental mediation*. LSE, London: EU Kids Online.

14 Mascheroni, G., & Ólafsson, K. (2014). *Net Children Go Mobile: Risks and opportunities*. Second edition. Milan: Educatt, p.39. www.netchildrengomobile.eu/reports

15 apti.ro/pozitia-apti-comisia-ITC-prepay-securitate-cibernetica

16 Draft Law 263/2014 on cyber security, and Draft Law 277/2014 on registering prepaid mobile SIM cards and public Wi-Fi users (issued in April 2014 for public consultation).

17 www.avocatnet.ro/content/articles/id_37763/Boc-Boc-Cine-e-Nu-conteaza-da-mi-telefonul-sa-caut-in-el.html

18 Centre for Research in Applied Ethics, Friedrich Ebert Stiftung Office Romania, The Sponge Media Innovation Lab, Knight-Mozilla Open News, and Coalition for Open Data.

19 coliberator.ro/index.en.html

20 As of 7 July 2014

21 Macedonian member organisation of the Association for Progressive Communications.

22 www.apador.org/en/parlamentul-aproba-proiect-lege-cartele-prepay

Online petition appeal launched at the Coliberator conference on 8 June 2014

Stop surveillance activities in Romania!

Romania is currently undergoing rapid and major technological development, but we have to make sure the new technology respects users' rights. Under Ceaușescu, Romanians were forced to register all typewriters to the Militia. Today, the government wants all Romanians to register all pre-paid SIM cards and record all traffic going through free public WiFi hotspots.

Preamble

Just one month after the ECJ decision declaring the Data Retention Directive invalid, the Romanian Government made three decisions to continue and even extend mass surveillance by:

- ignoring the ECJ decision and keeping the law 82/2012 regarding the data retention to be enforced anyway.
- adopting, without any kind of public consultation, a law requiring registration of all prepaid sim card users (including forcing the current 12 million users to submit their personal data during the next 6 months or face disconnection). This is all the more egregious given that this is the 4th such attempt since 2011.
- planning to require providers of free public WiFi hotspots to identify their users.
- adopting, without any kind of public consultation, a new law giving agents of the state the power to examine data in any computer system whatsoever without a court order, including your computer, in order to "have access to the data being held".

The signatories, participants of Fundația Ceata's Coliberator conference, as well as other people and organizations supporting this protest, are demanding the Romanian government and the Romanian public institutions to respect the citizens' privacy rights.

Thus, the signatories:

1. Remind that privacy is a fundamental human right, and that it is central to the existence and survival of democratic societies. It is essential to human dignity and it reinforces other rights, such as freedom of expression and information, and freedom of association, and is recognised under international human rights law. Activities that restrict the right to privacy, including communications surveillance, can only be justified when they are prescribed by law, when they are necessary to achieve a legitimate aim, and when they are proportionate to the aim pursued. (International Principles on the Application of Human Rights to Communications Surveillance)
2. Demand the immediate rejection by Parliament and withdrawal by the Government of the above mentioned draft laws that are infringing the right of privacy of the Romanian citizens.
3. Ask for rapid annulment of the data retention law in order to respect the ECJ decision.
4. Underscore that any future action of the government that could affect the right of privacy or any other fundamental rights must be drafted and adopted only after meeting the transparency requirements made by Law 52/2003, with a full human rights impact assessment and with a mandatory opinion from the Romanian Data Protection Authority.

Note: English translation by the petition organisers.

SOURCE: <http://coliberator.ro/petition/>

fourth attempt to adopt a "Big Brother Law" in three years, all opposed by civil society organisations and industry – three times successfully.²³ On 3 July 2014, civil society organisations issued a statement highlighting the lack of real consultation during the legislative process, and asking that the Romanian Constitutional Court take note of the unconstitutional character of the law.²⁴ On 7 July 2014, nine Romanian civil society organisations issued a request to the presidency, asking it to notify the Constitutional Court on the unconstitutional character of the surveillance law.²⁵

Conclusions

Steady technological development has connected many Romanians to the global digital culture, but when it comes to skills, awareness and participation, there is a long way to go: 85% of the population has low or no digital skills, and 45% has never used the internet. Governmental machineries and interests are still dominating the public arena, but civil society organisations have strong capacity to channel energies and to protect vulnerable users' right to privacy. Romanian organisations were able to mobilise, and in one month 1786 signatures were gathered protesting against an abusive surveillance law.

Two draft laws were issued in April 2014: one on cyber security, with a pending status in July

2014, and the other on monitoring prepaid SIM card holders and public Wi-Fi users – the latter was pushed through the legislative apparatus in one month, from 2 June to 2 July 2014. The future remains uncertain: it is more likely that a top-down authoritative voice from the EU would be able to prevent Romanian authorities from invading citizens' privacy.

Ironically, while the ECJ has rejected the EU surveillance directive, Romanian authorities still adopted an abusive law that throws the country into a "digital cage".

Action steps

A multi-stakeholder approach to ICT issues, including digital rights, should be promoted and implemented at a national level in Romania. Civil society organisations should act as barometers of freedom and watchdogs of democracy by:

- Building stronger coalitions with local and international digital rights activists.
- Developing common platforms and strategies with businesses and international governmental organisations, such as EU organs.
- Initiating and implementing ICT educational programmes in order to raise the level of digital literacy in Romania.

²³ apti.ro/Ini%C5%A3iativ%C4%83-legislativ%C4%83-privind-%C3%AEnregistrarea-utilizatorilor-serviciilor-de-comunica%C5%A3ii-electronice-tip-Prepay

²⁴ apti.ro/solicitare-sesizare-CCR

²⁵ apti.ro/apel-catre-presedentie-impotriva-inregistrare-prepay

RUSSIA

Sliding downhill after Sochi



Human rights and electronic surveillance journalist
Oliver Poole

Introduction

They are the two most famous people in Russia: Vladimir Putin, the country's president, who publicly stated that the internet is a "CIA project",¹ and Edward Snowden, the US National Security Agency (NSA) whistleblower who sought asylum in Moscow. For months neither was known to have talked. Then, this April, they appeared in a television debate.² Speaking via video link, Snowden asked: "Does Russia intercept, store or analyse in any way the communications of millions of individuals?" Putin's answer was adamant. "We don't have a mass system for such interception," he said, "and according to our law it cannot exist."

Unfortunately for the country's internet users, there is a weight of evidence – much of it recently uncovered by researchers – that a mass system of interception does in fact exist and that Russia does have laws which enable it to exist. In Russia, as Snowden surely knew, the question increasingly is not which parts of the internet are being monitored by the state but which parts are not. It is why his new home is an unlikely refuge for a champion of communications privacy.

Policy and political background

The Soviet Union (USSR) had no qualms about surveillance. From its inception, the secret services pried into the private lives of its citizens. In the 1980s this resulted in the development of an automated nationwide communications interception service which could monitor the government-owned telecommunications services.

This did not stop with the USSR's collapse.³ The KGB's⁴ successor, the Federal Security Service

(FSB), remained committed to surveillance. The telecommunications sector was no longer owned by the state, but the Ministry of Communications stipulated that the newly privatised companies install a device that is believed to enable the FSB to listen to or record calls without the provider's knowledge. This was SORM (System of Operative-Investigative Measures). Its capabilities have since been increased, first under SORM-2 and then SORM-3. Described by one expert as "Prism on steroids",⁵ it is now an intercept programme that privacy campaigners maintain permits the FSB to monitor and collect traffic without the knowledge of internet service providers (ISPs) or their users.

The country's laws do contain prohibitions on mass surveillance and FSB officers are required to obtain a court order to access communications.⁶ Once a warrant has been obtained, however, it does not have to be shown to phone or internet providers, as is required in much of the West. Free speech activists have shown that the only person the FSB officer must show the court order to is his superior.⁷

Assume any electronic device can be exploited

Ahead of the Sochi Winter Olympics, the US State Department's Bureau of Diplomatic Security warned staff visiting the Games: "Assume any electronic device you take can be exploited. If you do not need the device do not take it."

Visitors were given a series of dos and don'ts to protect their privacy, according to those who have seen the document.⁸ It read like something from a John le Carré novel. "Essential devices should have all personal identifying information and sensitive files removed or 'sanitized'. Devices with wireless connection capabilities should have the Wi-Fi turned off at all times... Do not connect to local ISPs

at cafés, coffee shops, hotels, airports or other local venues... Change all your passwords before and after your trip... Be sure to remove the battery from your Smartphone when not in use."

On how the Russian state apparently gained such penetration, we primarily have two Russian investigative journalists – Andrei Soldatov and Irina Borogan – and the website they co-founded, Agentura.ru, to thank. For Sochi, the pair collated dozens of open source technical documents on the government procurement website Zakupki,⁹ cross-referenced with the public records of various oversight agencies, to show how telephone and Wi-Fi networks were being amended in the run-up to the Games.

The organisers of Sochi had trumpeted it as the most technologically accessible Games ever with free high-speed Wi-Fi access at all venues, and at media centres and hotels, as well as a 4G LTE¹⁰ network. Soldatov and Borogan detailed in "Surveillance at the Sochi Olympics 2014" how wireless encryption had apparently been disabled in this network so that, although communications remained encrypted against casual eavesdropping by hackers, they would not be for the FSB.¹¹ The pair furthermore produced documents showing Rostelecom, the national telecoms operator responsible for the 4G network, was installing deep packet inspection (DPI) devices.¹²

Soldatov and Borogan also revealed the existence of an FSB presentation on how SORM was being upgraded for the event.¹³ The existence of SORM is well known. Indeed Russian internet users never seem to have been under the illusion, as in the West pre-Snowden, that internet use was private.¹⁴ In every Russian town there are widely believed to be underground cables that connect the local FSB bureau with ISPs and telecom providers. Originally created by the KGB to monitor phone calls, from 1998 SORM could also access the internet.¹⁵ This incarnation of SORM enabled only a limited amount of data to be collected, however, not least because many intercepts were operated manually

by agents. According to Soldatov and Borogan, this is no longer the case. SORM's Sochi incarnation collects information from all forms of communication and provides long-term storage. Furthermore, they write, the introduction of the DPIs enables those sending and receiving specific packets of electronic information to be identified, and for the information in those packets to be filtered.

Since 2000 eight Russian agencies have access to intercepts: the Interior Ministry, the FSB, the Federal Protective Service, the Foreign Intelligence Service, Customs and Excise, the Federal Anti-drug Agency, the Federal Prisons Service and the Main Intelligence Directorate of the General Staff.¹⁶ Independent privacy watchdogs report that it is the ISPs who are required to cover the cost of installing the devices enabling traffic to be monitored, but they are denied access to the surveillance boxes so neither service providers nor their users know what is being collected or when. Those that resist face penalties:¹⁷ first a fine; then, if they do not comply, the possibility of their licence being revoked. A joint investigation by Agentura.ru, Citizen Lab and Privacy International found 16 such warnings to telecoms and internet providers in 2010. For 2011 they found 13. In 2012 the number had jumped to 30.¹⁸ The use of SORM also appears to be growing. Figures from the Russian Supreme Court showed a doubling of telephone communication intercepts between 2007 and 2012 from 265,937 to 539,864.¹⁹ These figures did not include counterintelligence conducted on Russian citizens and foreigners – and it was before Snowden's NSA revelations.

Keir Giles of Chatham House has argued that the Russian authorities have long approached the internet differently to the West.²⁰ Democratic societies traditionally see freedom of expression and individual liberties as core rights to be protected. But the Russian perspective is to dwell on national security dangers. Snowden's disclosures renewed belief in government circles that internet use in Russia must be more carefully controlled and free of foreign interference – and gave a fresh justification to those who already wanted it to be so.²¹

1 Al Jazeera. (2014, April 25). Putin says Internet is a CIA project. *Al Jazeera*. www.aljazeera.com/news/europe/2014/04/putin-says-internet-cia-project-201442563249711810.html

2 Mackey, R. (2014, April 17). Video of Snowden Asking Putin About Surveillance. *The New York Times*. thelede.blogs.nytimes.com/2014/04/17/video-of-snowden-asking-putin-about-surveillance/?_php=true&_type=blogs&_r=0

3 agentura.ru/english/projects/Project_ID/PIproject

4 Former Russian secret service.

5 Walker, S. (2013, October 6). Russia to monitor 'all communications' at Winter Olympics in Sochi. *The Guardian*. www.theguardian.com/world/2013/oct/06/russia-monitor-communications-sochi-winter-olympics

6 Federal Law No. 144-FZ on Operational - Search Activities (1995, last amended 2004). www.legislationline.org/documents/id/4191

7 Soldatov, A., & Borogan, I. (2013). Russia's Surveillance State. *World Policy Journal*, Fall. www.worldpolicy.org/journal/fall2013/Russia-surveillance

8 Ibid.

9 www.zakupki.gov.ru/epz/main/public/home.html

10 A standard for wireless communication of high-speed data for mobile phones.

11 www.agentura.ru/english/projects/Project_ID/sochi

12 zakupki.gov.ru/223/purchase/public/purchase/info/common-info.html?noticelid=507603&epz=true

13 infosystems.ru/assets/files/Sochi%202010/Kuzmin_RNT.pdf

14 Giles, K. (2013, October 29). After Snowden, Russia Steps Up Internet Surveillance. *Chatham House*. www.chathamhouse.org/media/comment/view/195173

15 Pincus, W. (2014, April 21). In questioning Russia's Putin about surveillance, Snowden misses the point. *The Washington Post*. www.washingtonpost.com/world/national-security/in-questioning-russias-putin-about-surveillance-snowden-misses-the-point/2014/04/21/c3e09352-c732-11e3-bf7a-be01a9b69cf1_story.html

16 Soldatov, A. (2012, October 11). Privacy International and Agentura.ru launch the joint project 'Russia's Surveillance State'. *Privacy International*. <https://www.privacyinternational.org/blog/privacy-international-and-agentura-launch-the-joint-project-russias-surveillance-state>

17 One such court decision can be seen here: msud106.krd.msudrf.ru/modules.php?name=info_pages&id=1002&cl=1

18 Soldatov, A., & Borogan, I. (2013). Op. cit.

19 Ibid.

20 www.conflictstudies.org.uk/publications.php

21 Ames, M. (2014, January 16). Edward Snowden demands press freedom (for journalists who don't live or work in Russia). *Pando Daily*. pando.com/2014/01/16/edward-snowden-demands-press-freedom-for-journalists-who-dont-live-or-work-in-russia/

In December the Russian Duma extended the so-called internet “black list” with a law allowing “extremist” websites to be blocked without court consent. The definition of “extremist” included the calling of unauthorised demonstrations. The Kremlin’s own Committee on Human Rights warned that this risked infringing the country’s constitution.²² However, three independent sites were blocked shortly afterwards, and more followed as the crisis escalated in Ukraine. Furthermore, to the concern of Reporters Without Borders and others, from August bloggers with more than 3,000 daily viewers will be placed under the same content restrictions as newspapers and television.²³ This means they will have to register with the authorities. A number of blogging sites are removing features showing visitor numbers as a result. In addition Lenta.Ru, a major online current affairs site, was effectively destroyed in March when its editor-in-chief and executive director were sacked, resulting in the resignation of its entire team of journalists.²⁴

Soldatov and Borogan have said that Russian businesses that rent space on servers in Russia are required under the stipulation of their licences to give access to the security services via SORM.²⁵ But platforms such as Facebook, Twitter and Google are not hosted in the country. Indeed Facebook and Twitter did not even have a formal representative entity there. This is a particular problem for anyone wishing to intercept their traffic, as social network sites are notoriously difficult to monitor due to being closed accounts and therefore resistant to semantic analysis.

Snowden’s revelations seemingly prompted renewed effort to bridge this knowledge gap. Legislation has been introduced to make website owners and operators (including Facebook, as the law states it includes foreign websites with Russian users) archive user data for six months and be willing to provide it to the government when requested.²⁶ Foreign internet companies are also being pressured to invest in local data storage facilities. In April, Maksim Ksenzov, the deputy director

of Roskomnadzor (the Agency for the Supervision of Information Technology, Communications and Mass Media), hinted that those who did not comply could be switched off.²⁷ Prime Minister Dmitry Medvedev sharply denied this was the case, calling on officials to “use their brains” before announcing the closure of social networking sites. However, Kommersant has published leaked documents that it claims show the government intends to prohibit any DNS²⁸ server outside of Russia from using the .ru or .rf domains.²⁹

It is not just international social media owners that are under pressure. Vkontakte is the country’s largest independent social media site – and a favourite of opposition activists after its founder, Pavel Durov, refused to close groups organising protest marches during the early 2012 protests. Durov initially resisted attempts by Vkontakte’s Kremlin-friendly shareholders, including Alisher Usmanov, to force him out.³⁰ This April, however, he left not only the company but the country. A few days earlier he wrote on his blog that the FSB had ordered him to provide personal data on the organisers of 39 groups on Vkontakte, allegedly linked to Ukraine’s Euromaidan movement.³¹

Explaining his departure, Durov warned it had become “harder and harder to remain with those principles on which our social network is based.” His statement ended with a quote from Douglas Adams’ comedy science fiction novel *The Hitchhiker’s Guide to the Galaxy*. Given Russia’s increasingly hypnagogic internet – officially free but in practice looking anything but – it was an aptly surreal choice. “So long,” he said, “and thanks for all the fish.”

Conclusion

Snowden seemingly acknowledged SORM’s invasive net when, after his exchange with Putin, he called on journalists to pressure the Russian president “for clarification as to how millions of individuals’ communications are not being intercepted, analyzed or stored, when at least on a technical level the [Russian] systems that are in place must do precisely that in order to function.”³² It is this

question – what the Russian state is doing with the interception network it appears to have spent millions of roubles creating – that is of such concern to privacy, security and human rights campaigners.

There is a public security cause for the central government to keep an eye on electronic communications. The extent of the Sochi programme, which also saw 5,500 video cameras installed and drones – some with thermal vision – deployed, was in part a reflection of the heightened terrorist threat from regional separatist groups. But the evidence indicates that this intercept programme is seemingly being extended far beyond such extremist groups.

The amount of data produced by Russia’s 75 million internet users is vast, and data capture, let alone storage, may well be beyond the capacity of many telecoms operators.³³ Soldatov has said that Russian technology for storing and intercepting communications is not as advanced as that used by the US.³⁴ Moreover, as InfoWatch head Natalia Kasperskaya has pointed out, Russia remains dependent on Western computer technology following the near collapse of the country’s own microelectronics industry in the 1990s.³⁵ Any attempt to “balkanise” the Russian web would only lead to poorer access, slower speeds and greater costs to the consumer.

Nevertheless, the policy trajectory appears clear. First the Kremlin targeted phones. Then it targeted emails and internet pages. Now there is an assault on social networks. A raft of lawful methods

now exist for the Russian state to collect information and block unwanted online content – while Soldatov and Borogan have detailed a range of extralegal approaches allegedly being adopted as well. Given such circumstances, the Bureau of Diplomatic Security’s warning ahead of Sochi appears not only prudent for its staff but for anyone wishing to protect their communications in modern-day Russia.

Action steps

The following advocacy steps can be recommended:

- Lobby national governments to encourage Russia not to suppress free expression online, to drop proposed restrictions on bloggers, and to end pressure on social networks and independent websites.
- Promote legal support for media organisations with limited financial capacities, including by creating collective legal tools.
- Create and disseminate best practice guidelines to promote protection on the internet.
- Conduct outreach programmes for the wider public to highlight the social and economic advantages of a free and open internet.
- Lobby the Russian government to adopt transparent civic discussions ahead of the adoption of new laws impacting on communications freedom.

22 Sugarman, E. (2014, March 27). Russia’s War on Internet Freedom Is Bad for Business and the Russian Economy. *Forbes*. www.forbes.com/sites/elisugarman/2014/03/27/russias-war-on-internet-freedom-is-bad-for-business-and-the-russian-economy/

23 Reporters Without Borders. (2014, April 18). Will the Russian internet soon be under complete control? *Reporters Without Borders*. en.rsf.org/russia-will-the-russian-internet-soon-be-18-04-2014,46167.html

24 Human Rights Watch. (2014, April 24). Russia: Veto law to restrict online freedom. *Human Rights Watch*. www.hrw.org/news/2014/04/24/russia-veto-law-restrict-online-freedom

25 Soldatov, A., & Borogan, I. (2013). Op. cit.

26 Sugarman, E. (2014, March 27). Op. cit.

27 Hille, K. (2014, May 16). Russian regulator threatens to block Twitter. *The Financial Times*. www.ft.com/cms/s/0/a3ea4946-dd06-11e3-b73c-00144feabdc0.html#axzz39plsMHbi

28 Domain name system.

29 www.kommersant.ru/doc/2462760

30 Walker, S. (2014, April 2). Founder of Vkontakte leaves after dispute with Kremlin-linked owners. *The Guardian*. www.theguardian.com/media/2014/apr/02/founder-pavel-durov-leaves-russian-social-network-site-vkontakte

31 Human Rights Watch. (2014, April 24). Op. cit.

32 Pincus, W. (2014, April 21). Op. cit.

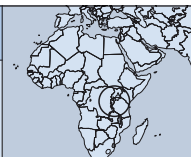
33 Giles, K. (2013, October 29). Op. cit.

34 Lake, E. (2014, April 18). Sorry, Snowden: Putin Lied to You About His Surveillance State – And Made You a Pawn of It. *The Daily Beast*. www.thedailybeast.com/articles/2014/04/17/sorry-snowden-putin-lied-to-you-about-his-surveillance-state-and-made-you-a-pawn-of-it.html

35 tvrain.ru/articles/natalja_kasperskaja_majkrosoft_pozhaleet_esli_podderzhit_sanktsii_v_otnoshenii_rossii-367814/

RWANDA

Ensuring security, or violating privacy and freedom?



Emmanuel Habumuremyi
www.giswatch.org/users/ehabumuremyi

Introduction

The rapid growth of information and communications technology (ICT) services in Rwanda has brought new policies, laws and strategies. These are aimed not only at alignment with established economic development and poverty reduction strategies, but also at ensuring that citizens and non-citizens enjoy full freedom, security and privacy. At the moment, the mobile phone penetration rate is estimated at over 65.4% when it comes to active SIM cards,¹ up from 53.1% in December 2012, and the internet penetration rate was approximately 22% in terms of mobile broadband subscriptions by June 2014.² The statistics are based on a population of 10,515,973 recorded in the 2012 national census.³ However, communications surveillance is not a common issue discussed publicly. The reasons are hypothetical, including a lack of awareness of why surveillance is necessary, what its advantages or disadvantages are for people's rights, and how it is done.

The focus of this report is to discuss existing measures to keep citizens' personal data safe from internal and external intruders, and to examine the reasons and conditions under which surveillance of communications is conducted, as well as who is authorised to do so. It explores the current Rwandan legal framework, government commitments in this area and the international community's views on how the government honours these commitments.

Policy and political background

As Rwandans are becoming active users of smart devices (like mobile phones, iPads and tablets), as well as consumers of social media and other online facilities, on the one hand people are discovering how ICTs are helping them to share their private information, store personal data and discuss

sensitive issues. On the other, they are finding out that if these communications are not well protected, they can be misused or abused by corporate entities, malicious people and public officials.

While writing on the rights to privacy in the digital age, the National Commission for Human Rights (NCHR) in Rwanda ascertained that measures have been taken at the national level to ensure respect for and protection of citizens' freedom and rights to privacy, including in the context of digital communications.⁴

The NCHR says that the first measures can be traced to the Constitution of the Republic of Rwanda,⁵ which guarantees the protection and respect of the right to privacy. Article 22 states that the private life, family, home or correspondence of a person shall not be subjected to arbitrary interference, and that a person's home is inviolable. Article 34 paragraph 2 states that freedom of speech and freedom of information shall not prejudice public order and good morals, the right of every citizen to honour and good reputation, and the privacy of personal and family life.

The most cited laws established to ensure the respect of the right to privacy and data protection in Rwanda are the following:

- Law No. 02/2013 of 8 February 2013 regulating media (article 9)⁶
- Law No. 03/2013 of 8 February 2013 regulating access to information (article 4)⁷
- Law No. 48/2008 of 9 September 2008 relating to the interception of communications⁸
- The recently enacted ICT law⁹

4 National Commission for Human Rights. (n/d). *The rights to privacy in the digital age*. www.ohchr.org/Documents/Issues/Privacy/RwandaNHR.pdf

5 www.parliament.gov.rw/fileadmin/Images2013/Rwandan_Constitution.pdf

6 www.mhc.gov.rw/fileadmin/templates/PdfDocuments/Laws/Official_Gazette_n_10_of_11_March_2013.pdf

7 www.mhc.gov.rw/fileadmin/templates/PdfDocuments/Laws/Official_Gazette_n_10_of_11_March_2013.pdf

8 lip.alfa-xp.com/lip/AmategekoDB.aspx?Mode=r&pid=7801&iid=2369

9 www.parliament.gov.rw/uploads/tx_publications/DRAFT_LAW_GOVERNING_INFORMATION_AND_COMMUNICATION_TECHNOLOGIES.pdf

1 www.rura.rw/fileadmin/docs/Montly_telecom_subscribers_telecom_subscribers_as_of_June.pdf

2 Republic of Rwanda. (2004). MYICT performance contract for FY 2014-2015, p. 4.

3 www.statistics.gov.rw

- Law No. 44/2001 of 30 November 2001 governing telecommunications¹⁰
- Law No. 18/2010 of 12 May 2010 relating to electronic messages, electronic signatures and electronic transactions (the e-signature law)¹¹
- Law No. 54/2011 of 14 December 2011 relating to the rights and the protection of the child (Article 16).

The government of Rwanda honours international commitments on internet governance. During the NETmundial internet governance discussions, at which Rwanda was represented by its Minister of Youth and ICT Jean Philbert Nsengimana,¹² the internet was taken as “a universal global resource, that should remain a secure, stable, resilient, and trustworthy network” and Rwanda supported the proposal of an internet governance framework which is “inclusive, multistakeholder, effective, legitimate, and evolving.”¹³

Rwanda ratified the International Covenant on Civil and Political Rights, and is therefore bound by Article 17, which states: “No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.”¹⁴

The above-mentioned regulations are applied domestically. According to Privacy International, the corporate sector plays a critical role in facilitating surveillance.¹⁵ Interception and monitoring of individuals' communications are becoming more widespread, more indiscriminate and more invasive, just as our reliance on electronic communications increases.¹⁶ This report does not have data on how big corporations' privacy policies, such as those of Google and Yahoo, among others, affect internet users in Rwanda. This is a matter for attention, since some of the spokespeople of these companies have been wilfully tone-deaf on the issue in the past: “If you have something that you don't want anyone to

10 www.rura.rw/fileadmin/laws/TelecomLaw.pdf

11 www.rwanda.eregulations.org/media/Electronic%20law.pdf

12 Kenyanito, E. P. (2014, May 9). What did Africa get out of NetMundial internet governance discussions? Access. https://www.accessnow.org/blog/2014/05/09/spotlight-on-african-contributions-to-internet-governance-discussions-part-

13 document.netmundial.br/1-internet-governance-principles

14 www.ohchr.org/en/professionalinterest/pages/ccpr.aspx

15 Nyst, C. (2014, July 17). UN privacy report a game-changer in fighting unlawful surveillance. *Privacy International*. https://www.privacyinternational.org/blog/un-privacy-report-a-game-changer-in-fighting-unlawful-surveillance

16 https://www.privacyinternational.org/issues/communications-surveillance

know, maybe you shouldn't be doing it in the first place.”¹⁷

Communications interception and collection of personal data vs international human rights principles

Rwanda, like many countries in the world, has put in place “measures to establish and maintain independent, effective domestic oversight mechanisms capable of ensuring transparency, as appropriate, and accountability for state surveillance of communication, its interception and collection of personal data.”¹⁸

A certain number of international human rights organisations and external journalist reports attack the government, at the level of ranking the country not free or partly free, citing the interception of communications among other factors they consider hindering freedom and privacy.

When the bill on the interception of communications was awaiting approval by the Rwandan Senate, sensational headlines in international newspaper reports and interpretations like “in the name of ‘public security’ Rwandan police and security forces will be able to spy on journalists, human rights defenders, lawyers and activists who criticise or oppose the Kagame regime” appeared.¹⁹

With today's global evolution driven by the advance of ICTs, the registration of identity information to activate a mobile SIM card is fast becoming universal in Africa. SIM registration and the collection of biometric data were among the most criticised projects when they were being implemented in Rwanda. They were considered by some as components of a growing surveillance assemblage that also incorporates other technologies such as electronic passport systems, new video surveillance technologies, and electronic health systems.²⁰

SIM registration

2013 was characterised by a campaign encouraging all citizens of Rwanda to begin registering their SIM cards, an activity started in February and ending in July the same year. According to

17 Taylor, A. (2014, June 16). Google and Yahoo want to ‘reset the net’. But can it work? *The Guardian*. www.theguardian.com/commentisfree/2014/jun/16/google-yahoo-reset-the-net-tech-nsa-data-collection

18 National Commission for Human Rights. (n/d). Op. cit.

19 Nyst, C. (2012, August 25). Rwandan government expands stranglehold on privacy and free expression. *Privacy International*. https://www.privacyinternational.org/blog/rwandan-government-expands-stranglehold-on-privacy-and-free-expression

20 Donovan, K. P., & Martin, A. K. (2014, February 3). The rise of African SIM registration. *First Monday*. firstmonday.org/ojs/index.php/fm/article/view/4351/3820

the then-director general of the Rwanda Utilities and Regulatory Authority (RURA), the exercise was due to “East African Community (EAC) resolutions where all countries agreed to implement the SIM card registration (SCR), which is related to the security of mobile subscribers – such as fighting mobile-based crimes – in the region.”²¹ This was confirmed by some researchers such as Nicola Jentzsch, who affirms that the East African Communications Organization (EACO) has been a major proponent of SIM registration, encouraging national governments in the region to adopt relevant laws and regulations, or to support voluntary initiatives. She went on to mention EACO’s motivation: the belief that forcing customers to register SIM cards will reduce the opportunities for malevolent actors to use mobile devices anonymously to undertake unlawful or socially harmful activities, including kidnapping, drug trafficking and terrorism.²²

East African countries like Kenya, Rwanda, Uganda and South Sudan are working towards establishing a cross-border SIM card registration framework in a new effort to curb the rise in crimes perpetrated through the use of mobile devices.²³

Biometric identity

A biometric system for the identification of citizens stores all the resources needed to identify a person, based on their digitised fingerprints and photographs.

In Rwanda, the National Identification Agency (NIDA) has opted for ICT-based initiatives to speed up citizen registration. Under the motto “Smart ID, Smart Ideas”, Rwanda has built a population register to issue secure national identity cards, driving permits and integrated smartcards that will be multi-purpose to enhance quick public services delivery.²⁴ Services that come with the card include personal identification, insurance assessments, and bank and immigration services, among others. This avoids the need to carry many cards to access the different services.

Since January 2014, citizens from three partner states (Rwanda, Kenya and Uganda) have begun to use the smartcard to cross their respective

borders without presenting any passport or pass.²⁵ The interconnected national ID system is meant to facilitate the faster movement of people between the three countries, and at the same time to ensure that people moving from one country to another do not fake their nationalities and identities.

Arguments against the establishment of biometric data collection state that studies of national ID card programmes have consistently found that certain ethnic groups are disproportionately targeted for ID checks by the police. Privacy International goes further by pointing to the genocide against Tutsis in 1994, when ID cards designating their holders as Tutsis cost thousands of people their lives. For them, an ID card enables disparate identifying information about a person that is stored in different databases to be easily linked and analysed through data-mining techniques. This creates significant privacy vulnerability, especially given the fact that governments usually outsource the administration of ID programmes to unaccountable private companies.²⁶

Following the success of the national ID programme, Rwandan government stakeholders are optimistic about the potential success of this initiative. Many stakeholders believe that the Rwandan smartcard initiative will enhance their quality of service delivery while reducing lengthy turnaround time.²⁷

Interception of communications

In August 2013, the Rwandan government passed amendments to a 2008 law relating to the interception of communications. While reading most media articles criticising the law, laypeople in the field lose track of what it is and what it is not, when it is lawful and when it is unlawful, and who is authorised to intercept communications.

The law defines communications interception as “any act of listening, recording, storing, decrypting, intercepting, interfering with, or carrying out any other type of surveillance over voice or data communications without the knowledge of the user and without explicit permission to do so.”²⁸

Relevant authorities are authorised to carry out interception of communications for national security purposes.²⁹ According to the law, this is done on a criminal suspect: “[W]hen all other procedures of obtaining evidence to establish truth have failed, the prosecutor in charge of investigations, may, after obtaining a written authorisation by the Prosecutor General of the Republic, listen, acknowledge and intercept record[ed] communications, conversations, telegrams, postal cards, telecommunications and other ways of communicating.”³⁰

The law governing telecommunications, meanwhile, recognises privacy and data protection, and forbids interception of communications in its Article 54. It states: “Every user’s voice or data communications carried by means of a telecommunications network or telecommunications service, remains confidential to that user and the user’s intended recipient of that voice or data communications.” If a court authorises the interception or recording of communications in the interests of national security and the prevention, investigation, detection and prosecution of criminal offences, the above article is not applied.

Government authorities of “the relevant security organs” are authorised to apply for an interception warrant. In May 2014, the government appointed the Ombudsman and Deputy Ombudsman as a team of inspectors in charge of monitoring that interception of communication which is done in accordance with the law.³¹ No person shall reveal any information which he/she accessed in the exercise of his/her responsibilities or duties in relation to this order, except when authorised by the head of the security organ which has carried out the interception (Article 8).³²

The following acts are not considered as interception of communications:

- Evidence of a crime collected after the message reached the receiver.
- Evidence based on communication recorded by the sender or the receiver or other person without using a monitoring device for interception of communications.³³

Conclusion

As is becoming the practice in most democratic countries, in Rwanda intercepts of oral, telephonic and digital communications are initiated by law enforcement or intelligence agencies only after approval by a judge, and only during the investigation of serious crimes.

Arguments against communication interception, based on asserting that the reasons advanced for interception are weak, seem to be on the extreme side when a developing country is involved. In the absence of clear case studies and unbiased opinions that consider both the pros and cons of communications surveillance, the public is not able to know how surveillance can make a safer society as proposed by governments, or how it can deteriorate their rights as argued by human rights activists.

With SIM registration, your email, ID and phone are linked together. The requirement by big corporations to provide a telephone number when using their services, for instance, is also dangerous and promotes unnecessary personal data surveillance, since users are not aware who is accessing their data and what the data is being used for.

Action steps

Apart from the existing laws in place, the Rwandan government should consider the following when it comes to communications surveillance:

- The government needs to sensitise Rwandan citizens through awareness campaigns on procedures, practices and legislation regarding the surveillance of communications. This should be done in order to increase their knowledge on matters related to surveillance on the one hand, and to help them use communication channels responsibly on the other hand.
- Telecommunications and internet service providers should increase the quality of what they offer to the clients, since poor service that requires citizens to seek help from a customer care desk is likely to expose the clients’ privacy.
- Rwandan civil society and human rights organisations should be in a position to understand well what is involved in communications surveillance in order to avoid relying on speculative information.

21 Bright, E. (2013, February 4). SIM card registration gets under way. *The Rwanda Focus*. focus.rw/wp/2013/02/sim-card-registration-gets-under-way/

22 Donovan, K. P., & Martin, A. K. (2014, February 3). Op. cit.

23 Wokabi, C. (2013, December 23). East African states to share SIM card, national ID data. *Pan African Visions*. panafrikanvisions.com/2013/east-african-states-share-sim-card-national-id-data

24 www.worldbank.org/content/dam/Worldbank/Event/social-protection/Building_Robust_Identification_Systems_Session_Packet.pdf

25 IWACU. (2014, January 14). ID cards to replace passports in EAC. *IWACU English News*. www.iwacu-burundi.org/blogs/english/id-cards-to-replace-passports-in-eac/

26 https://www.privacyinternational.org/issues/id

27 Sivan, S. K. (n/d). *Enhancing public and private sector delivery through Rwandan national smart card initiative*. www.appropriatetech.net/files/ENHANCING_PUBLIC_AND_PRIVATE_SECTOR_DELIVERY.pdf

28 Law relating to the interception of communications.

29 Ibid.

30 Law N° 13/2004 relating to the Code of Criminal Procedure. www.refworld.org/docid/46c306492.html

31 2014 Presidential Order appointing inspectors in charge of monitoring the interception of communication.

32 2014 Prime Minister’s Order determining modalities for the enforcement of the law regulating interception of communication.

33 Ibid.



JONCTION

Ababacar Diop
www.jonctions.org

Introduction

Senegal, located in West Africa, is a country formerly colonised by France which gained its independence in 1960. It currently has a population of roughly 13 million people.

The advent of the Senegalese digital society in the late 1990s and its exponential development since the 2000s has led policy makers to set up an institutional and legal framework for digital activity with the adoption in 2008 of a series of laws governing the internet in the country.¹ Policy makers found this necessary for reasons of national security, and to establish a legal and institutional framework to protect citizens against crimes related to online activity.

ICTs have brought real changes in the forms of communication and exchange, not only at the corporate level, but also in the relationships between citizens. However, even if it is proven that ICTs are great tools at the service of freedom of speech, they also constitute a real danger when it comes to the privacy of correspondence.

The Senegalese media continue to reveal scandals about citizens' communications being monitored either by the government or by private companies.² This will be the subject of our discussion, which attempts to analyse the institutional and legal architecture of communications surveillance in Senegal.

Political context

Senegal has signed and acceded to several international and regional human rights instruments, including the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, the International Covenant on

Economic, Social and Cultural Rights, and the African Charter on Human and Peoples' Rights.

The Universal Declaration of Human Rights states in Article 12: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks." The same UN text provides in Article 19: "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers."³

In addition, Article 17 of the International Covenant on Civil and Political Rights states: "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation."⁴

In compliance with Senegal's international commitments, its constitution states in Article 13: "The secrecy of correspondence and of postal, telegraphic, telephonic and electronic communications shall be inviolable. This inviolability shall be subject only to such restrictions as are made applicable by law."⁵

"Noticing echoes..."

Senegal, like many countries in the world – as demonstrated by the revelations of Edward Snowden – is threatened by the practice of illegal surveillance of communications. This practice, which does not meet international standards prescribed by the relevant United Nations texts, including the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights, is a real threat to privacy, freedom of expression and the right to confidentiality of communications.

Revelations made by the Senegalese press about the tapping of citizens' telephone conversations, but also the monitoring of communications of employees in a telecommunication company, illustrate this.

According to an article in the newspaper *Le Pays*, published on 5 September 2011 and posted on the OSIRIS website: "It is common: we often notice echoes in the middle of a call, unusual noise, interrupted conversations without apparent reason and even noise ... of mechanical tools. This implies that wiretaps are being made. To pierce the mystery surrounding the ongoing wiretapping that Senegalese are subject to, there could be no more appropriate source than a mobile phone company."⁶ Moreover, the same newspaper reports in its edition on 30 November 2011: "Wiretaps were organised internally by the top management and have practically turned the lives of the workers upside down, reveal anonymous Tigo agents. Senior employees were unpleasantly surprised to receive sanctions and other requests for explanations, based on the content of messages sent by email."⁷

If these claims are true, they show infringements on the communications of Senegalese citizens by both the government and private companies. This constitutes a real threat to the enjoyment of fundamental human rights which our country has committed to respect.

According to Article 13 of the Senegalese constitution, as noted above, the secrecy of correspondence and communications is inviolable, and this inviolability is "subject only to such restrictions as are made applicable by law."

Even if there is no specific legislation on phone tapping, there are several laws and regulations protecting the confidentiality of correspondence and other communications. These include Law 2008-12 on the Protection of Personal Data, Law 2011-01 of 24 February 2011 on the Telecommunications Code, and the decree on electronic communications made for the purposes of Law 2008-08 of 25 January 2008 on Electronic Transactions.⁸

According to Article 7 of the Telecommunications Code: "The operators of telecommunications networks open to the public and suppliers of public telecommunications services, as well as their staff members, are sworn to secrecy of correspondence and continuity of the service under penalty of prosecution pursuant to Article 167 of the Penal Code. They must also ensure that consumers and users have optimal network conditions that guarantee confidentiality and

neutrality of the service with respect to transmitted messages and the protection of privacy and personal data... There can be no exception to this rule unless under the conditions prescribed by law."⁹

Article 12 of the Telecommunications Code provides that "[a] judge or police officer, for the needs of the prosecution or an investigation, or the enforcement of a judicial ruling, may require that telecommunications operators and service providers or telecommunications networks make available useful information stored in the computer systems they administer. Telecommunications operators and service providers of telecommunications networks are required to submit the required information to the authorities."¹⁰ In other words, only a judge or police officer is authorised by law to order a restriction on the inviolability of private communications. This seems to be, for us, consistent with the principle of legality as well as that of the competent judicial authority provided by the 13 International Principles on the Application of Human Rights to Communications Surveillance.¹¹ According to the principle of legality, "Any limitation to the right to privacy must be prescribed by law. The State must not adopt or implement a measure that interferes with the right to privacy in the absence of an existing publicly available legislative act."

However, the law should be more precise to comply with the principle of adequacy, by specifying the extent and limits of an order by a judge or police officer under Article 12 of the Telecommunications Code. According to the principle of adequacy as established in the abovementioned 13 International Principles, "Any instance of communications surveillance authorised by law must be appropriate to fulfil the specific legitimate aim identified." For us, it seems to be necessary that the judge or police officer declare the legitimate aim pursued by the order, which has the advantage of avoiding any abuse by the authorities.

In light of this, there is no doubt that the incidents reported above are unfairly and severely violating the integrity of the communications of citizens, because they do not have any legal grounds. Beyond that, they are a breach of citizens' rights to privacy and freedom of expression as enshrined in the Senegalese legal system.

It is undisputed that, for security requirements, the state may conduct surveillance of communications. But monitoring the communications or correspondence of citizens outside of legal channels is an intrusive act against privacy and personal data protection, and stands against human dignity.

¹ www.jonctions.org/index.php?option=com_content&view=article&id=16&Itemid=62

² Enquête+. (2013, July 29). Les enregistrements téléphoniques comme moyens de preuves : "Illégaux" et "irrecevables", selon des juristes. Enquête+. www.enqueteplus.com/content/les-enregistrements-t%C3%A9l%C3%A9phoniques-comme-moyens-de-preuves-ill%C3%A9gaux-et-irrecevables-selon-des

³ www.un.org/en/documents/udhr/index.shtml#1a12

⁴ www.ohchr.org/en/professionalinterest/pages/ccpr.aspx

⁵ www.wipo.int/wipolex/en/details.jsp?id=6223

⁶ Diagne, E. (2011, September 5). Surveillance des communications téléphoniques : Pourquoi et comment l'État écoute les citoyens. OSIRIS. osiris.sn/Surveillance-des-communications.html

⁷ Seck, A. A. (2011, November 30). Tigo et le scandale des écoutes téléphoniques. Senenews.com. www.senenews.com/2011/11/30/tigo-et-le-scandale-des-ecoutes-telephoniques_17135.html

⁸ www.jonctions.org/index.php?option=com_content&view=article&id=16&Itemid=62

⁹ www.gouv.sn/IMG/pdf/code_des_Telecom_2011_senegal.pdf

¹⁰ Ibid.

¹¹ <https://en.necessaryandproportionate.org/text>

It is even more serious if illegal surveillance of employee communications is the work of private companies. The case of the telecommunications company cited earlier, illegally “spying” on its employees by monitoring their electronic correspondence and telephone communications, reveals serious issues when it comes to human rights and fundamental freedoms within the company. These rights are at the heart of corporate social responsibility.

In addition to the monitoring by the state and companies, citizens monitor each other. Often scandals involve people illegally recording the private conversations of others using mobile phones. These recordings not only infringe on privacy, but are sometimes used to attack the dignity of others.¹²

This is why the government – but also citizens – should proactively protect the right to privacy of correspondence, not only to be compliant with international standards of human rights, but also to ensure the safety and the social and democratic stability of our country.

Conclusion

The rapid growth of ICT use raises the issue of the security of communications and electronic exchanges. This is not only a technical issue but also a societal one. What are actually being threatened are the foundations of the rule of law and a democratic society, which are the aspiration of African countries, including our country, Senegal.

However, given the recent situation prevailing in Nigeria, with attacks and kidnappings carried out by Boko Haram, one can legitimately ask whether it is not useful to better monitor communications to effectively fight against terrorism. Our answer is no, because the fight against terrorism should not justify the restriction of fundamental freedoms and widespread infringement on the privacy of citizens. The phenomenon of mass surveillance is a serious danger which civil society organisations and human rights activists have to face.

In this regard, in order to counter the threats to privacy, security and civil liberties, African states face challenges in putting in place appropriate institutional and legal mechanisms to enforce the right to privacy of correspondence. Fraudulent and illegal surveillance of communications in Senegal is a reality and the government, as guarantor of civil

liberties, should find solutions. It is an absolute imperative of social and democratic stability, as well as of institutional and citizen security.

Although efforts are being made at the legislative and institutional level to respect the privacy of correspondence, the government must make an effort to protect citizens’ internet rights from the threat of evolving surveillance technologies. With the rapid development of sophisticated technology, it becomes possible for private entities or individuals to violate the privacy of communications with the simple aim of harming others. When a telecommunications company is authorised to spy on the correspondence and communications of its own employees, this deserves special attention. It is the same when a citizen is equipped with sophisticated technological means to intercept or record callers without their knowledge, and for a non-lawful use.

While the dynamism of the ICT sector is progressing at an accelerated pace in our country, tools for recording and monitoring communications are becoming increasingly sophisticated and are often out of the government’s control. Therefore it is necessary to implement appropriate legislation. The current legislation protecting the confidentiality of correspondence, freedom of expression and privacy does not, as we have seen, take care of all the issues and challenges of mass surveillance of communications.

Action steps

To better ensure the integrity of the digital space, privacy rights, and secrecy of correspondence, we recommend some actions that are absolutely necessary:

- Citizens should be constantly aware of surveillance practices in order to ensure respect of the right to privacy and protection of personal data and to defend against all unjustified and unlawful acts of communications monitoring.
- We recommend that the government further strengthen the legal and institutional framework for communications monitoring from the standpoint of respect for human rights. Also, the government should develop technical and human resources in order to have the ability to exercise appropriate controls on unauthorised wiretapping and communications surveillance technologies installed in Senegal, to ensure security and the public’s civil liberties.
- The government must ensure that any regulations on communications surveillance conform to the 13 International Principles on the Application of Human Rights to Communications Surveillance.

SERBIA

Access to retained data



SHARE Foundation/SHARE Defense

Milos Stojkovic and Djordje Krivokapic
www.shareconference.net/en/defense

Introduction

During 2012, Rodoljub Sabic, the Commissioner for Information of Public Importance and Personal Data Protection (CIIPD), oversaw the implementation and enforcement of laws on the protection of personal data and electronic communications. His work involved investigating four telecommunications operators: Orion Telekom, Telenor, VIP Mobile and Telekom Serbia. This related *inter alia* to the legality of the Ministry of Interior (MUP) and secret services accessing user telecommunications data that had been stored by the operators.

On 6 July 2012 the CIIPD publicly released findings showing that the national authorities had unauthorised, direct access to retained data (metadata) using the previous regulatory framework that allowed them to establish technical links with the systems used by telecommunications operators. The current legal framework requires that authorities submit an official request to the operator, together with a court order. The data released from one operator showed that the relevant authorities submitted only 3,600 official requests for access to retained data from 27 March 2011 until 27 March 2012. On the other hand, in the same period, the authorities approached one operator (Telenor) over 270,000 times. The number of unauthorised access requests is 130 times higher than official requests.

Policy and political background

The legal framework regulating surveillance in Serbia is outdated and imprecise. In addition, some provisions of the relevant laws have been declared unconstitutional. Constitutional safeguards regarding the protection of privacy are very strong. Article 41, Paragraph 2 of the Constitution of the Republic of Serbia prescribes that any restriction on the privacy of communication is only possible temporarily, and is only allowed on the basis of a court decision – if it is necessary for investigating a crime or for the protection of the national security of the country in line with the law.

However, most of the laws regulating access to retained data have been contrary to the safeguards provided by the constitution, and most provisions of these laws have been challenged and repealed in constitutional court proceedings. In addition, in practice, constitutional safeguards are often violated by various authorities and secret services. Although pressure from civil society and independent institutions is strong, there has been no progress in the reform of the legal framework and no changes in the way that secret services operate.

Regulatory cul-de-sac gives security agents free access to databases

As noted above, the CIIPD supervision over telecom operators revealed that the MUP and secret services have direct access to retained data, and that the access takes place in a manner which is contrary to the constitutional safeguards regarding the privacy of communications. It all started in 2008, when the Republic Agency for Electronic Communications (RATEL) prescribed technical conditions for operators that also determined their obligation to state bodies authorised for electronic surveillance. Technical conditions were adopted according to the provisions of the Law on Telecommunications, which was abolished in 2010 when the new Law on Electronic Communications was enacted. The technical conditions were related to telephony, internet and cable distribution operators, and they were the “legal basis” for establishing the technical link between state authorities and operators. These links enabled state authorities to access retained communications data without any control, and without any evidence that such access is legally based (in accordance with the mentioned constitutional safeguards).

In July 2010, the new Law on Electronic Communications, in line with the European Framework for Electronic Communications 2003, was adopted by the National Assembly. In the public debate over the draft of the law, the CIIPD and Protector of Citizens (PC) argued that some of the provisions of the law are contrary to the constitutional safeguards regarding the privacy of communications. The provisions in question were related to accessing

¹² Nettali.net. (2010, November 23). Affaire Diombasse Diaw : Khadija Mbaye et ses complices prennent 6 mois, Abdou Aziz Diop relaxé. Xalimasn. xalimasn.com/affaire-diombasse-diaw-khadija-mbaye-et-ses-complices-prennent-6-mois-abdou-aziz-diop-relaxe (In this case, the defendants were charged with, among others, acts of cyber crime. The victim was filmed without his knowledge by a supposed friend while he was naked and the footage was then found on the internet.)

retained data. The draft prescribed that accessing retained data is “possible for the purpose of conducting investigations, crime detection and criminal proceedings, in accordance with the law regulating criminal proceedings, as well as for the purpose of protecting national and public security of the Republic of Serbia, according to the law which governs the operation of security services of the Republic of Serbia and the operation of the authorities in charge of internal affairs.” Other laws contained problematic provisions that gave the secret services access to retained data even without a court order in exceptional cases.

After the adoption of the Law on Electronic Communications, both independent institutions (the CIIPD and the PC) launched separate proceedings before the Constitutional Court. The result was that controversial provisions from the Law on Electronic Communications, the Law on the Military Security Agency and Military Intelligence Agency, as well as the Law on Criminal Proceedings, were repealed. The decision of the Constitutional Court meant that access to retained data is possible only on the basis of a court order. For example, before the decision of the Constitutional Court, the Law on Criminal Proceedings prescribed that the police are authorised to obtain telephonic listing data and data regarding the usage of a base station, as well as data on location of a communication, simply upon the order of the Public Prosecutor. After the Constitutional Court decision, the provision was changed in a way that obtaining this data is possible only upon the order of an authorised court (a court dealing with the initial proceedings of a case).

However, without provisions prescribing the manner and conditions of access on the technical level, and with existing technical links to telecommunications operators, there was still a high risk of unauthorised access. Unfortunately, data released by the CIIPD showed that unauthorised access is common practice among the secret services and other state bodies. Over 270,000 unauthorised data requests for just one operator showed that constitutional safeguards and even legal provisions are not respected. The only basis for direct access is RATEL’s technical conditions, which could not be in force, because they are bylaws adopted according to the Law on Telecommunications that ceased to exist. Somehow it is still applicable because new technical conditions have not been adopted. It is obvious that such a regulatory cul-de-sac creates a situation in which state authorities can access and use the retained data without any control.

After its findings concerning telecommunications operators, on 4 November 2013 the CIIPD began to investigate internet operators. The supervision is still ongoing, but there is a high level of certainty that similar or even worse results will be revealed regarding the protection of privacy.

Conclusions

The findings of the CIIPD showed that there is a huge gap between constitutional safeguards and practice. Unauthorised access by state bodies implies that there is no appropriate balance between the legitimate interests of protection of privacy on one side, and investigating crimes and protection of security on the other. The privacy of communication, among other human rights, can be restricted. However, there are standards that should be fulfilled. Any restriction has to be prescribed by the law and must be necessary to protect vital interests of society (e.g. national security). There also has to be proportionality in the imposed restriction and the goal which the restriction intends to achieve, and any restrictions should be the least intrusive on the free exercise of human rights (principle of proportionality). Unfortunately, these conditions are not fulfilled at the moment, and it is clear that something has to be changed.

The current state of affairs is not satisfactory, because there is wide scope for interfering with telecom users, regardless of the type of communications technology they use. As long as state bodies have opportunities to access large amounts of data without any restrictions, such as data about the location of telecommunications devices, and data regarding the destination, or duration of communications, users will be in constant fear that their “everyday” life is monitored by government. The protection of state security is undoubtedly in the interests of every society, but the manner of protection must be in line with human rights standards. This implies the oversight and involvement of as many stakeholders as possible, from state bodies to independent institutions and NGOs dealing with human rights.

Action steps

In order to improve the privacy of communications, the legal framework should be completely in line with constitutional safeguards. That means that laws which regulate access to retained data should be changed in a manner which provides clear and unambiguous rules about who is authorised to access the data, what their obligations are, and what safeguards exist when it comes to the misuse of

data. Second, civil society, state authorities and independent bodies have to initiate a public debate on all aspects of the work of secret services and other state bodies, including their access to retained data. Finally, state bodies which are authorised to access retained data have to adapt so that their

work conforms to the principles of transparency, civil control and accountability. Only through such an approach is it possible to achieve mutual understanding between various stakeholders, and only then will it be possible to achieve the appropriate balance between privacy and security.

SLOVAK REPUBLIC

The quest for privacy in Slovakia: The case of data retention



European Information Society Institute (EISI)

Martin Husovec and Lubomir Lukic
www.eisionline.org

Introduction

Shortly after a series of coordinated suicide attacks in Madrid in 2004 and central London in 2005, the European Union reacted by passing the so-called Data Retention Directive in 2006. The directive obliged all EU member states to implement laws forcing telecommunications providers to monitor and store a wide range of metadata concerning the online and phone activities of their citizens for periods ranging from several months to years. The hope was that this data could help Europe to better fight terrorism and other serious crimes. Strong protests by citizens in some of the member states could not stop the scale of this imposed surveillance.

In September 2010, when the European Information Society Institute (EISI) was formed in the Slovak Republic (also known as Slovakia), the fight against surveillance in other member states had already been going on for several years. The German Constitutional Court in March of that year suspended Germany's implementation of the directive and many other national initiatives began appearing. Encouraged by the efforts and fruits of the labour of our colleagues, EISI decided to make litigation against data retention in Slovakia its first goal. There was, at the time, no civil society organisation to do the job in the country; there was virtually no public debate and very little, if any, public resistance against data retention.

Policy and political background

After the Data Retention Directive was implemented at the national level throughout the EU, the resulting legislation was subject to numerous challenges at the national level.¹ However, it took almost a decade to challenge the source of all of this: the directive itself. In April 2014, the Court of Justice of the EU (CJEU) – in its historical role as a constitutional court for the Union – repealed the

entire Data Retention Directive² and also broadly quashed any future hopes for similarly far-reaching measures. This, however, did not exhaust the advocacy role for civil society groups. Today, there is a great need to sweep clean numerous post-directive consequences. In Slovakia, this entails the review of the Act on Electronic Communications and some other acts.

This report outlines the struggle of launching a challenge against the implementation of the directive in Slovakia. It presents a picture of non-responsive local authorities, a lack of public awareness and little resistance to an invasion of privacy rights among Slovak civil society and ultimately citizens. It also illustrates a misuse of retained data and the real practice of disclosure, which is often distant from the letter of the law.

Challenging the implications of the Data Retention Directive at the local level

Soon after its launch, EISI authored a brief report pointing out the basic discrepancies between the Act on Electronic Communications ("the Act") and its data retention provisions, and the fundamental rights embodied in the Slovak constitution, the EU Charter of Fundamental Rights and Freedoms, and the Convention for the Protection of Human Rights and Fundamental Freedoms. This report was then presented in the form of a motion³ to two local authorities, which were entitled to initiate proceedings before the Constitutional Court. These authorities were the General Prosecutor's Office and the Ombudsman.

Both of the local authorities, despite the evidence, reached the view that the data retention provisions do not lead to an interference with the fundamental rights and freedoms of citizens. And so they refused to initiate any proceedings before the Constitutional Court, which could review the constitutionality of the provisions of the Act.

When easier ways of initiating proceedings before the Constitutional Court were exhausted, EISI

had to try more complicated and resource-intensive ways. We put together a submission for the Constitutional Court⁴ and started asking for the support of members of parliament, who can also initiate such a constitutional review. The required number of signatures is relatively high – at least each fifth member of parliament needs to sign such a submission (a total of 30 MPs).

It probably does not need to be stressed too much that this requirement slowed down the process. Because EISI has no regular staff members, but only volunteers, it took a few years to both draft the submission and get the necessary support for it. And had the work on the submission not been supported by the research of one of its members, it could have taken even longer than that.

The ultimate aim of the submission, which was later presented to MPs, was to succinctly point out conflicts between the data retention provisions and fundamental rights and freedoms. The submission described the overall situation, the fundamental features of which are presented below.

According to the Act, an undertaking⁵ is obliged to retain traffic data, location data and data of the parties who communicated. The data retention period was set to six months in the case of internet access, email and voice over internet protocol (VoIP), and 12 months in the case of other types of communications. The scope of the retained data is very broad. It can probably be best divided into the following categories: i) data necessary to trace and identify the source of a communication; ii) data needed to identify the recipient of communication or to identify the date, time and duration of communication and iii) data needed to identify the type of communication, the users' end equipment (or what seems to be their equipment) and the location of mobile devices.

In the opinion of EISI, the introduction of these obligations constituted a substantial encroachment upon the private life of individuals – especially because this mandated a blanket monitoring of all inhabitants of Slovakia, regardless of their innocence or prior behaviour. The data retention requirements mandated that every day the data about every inhabitant of Slovakia must be collected, amassing a profile of who called whom, to whom someone sent an SMS or email, when the

person sent it, from which location, using what type of device or service, how long the communication took, and many other details. It is needless to say that the combination of this information made it possible to perfectly describe the movement of every inhabitant of Slovakia who uses a mobile phone or the internet. In this way, the behaviour, circle of acquaintances, hobbies, health, sexuality and other personal secrets of all the citizens can be predicted.

It therefore comes as no surprise that EISI considered the legislation to be entirely disproportionate and lacking any safeguards against the misuse of the sensitive data. The legislation created a regulatory free space which increasingly minimised citizens' privacy. Moreover, the main duties and details of data retention regulation were left to private companies, which are naturally more interested in minimising their costs, since the state did not reimburse them for the cost of this obligation.

The submission argued that in the light of the application of the proportionality test, the data retention legislation turns out to be clearly unconstitutional. It also argued that the retention of metadata can in a concrete way result in even more intrusive interference with the right to privacy than a scenario in which the content of the communication itself is retained.

Moreover, the legislation, in contrast with other legal requirements for criminal proceedings, did not exempt persons who are otherwise bound by professional secrecy (e.g. lawyers, doctors), or who cannot be surveilled or wiretapped when they perform certain activities (e.g. relationships between advocate and accused).

EISI argued that the national provisions on data retention were therefore in direct conflict with the principle that the restriction of fundamental rights and freedoms has to comply with their essence and meaning. The restrictions can only be implemented when there is a clear, stated aim. It is a violation of provisions if the state restricts fundamental rights and freedoms in a way that both lacks an achievable goal and, especially, threatens the very essence of those freedoms.

We furthermore believed that blanket data retention is unconstitutional for several reasons, and that the Data Retention Directive itself is invalid because of this. First of all, data retention is not a sufficiently effective tool to combat serious crime: it affects ordinary people more than the perpetrators of serious crimes. Therefore it disproportionately infringes on the right to privacy and the right to protection of personal data. It also disproportionately

1 Jones, C., & Hayes, B. (2013). *The EU Data Retention Directive: a case study in the legitimacy and effectiveness of EU counter-terrorism policy*. secile.eu/data-retention-in-europe-case-study

2 Digital Rights Ireland C-293/12 and Kärntner Landesregierung C-594/12.

3 www.eisionline.org/index.php/projekty-m/ochrana-sukromia/22-podanie-generalna-prokuratura

4 www.eisionline.org/index.php/projekty-m/ochrana-sukromia/28-vzorove-podanie-na-ustavny-sud-sr-vo-veci-plosneho-sledovania-obcanov

5 For the purposes of the Act on Electronic Communications, "undertaking" means every person who provides a network or service; undertaking activity means a network or a service provision in the electronic communications sector for a third party.

restricts freedom of expression and media freedom. Moreover, the length and extent of retained data was prescribed without the support of any empirical research.

EISi also argued that many provisions of both the Data Retention Directive and the Act are vague and provide too much room for abuse by both public authorities and the private sector. The real-life practice of Slovak service providers retaining and storing data was found to be entirely arbitrary, because often the data retention was not required by law and/or data was provided to authorities who have no legal right to request them. So both the scope of retention and scope of access often exceeded the law.

Access to stored data is not regulated by any precise legislation. This enables law enforcement authorities to take advantage of a messy legal situation and request data for less serious crimes. This is constitutionally incompatible with human rights such as the right to privacy and freedom of expression. EISi presented evidence which illustrated a real misuse of data when it comes to disclosures. It was established that the practice is often very distant from what the letter of the law says. This is especially the case given that there is very little supervision from the public authorities responsible for this.

The submission asked the Constitutional Court to file for a preliminary reference before the CJEU arguing that the Data Retention Directive itself is invalid.

After several months of negotiations with members of parliament, the required number of signatures was reached to support our initiative. Finally, after six months, EISi managed to get the submission before the Constitutional Court. At this point, however, it had already been three years since we had started the initiative.

In October 2012, the submission⁶ demanding a review of the data retention provisions embodied in the Act was officially submitted to the Constitutional Court.⁷ Shortly after the submission was filed, a preliminary submission concerning the constitutionality of the Data Protection Directive was filed before the CJEU. The referring Austrian and Irish courts made a reference similar to the one EISi proposed for the Slovak Constitutional Court in the proceedings before it. Due to the inactivity of the Slovak Constitutional Court, it soon became clear that the Court had decided to wait for the decision

of the CJEU first. In April 2014, the CJEU annulled the Data Protection Directive.⁸

Conclusions

By repealing the Data Retention Directive, the CJEU not only invalidated a single act of the Union's secondary law, but also defined the scope of their discretion. Slovak transposing acts, which are at the moment under the scrutiny of the Slovak Constitutional Court, were thus not only deprived of the reason for transposition, but are now also in a direct contradiction with the explicit standard set by the CJEU in Digital Rights Ireland C-293/12 and C-594/12.

According to the decision of the CJEU, any kind of blanket data retention that does not distinguish between persons who can be connected to major criminal activity and other persons, does not conform with the rights to privacy and protection of personal data.

In terms of future legislation:

- Any kind of metadata retention must (i) be aimed at specific persons or circle of persons, and (ii) have a specific time period and/or (iii) geographical area.
- Access to data must be restricted to investigating acts of a serious nature that can justify the significant interference with fundamental human rights such as the respect of private and family life and protection of personal data.
- Access to data must be subject to judicial supervision or the supervision of an independent administrative body which can allow such access based only on a substantiated application to the courts.
- Data retention must reflect the special status of persons bound by a duty of confidentiality conferred by national law, such as attorneys or doctors.
- When grounds for data detention are not relevant anymore, the particular person must be notified of the fact that he/she was under surveillance in the past.
- The period and types of retained data in a specific case must be adapted to what is necessary for achieving a particular aim.
- The data retention must provide clear safeguards against possible misuse or unauthorised access to this data.

- Legal regulations must clearly describe how the data can be stored and how the data will be destroyed after it is used.
- Any kind of access and subsequent use of meta-data must fall within a clearly defined scope and be for a clearly defined aim.

On 23 April 2014, the Slovak Constitutional Court preliminarily suspended the national implementing Act. This measure means that the retention laws are still formally in place, but have no legal effect until the Court decides on the merits of the complaint. However, at the same time, data that has already been collected will not need to be destroyed, and it remains open to interpretation whether service providers may or may not hand over data collected in the past to state authorities upon request.

On the other hand, the Slovak Parliament came up with a proposal to amend the Penal Procedure Code, which is one of the acts regulating the access to this type of information. The proposal fails to live up to the standard set by the CJEU. Yet no civil society organisation, and very few in the mainstream media, picked up on the topic. This creates little pressure on legislators. It appears that even after the landmark decision of the CJEU and our efforts, sensitivity to privacy rights is still rather low in Slovakia. Even less significant copyright developments enjoy better coverage in the media and garner more public interest than most privacy-related issues.

Action steps

Slovakia still lacks a strong privacy advocacy group. EISi, as a think tank focusing more on litigation, is not well suited to fulfil this role. Our example shows that the presence of expertise and litigation coming from civil society does not necessarily improve social sensitiveness to the issues among the general public. Slovakia needs, in our view, the following:

- A strong privacy activist group needs to be established.
- The work of the Slovak Data Protection Authority needs to be improved. Currently, it is not only failing to act *ex officio*, but also in cases when data is requested by the authorities, and its work is marked by a lack of expertise.
- The opportunity for civil society to object to legislation before the Constitutional Court, even without political support, needs to be legislated in Slovakia. When the general public is not sensitive to certain issues, neither are the public authorities.

All this will be important after the decision by the Constitutional Court is made, when the debate will again be shifted to the national parliament. In the absence of broader interest by civil society, the strength of the pro-privacy opposition will remain very small and we will witness a race to the bottom.

6 PL. ÚS 10/2014

7 www.eisionline.org/index.php/projekty-m/ochrana-sukromia/49-slovak-case-on-data-retention

8 www.eisionline.org/index.php/projekty-m/ochrana-sukromia/74-us-data-retention-suspension

SOUTH AFRICA

Communications surveillance in South Africa:
The case of the Sunday Times newspaper



Department of Journalism, Film and Television,
University of Johannesburg
Jane Duncan
www.uj.ac.za

Introduction

This article discusses the communications surveillance of two investigative journalists from the biggest weekend newspaper in South Africa, the *Sunday Times*. The paper is owned by one of the four largest press groups, Times Media Limited. The journalists, Stephan Hofstätter and Mzilikazi wa Afrika, had their communications intercepted by the Crime Intelligence Division of the South African Police Service (SAPS), in order to disrupt their work as journalists and uncover their sources. This story has been chosen as a case study of just how corruptible South Africa's communications monitoring and interception capacities are, in spite of the government claiming that it offers all the necessary protections for civil liberties.

The revelations by former National Security Agency (NSA) contractor Edward Snowden – that the NSA was conducting mass surveillance of US citizens, as well as political leaders such as German Chancellor Angela Merkel – have created a serious international controversy. Other countries have also been exposed as conducting mass surveillance too, and many people in South African civil society and the media have been concerned that the country's authorities may be doing the same. This report examines one case where clear proof emerged of abuses, and what the case tells us about the state of civil liberties in relation to communications networks.

Policy and political background

South Africa is not a terrorist target, yet growing social protests mean that the temptation is there for less principled members of the security apparatus to abuse the state's surveillance capabilities to advantage the faction currently in control of the ruling African National Congress (ANC) and disadvantage their perceived detractors. South Africa has some excellent investigative journalism teams, and the state could easily misuse its surveillance

capabilities to harass them and expose their confidential sources of information, especially if they threaten ruling interests.

South Africa has a law that governs the surveillance of domestic communications on both criminal justice and national security matters, the Regulation of Interception of Communications and Provision of Communications Related Information Act (RICA). RICA forbids the interception of communications without the permission of a designated judge, and sets out the conditions for the granting of interception directions. According to the Act, interception directions should be granted only if there are reasonable grounds to believe that a criminal offence has been or is being or probably will be committed.¹ The Act also requires all South Africans to register their subscriber information management (SIM) cards with their mobile phone providers, so that the state can track the activities of suspected criminals or victims if they need to.²

In spite of the fact that RICA attempted to strike the correct balance between the interests of justice and national security on the one hand, and civil liberties on the other, the Act has insufficient guarantees for civil liberties online. It ignores many of the most basic protections set out in the recently released Application of Human Rights Principles to Communications Surveillance, otherwise known as the Necessary and Proportionate Principles.³

An added problem is that foreign signals intelligence gathering does not fall under RICA, which means that this practice is unregulated by law. This is particularly worrying as the state's bulk monitoring capacity is held by the interception centre that undertakes foreign signals intelligence; so the state agency with the greatest capacity for mass surveillance is also the one that is least regulated by law.

In 2005, the state's mass surveillance capacity was misused to spy on perceived opponents of the then contender for the presidency, Jacob Zuma. Several politicians and activists have also alleged

that their communications are being surveilled, although it is difficult to say whether this is the case. Another weekly newspaper, the *Mail & Guardian*, has quoted sources inside the police and State Security Agency (SSA) alleging that security personnel often do not even bother obtaining directions to intercept communications.⁴ These incidents and allegations arise from the fact that there are systemic weaknesses in the country's communications surveillance regime, which predispose it to abuse.

The Sunday Times case

Hofstätter and wa Afrika are part of an award-winning investigative journalism team at the *Sunday Times*. They have been responsible for some of the most important stories exposing government corruption and malfeasance, and as a result have earned the ire of some government officials who would prefer to keep their dark secrets just that.

The journalists were responsible for a story that saw South Africa's top cop, National Police Commissioner Bheki Cele, being fired by the president in 2012 for dishonesty, unlawfulness and mismanagement in concluding a lease deal for offices for SAPS in the capital city of Pretoria and in Durban. The deal was concluded with businessman Roux Shabangu, who was close to President Jacob Zuma. Their stories exposed how Cele had broken treasury rules to advantage an associate of Zuma's financially.

The team also investigated allegations of corruption against Cele when he was the member of the executive council (MEC) responsible for transport, safety and security in the KwaZulu-Natal province of South Africa. Moreover, they published damning exposés of the serious and violent crimes unit of SAPS in the township of Cato Manor, which they claimed turned rogue by operating a "death squad" and killing suspects. The police members alleged to have been involved still have to stand trial.

As they deal with extremely sensitive stories, Hofstätter and wa Afrika must do their utmost to protect their sources, including those located inside the police. In an attempt to do just that, they carry two phones: one with a SIM card that has been registered in terms of RICA and one with a card that has been registered by someone other than themselves. "Pre-RICA'd" SIM cards – SIM cards that are registered before they are bought – can be bought fairly easily in South Africa, and cannot be traced back to their users as they are not registered in their names. They use the first for non-sensitive communications

and the second for sensitive communications with confidential sources, assuming that communications using pre-RICA'd SIM cards will be impossible to trace back to their sources.

Wa Afrika had a sinister run-in with the authorities in 2010, when his communications were intercepted by the police on the pretext that he was suspected of gun running. The journalist had travelled in and out of the country several times on stories, and the police used this as "evidence" that he may well have been involved in crime. The existence of the interception direction was confirmed by the Inspector General of Intelligence, who also confirmed that the direction was lawful.⁵ The vague and speculative grounds for the issuing of interception directions worked to the police's advantage, and they used this to pursue an investigation of a non-existent crime.

However, according to Hofstätter and wa Afrika, later in 2010, the police managed to obtain their pre-RICA'd numbers, and slipped them into a larger application for an interception direction for the designated judge, Joshua Khumalo, to approve. The police claimed that the numbers were of suspected members of a criminal syndicate, and the journalists' numbers were included under fictitious names. Oddly enough, the Police Commissioner's number was also included in the application, although Cele's number was subsequently cancelled.

Apparently the police obtained these numbers from one of their sources, who had decided to betray the journalists in return for a promotion.⁶ The journalists learned these details from other sources. The bugging of their phones was confirmed by a Pietermaritzburg magistrate, who stated that the KwaZulu-Natal provincial crime intelligence chief had sent him as an emissary to apologise for the bugging. However, the chief has refused to be drawn into a discussion with the journalists directly.⁷

The *Sunday Times* has taken this case to court, and two officers are being charged with having violated RICA. The sanctions for having done so are stiff: any person intercepting communications unlawfully could be imprisoned for up to 10 years or fined up to ZAR 2 million (approximately USD 200,000). The journalists claim that they have not been involved in any crimes, and as a result there is no valid reason for the police to investigate them.⁸

1 Section 5(a)(i), Regulation of Interception of Communications and Provision of Communications-Related Information Act, www.justice.gov.za/legislation/acts/2002-070.pdf

2 Section 39, Regulation of Interception of Communications and Provision of Communications-Related Information Act. www.justice.gov.za/legislation/acts/2002-070.pdf

3 en.necessaryandproportionate.org/text

4 Swart, H. (2011, October 14). Secret state: How the government spies on you. *Mail & Guardian*. mg.co.za/article/2011-10-14-secret-state

5 Discussion with Stephan Hofstätter and Mzilikazi wa Afrika, Rosebank, 20 March 2014.

6 Discussion with Stephan Hofstätter and Mzilikazi wa Afrika, Rosebank, 20 March 2014.

7 Affidavit by Stephan Hofstätter, 24 March 2012.

8 Affidavit by Stephan Hofstätter, 24 March 2012.

The only reason why they were placed under surveillance must be that they were being harassed for their investigations into the police, and that the police wanted to uncover their sources so that they could plug the leaks. In fact, in an affidavit for the case, one of the police officers on trial, Brian Padayachee, stated that he was given an instruction by a higher-ranking officer to undertake a covert investigation into the activities of certain journalists that, it was claimed, posed a threat to the organisation. This investigation included the interception and monitoring of their calls.⁹ Apparently, the ultimate instruction came from Cele, who was concerned that the journalists were attempting to infiltrate the police with an intention of tarnishing the image of the police; but, in a bizarre twist, this very direction that he had given the instruction for was used against him to place him under surveillance.

These incidents showed just how easy it is to intercept journalists' communications, or indeed the communications of any citizen who asks inconvenient questions about those in authority. There has been growing evidence of South Africa's security cluster – consisting of the police, the intelligence services and the military – becoming increasingly powerful and unaccountable. Unless the state's surveillance capacities are regulated properly, then abuses for political reasons are likely to continue. As Hofstätter noted, "...there is a complete free-for-all for the intelligence services to intercept whatever they want. They just come up with spurious grounds. There is a time-honoured practice to circumvent RICA, and all they do is just slip the numbers in."¹⁰

Analysis and conclusion

The *Sunday Times* case reveals several systemic weaknesses in the regulation of communications interception in South Africa. One of the most serious weaknesses is that no one is even informed that their communications have been intercepted, even after the investigation is complete. This means that the authorities are given a power that is, to all intents and purposes, hidden from the public eye. This violates the requirement in the Necessary and Proportionate Principles that individuals should be notified of a decision authorising communications surveillance with enough time and information to enable them to appeal the decision, and should have access to the materials presented in support

of the application for authorisation.¹¹ Needless to say, this principle should apply only if there is no risk to the purpose of surveillance, in which case *post facto* notification is appropriate.

In the United States' system, in order to protect the rights of the people under surveillance in criminal matters, within 90 days of the termination of the court order the judge must ensure that the person whose communications were intercepted is informed about the order.¹² The fact that a similar provision does not exist in RICA lays it wide open to abuse, as the authorities can rest assured that their abuses will most probably never come to light. The only reason why the *Sunday Times* learned of the abuse was because they have extensive contacts within the police; sources of information that would generally not be available to ordinary citizens.¹³

Another problem this case highlights is the speculative nature of the grounds for issuing interception directions using RICA. Privacy International has argued that the grounds are too vague, and that the higher standard of "probable cause" or a similar level of finding is generally required for a judge to issue an interception direction.¹⁴ Directions may also be issued in relation to serious offences that may be committed in future, which may not be constitutional as it allows law enforcement officers to speculate on future acts that have not yet occurred.¹⁵

Furthermore, the granting of directions is an inherently one-sided process, which means that the judge has to take the information that is given to him on trust. No ombudsman is present to represent users' interests; as a result, the process lacks an adversarial component, which also predisposes it to abuse.

The level of information provided by the designated judge that is eventually released is inadequate. The annual report provides bare details about the number of applications for interception directions, the state agency that made the applications and the number that were granted or refused.

The judge may also include some general comments on trends. No information is available in these reports on the number of interceptions that actually result in arrests and convictions. For instance, insufficient information was provided to understand why there was a huge 231% increase in the number of interception directions granted by the designated judge to Crime Intelligence between 2009 and 2010, the year that Hofstätter and wa Afrika's communications were intercepted.¹⁶

Furthermore, other democracies have established independent commissions to oversee all monitoring and interception activities. Such commissions undertake full and public reporting processes, with the most sensitive areas being removed. Yet in South Africa, the parliamentary reports are written by the very judge who took the decisions, which is not healthy as the judge is unlikely to reflect adequately on the weaknesses of his or her own decisions.

South Africa's Act also does not recognise the right of journalists to protect their sources of information, either in the form of express provisions in the Act or in the form of a protocol that law enforcement or intelligence officials are required to adhere to in investigating journalists.

All these problems make for an Act that is not human rights-compliant, and is likely to continue being abused unless safeguards are introduced.

Action steps

In 2014, the Department of State Security will launch a review of intelligence policy, to assess the strengths and weaknesses of all national security-related policies. The Department of Communications has also launched a review of ICT policy and legislation. Civil society needs to present researched alternatives to the existing communications surveillance regimes that enhance respect for basic rights and freedoms. Particular emphasis should be placed on ensuring that the regime conforms to the Necessary and Proportionate Principles and that these principles are domesticated in South African surveillance policy and practice.

These advocacy efforts should focus particularly on the following areas:

- Strengthening the grounds for the issuing of interception directions in RICA.
- Increasing transparency in reporting levels on communications surveillance practices.
- Ensuring that a user-notification provision is inserted into RICA.
- Ensuring independent oversight over the process of issuing interception directions.
- Implementing a protocol with respect to the surveillance of journalists' communications, setting out the circumstances in which such interceptions can take place, and the procedures.
- Including a provision in RICA for an ombudsman to represent users and the public interest when applications for interception directions are made.

⁹ Affidavit by Brian Padayachee, 14 March 2012.

¹⁰ Discussion with Stephan Hofstätter and Mzilikazi wa Afrika, Rosebank, 20 March 2014.

¹¹ International Principles on the Application of Human Rights to Communications Surveillance. en.necessaryandproportionate.org/text

¹² US Code § 2518 - Procedure for interception of wire, oral, or electronic communications. www.law.cornell.edu/uscode/text/18/2518

¹³ Discussion with Stephan Hofstätter and Mzilikazi wa Afrika, Rosebank, 20 May 2014.

¹⁴ Privacy International. (2001). Submission to the Parliamentary Committee on Justice and Constitutional Development, 14 August.

¹⁵ Bawa, N. (2006). The Regulation of Interception of Communications and Provision of Communications Related Information Act. In L. Thornton, Y. Carrim, P. Mthaulana, & P. Reburn (Eds.), *Telecommunications Law in South Africa*. www.wits.ac.za/academic/clm/link/publications/22988/telecommunications_law_in_south_africa.html

¹⁶ Khumalo, J. A. M. (2010). Statistical briefing by designated judge for the period 1 April 2009 to 31 April 2010, p. 3-4.

SUDAN

Systematic violations of digital rights



Liemia Eljaili Abubkr
lemiakatib.katib.org

Introduction

Since 1989 Sudan has been ruled by the National Congress Party (NCP), which came to power through a military coup, supported by militant Islamists. In relation to freedom of expression and the media, the current regime, policies and laws are undemocratic, contradicting Sudan's constitution, which respects freedom of expression and opinion.¹ The telecommunications sector in Sudan is regulated by the National Telecommunication Corporation (NTC).

In 2007, Sudan enacted the IT Crime Act, which does not guarantee free speech and criminalises the establishment of websites that criticise the government.² The Act provides for fines and prison sentences of between two and five years. In 2008 Sudan established its first Attorney General for Cyber Crimes.

In response to the Arab Spring in different neighbouring countries, Sudan imposed further restrictions on freedom of expression and the media. It also imported advanced technologies and equipment to censor and filter internet communications. The National Intelligence Security Services (NISS) set up a special internet filtering unit called the "Cyber Jihad Unit" to conduct "online defence operations".

This report will discuss the effect of limiting the internet and censorship on activists and human rights defenders during last year's September-October demonstrations against fuel subsidies, the challenges they faced and how to learn from these experiences to develop their capacity and work.

Policy and political background

In 2007 the NTC set up a special unit to censor and filter internet content before it reaches users inside Sudan. According to its policy, the unit filters content that is "morally offensive and violates public ethics" and "forestalls evil in the society".³ In practice this unit censors and filters the opposition's websites, including social media and email communications. In 2011 the NISS imported a remote control system (RCS) to manipulate information and to spy on government opposition, journalists, human rights activists and different youth groups.

In December 2012, a media law was proposed and discussed by the information committee in the national assembly. The new draft imposes more restrictions on media and freedom of expression, and includes provisions to regulate online media.⁴

While the government spent a lot of money on raising the capacity of its staff and imported advanced equipment for surveillance, human rights defenders, journalists and activists lack opportunities for proper training. They also do not have access to specialised ICTs and new media tools because of a United States digital technology sanction against the country, which was imposed on Sudan in 1997. Sudanese cannot buy original software, nor access training or courses online. This situation exposes civil society to serious security threats.

No privacy, no protection

"While I was filming a boy was shot and fell dead right in front of me, around two metres away. I was in a state of shock. I started screaming and I continued filming. I had documented the entire killing of the boy. The officers then approached me and snatched my phone." This is the testimony of Dr. Samar Mirghani to the local and international media, after her detention and her experience while witnessing protests in her neighbourhood. Mirghani, a pharmacist and social media activist, was detained, harassed and tortured by security forces in September 2013. This was after she was pressured by security forces

to provide the password to her mobile phone. She refused to do so, and they beat her and opened a case against her. She was charged with the crime of public disturbance.⁵ Mirghani's case illustrates the tough and hostile environment in which social media activists operate, the difficulties they face, and the impact of government restrictions on their work. Social media activists face gross violations of their right to privacy, detention, ill treatment, sexual harassment and extralegal intimidation. Mirghani documented the killing of a boy on her mobile. Unfortunately, instead of using the video as evidence against the perpetrator, she has been fined and accused of public disturbance.

During demonstrations and political or economic crisis, the NISS places extra-restrictive measures on the media, targeting journalists (whether local or international correspondents), social media activists and human rights defenders. In Sudan, during the mass protests known as the "September Revolts", which broke out on 25 September 2013, the authorities responded with excessive force, including the use of live ammunition against protesters by security forces. The people were demonstrating against the government's decision to lift fuel subsidies. More than 177 people were killed and more than 800 were detained. Many well-known political activists and human rights defenders were arrested in their homes in an apparent attempt to stop them from documenting violations and to curb future mobilisation efforts.⁶

Bloggers and activists played an effective role in documenting human rights violations during the protests. They mobilised using the internet – emails, websites, social media and blogs – in the preparation and organisation of demonstrations, and shared news, photos and videos. They succeeded in informing the world about the excessive force used against protesters, which was condemned by the international community. Digital media activism enabled the protest to spread from its starting point in Khartoum and Wed Madni to other cities and urban areas around the country.

The restrictions on freedom of expression and the media in Sudan present serious challenges to the protection and promotion of human rights, the rule of law and democracy. The NISS used to visit newspapers daily to read the content before allowing them to print, and confiscated the papers

supporting independent and opposition parties after they had been printed. More than 20 topics were considered "red line", meaning the media were not allowed to write about them. These included issues to do with price increases, demonstrations, and the conflict in Darfur, South Kordofan and Blue Nile. In order to suppress the media to prevent coverage of human rights violations during the demonstrations, the NISS summoned the editors of the main newspapers to its headquarters and forbid them to publish any information about the protests that did not come from government sources.⁷

Many progressive and independent journalists published actively using new media during the demonstrations, in order to disseminate news and articles which they could not publish in local newspapers. Some newspapers published censored material on their websites, blogs or Facebook pages. Informal journalist groups and youth groups used their websites and Facebook pages to publish reports and news about government violations of human rights and freedom of expression. These included Journalists for Human Rights (JHR), the Sudanese Journalists' Network, Change Now, Abyana and Grifna. At the same time, the security forces used social media to spread false information about activists, protests and gathering places for protests, to mislead the protesters and activists.

The NISS also used social media to spread false information about the situation in Darfur, and about opposition party leaders, rebels and human rights defenders, sometimes accusing them of committing crimes against the state or immoral behaviour. They organised these activities through the Cyber Jihad Unit, using advanced technology and equipment. The government, since 1995, had allocated more than 70% of its budget to defence and security activities. Part of this money was used in importing advanced technology and in training the technical officers of the unit.

The Citizen Lab reports that Sudan, is one of 21 governments that are currently using or have used Hacking Team's RCS spyware.⁸ According to Reporters Without Borders, "The NSA [National Security Agency in the United States] and GCHQ [Government Communications Headquarters in the United Kingdom], Ethiopia's Information Network Security Agency, Saudi Arabia's Internet Services Unit, Belarus' Operations and Analysis Centre, Russia's FSB [Federal Security Service] and Sudan's National

1 Article (39) of the national interim Constitution 2005 provides that "[e]very citizen shall have unrestricted right to the freedom of expression, reception and dissemination of information, and access to the press without prejudice to order safety or public moral as determined by law - the state shall guarantee the freedom of press and other media shall be regulated by law in a democratic society".

2 Freedom House. (2013). *Freedom on the Net 2013*. www.freedomhouse.org/report/freedom-net/2013/sudan#.Uz28gVlPLcf2

3 National Telecommunication Corporation, Internet Information Filtering (Blocking Unit). www.ntc.gov.sd/index.php/en

4 A member of the Sudanese National Council revealed in an interview with the Doha Centre for Media Freedom in April 2013 that the new law would include regulations on online media.

5 sudanspeaks.blogspot.fr/2013_10_01_archive.html; see also Copnall, J. (2013, November 14). Sudan feels the heat from fuel protests. BBC News. www.bbc.com/news/world-africa-24938224

6 ACJPS. (2013, October 4). Over 170 dead, including 15 children, and 800 detained as demonstrations spread throughout Sudan. African Centre for Justice and Peace Studies. www.acjps.org/?p=1663

7 Among others, the newspapers *Al-Midan* and *Al-Jareeda*.

8 Marczak, B., Guarnieri, C., Marquis-Boire, M., & Scott-Railton, J. (2014, February 17). Mapping Hacking Team's "Untraceable" Spyware. *The Citizen Lab*. https://citizenlab.org/2014/02/mapping-hacking-teams-untraceable-spyware

Intelligence and Security Service are all security agencies that have gone far beyond their core duties by censoring or spying on journalists and other information providers.”⁹

Using its advanced technology and equipment on 25 September 2013, the NISS disconnected the internet throughout the country for more than 24 hours. Then, on the following days, the internet slowed down drastically.¹⁰ The international monitoring group Access wrote an open letter to telecom service providers in Sudan on 11 October asking about the internet blackout, which states: “We write with serious concerns over reports of the disruption of Sudan’s international internet connectivity on September 25 and 26 [when] a substantial portion of the country’s networks became unreachable, effectively removing Sudan from the broader Internet at the height of protests in Khartoum. This shutdown occurred on all major data providers (...) and appears to have been the result of actions taken by the service providers.”¹¹

During the internet blackout, many reported that even SMS messages were blocked. And services such as tweeting via SMS were interrupted by the sole telecommunications provider that carries this service, Zain.¹² The authorities had done the same in June 2012. According to Reporters Without Borders (RSF), at that time there was an eight-hour internet blackout during a gathering organised by the Umma Party¹³ that attracted thousands of people. During these protests, the internet slowed down drastically on the night of 29 June, before a large protest was announced.¹⁴ Sudanese news websites such as *Sudanese Online*, *Hurriyat* and *Al-Rakoba* were shut down and YouTube was blocked several times.

The opposition parties accused the NISS of spying and filtering opposition leaders’ phone calls, Twitter accounts, Facebook pages and emails. According to *Elterieg*, a Sudanese online news site, the NISS established special filtering units in each of the telecommunications companies in Sudan. These units are totally controlled by the NISS.¹⁵

The website mentioned that the NISS asked the communications companies to save SMS and online communications data for five years, instead of two years in the past.

Despite this hostile environment, the blocking of websites and the imposition of restrictions on different types of media, Sudanese activists and human rights defenders succeeded in organising, mobilising the people, cooperating and communicating with the international community, and reporting on most of the violations that occurred during demonstrations. They used proxy programmes such as Tor and Hotspot Shield to open blocked websites and developed their digital skills to find secure ways to upload their images, videos, news and articles.

Social media activists developed different measures to protect themselves in case of detention. They informed close relatives or friends about their Facebook and email passwords so that they could change them or delete the accounts in case of detention. These applications and platforms could expose them to torture or ill treatment by security forces during detention. Other activists had more than one Facebook page with different accounts in order to confuse the authorities.

On 27 May 2014 the NTC announced that it was conducting technical studies on social networking sites, particularly Facebook and WhatsApp, in a bid to find ways to control their use in the country. Many observers believe that this is an attempt to prevent the leaking of information on government corruption relating to senior figures.¹⁶ By taking these measures, the government can easily block citizens from online information and communication with the international community. This will free the NISS’s hand to torture and harass journalists, online activists and human rights defenders without fear of punishment or the condemnation of the international community.

On 19 May 2014 the minister of communications, in a report submitted to parliament, showed the difficulty in controlling Facebook and WhatsApp. The report explained that the Ministry of Culture and Information in Khartoum state is seeking to block Facebook and WhatsApp sites using advanced and sophisticated equipment, adding that the government will continue its strategy and policy to control and suppress social media using different tools. Their aim is to legalise the blackout of social media and other websites. The government is trying to convince the Sudanese that they are doing this to

protect the community from the negative impact of social media, and content which goes against traditions and religious beliefs.

In 2012 the Sudanese authorities proposed a new media law, which seeks to control social media and online activities. The proposed law gives authorities the power to ban journalists from writing, and to censor newspapers and internet content.

The NISS Act (2010) gives security officers power to spy, to intercept the communications of any citizen without judicial permission, and to track them in real time. The act gives the NISS immunity from prosecution.

Conclusions

The crackdown against internet freedom and grave violations of privacy rights pose a serious security situation for human rights defenders and online media activists. Because of mass surveillance, most of them are subject to detention, torture and ill treatment by NISS officers. At the same time there is no legislation protecting human rights and privacy rights. Most journalists, social media activists and human rights defenders lack awareness of protection and digital security and have limited knowledge of ways to stay digitally safe. To improve the situation there is a genuine need to reform the current legislation to be in line with human rights standards and the country’s constitution. There is also a need to raise the capacity of human rights defenders, journalists and social media activists when it comes to online protection and digital security.

According to Reporters Without Borders, Sudan scores high in censorship – it is considered one of the 2014 “Enemies of the Internet”. Most of the information about freedom of expression and human rights defenders is researched and published by international organisations such as Reporters Without Borders, Human Rights Watch, Freedom House and Amnesty International, by regional human rights organisations such as the East and Horn

of Africa Human Rights Defenders Network and the African Centre for Justice and Peace Studies, or by Sudanese organisations in the diaspora and their allies inside the country, such as JHR.

Restrictions on NGOs limit their role in monitoring and documenting human rights violations and internet censorship, as well as their ability to develop capacity-building projects and training programmes for human rights defenders and activists.

Action steps

The deterioration of the human rights situation and restrictions on freedom of expression in Sudan as a result of the economic crisis and armed conflict in five countries in the region is a matter of concern and needs to be addressed at regional and international human rights platforms such as the UN Human Rights Council and the African Commission on Human and Peoples’ Rights. According to activists, regional and international pressure helps advocacy initiatives.

Human rights organisations have for years used different tools to mobilise available avenues to inform the world about gross violations of human rights and freedom of expression in Sudan, and to ask the state to fulfil its international and regional human rights obligations. In 2015 Sudan will submit its second Universal Periodic Review (UPR) report to the UN Human Rights Council. The government of Sudan should take serious steps to implement the recommendations which were received in the first UPR process and accepted by Sudan.¹⁷ The recommendations include ratifying international human rights treaties; reviewing the institutional and legislative framework to be in accordance with international human rights standards; reforming the repressive Press and Publication Act of 2009 and the 2007 IT Crime Act; and lifting restrictions on freedom of expression and censorship of the internet.

9 Reporters Without Borders. (2014). *Enemies of the Internet 2014*. 12mars.rsf.org/2014-en/enemies-of-the-internet-2014-entities-at-the-heart-of-censorship-and-surveillance

10 Reporters Without Borders (2013, September 30). All-out censorship in response to anti-government protests. *Reporters Without Borders*. en.rsf.org/sudan-all-out-censorship-in-response-to-30-09-2013,45248.html

11 <https://www.accessnow.org/page/-/Open%20Letter%20to%20Sudan%20Telcos.pdf>

12 Access letter to data providers, on file with Human Rights Watch, dated 11 October 2013.

13 A political party led by Sudanese ex-prime minister Sadiq al-Mahdi.

14 Reporters Without Borders. (2014). Op. cit.

15 www.altareeq.info/ar/control-the-internet-and-phones-open-spaces-in-the-hands-of-the-security/

16 Sudan Tribune. (2014, May 27). Sudan looking into ways to control Facebook and WhatsApp. *Sudan Tribune*. www.sudantribune.com/spip.php?article51144

17 Statement made by Sudan under review at the HRC under item 6 after the adoption of the UPR report on 16 March 2012.

SWITZERLAND

“All eyes on you”



Communica-ch

Wolf Ludwig
www.comunica-ch.net

Introduction

As in various neighbouring countries, the Snowden revelations in early June 2013 caused increasing awareness and concerns in Switzerland about “Big Brother watching you” and surveillance by state authorities. While related discussions have been limited to few and informed circles in the country so far, the revelations have set a new landmark, with public opinion drifting somewhere between overload and resignation. However, the still ongoing revision of the Swiss Federal Act on the Surveillance of Post and Telecommunications (BÜPF) – a long-standing process – has gained broader public attention now and is more contested than ever before (see the Swiss country report from GISWatch 2011).¹ As in surrounding countries, widespread security considerations – mostly referring to terrorist threats or child pornography – are increasingly threatening and undermining principles of access and openness, as well as civil rights. Over the years, starting in May 2010, the federal government (Bundesrat) and its justice and police department are relentlessly pointing to the necessity of new technical means to combat crime and enhance law enforcement.² Such means, like Trojan horses on computers of suspects and the prolongation of the current data retention period from six to 12 months, are sold as “technological upgrades”, while providing “not more, but better surveillance”.

Policy and political background

In the first round of the usual consultations on new laws between May and September 2010, the suggested BÜPF revisions were harshly criticised by most stakeholders from the business sector and

civil society. The strongest concern was raised about the intended installation of Trojan horses on computers of suspects, and the prolongation of the current data retention period from six to 12 months. Under the contested data retention rules, internet service providers (ISPs) are obliged to store comprehensive customer data to be delivered to security forces on demand. Another bone of contention, besides privacy concerns, was a new broad definition of “access providers”, including all sorts of internet-related services. The broad resistance from various parts of society – including the right-wing Swiss Peoples Party (SVP/UDC), usually at the law and order front – caused some delays in the legislative procedure and pulled the Federal Department of Justice and Police into a crisis of needing to explain its position.³ A year later, in November 2011, the Federal Council announced a revised version of the Ordinance on the Surveillance of Post and Telecommunications (VÜPF), which was to come into effect in January 2012. With the revised VÜPF, the government cunningly bypassed the contested BÜPF by introducing new surveillance measures at the ordinance level – such as prescriptions for telecom and service providers to monitor mobile and internet traffic.⁴

The BÜPF: Extending surveillance

At the time, critics surmised that this accelerated revision of the Ordinance actually circumvented the legislative power of the parliament, without creating the required legislative basis for any new surveillance laws by simply creating precedents. The Ordinance’s field of application was adjusted by including internet access providers alongside their telecom equivalents. These providers are obliged to secure infrastructure to facilitate surveillance and to implement new surveillance measures either by themselves or to task a third party to do this. Internet access providers were given a reprieve of 12 months for implementation.

With the revised VÜPF the government announced an overhauled schedule for the ongoing revision of the BÜPF.⁵ Two years later, in February 2013, the Federal Council submitted its Memorandum (Botschaft) to the parliament regarding the BÜPF – a usual legislative procedure in the country. The purpose of the revision would be “to provide a clear and restrictive legal basis” for law enforcement and the use of GovWare for criminal procedures. This special software is used by police to monitor communication data such as sender, recipient, date, duration and ways of communication.

On the other hand, the new law did not allow the online investigations of computers or surveillance of spaces using cameras and microphones from infiltrated computers. The use of GovWare was supposed to be limited to “hard crimes” only, which justified covert investigations.

The government insisted on the prolongation of data retention from six to 12 months. According to the new law, surveillance by law enforcement bodies cannot be done in a preventive manner but only in the course of a criminal procedure. It must be ordered by public prosecutors and approved by court decision. Suspects may object to surveillance – if or whenever they get to know about it.

Compared to the VÜPF, the field of application in the revised BÜPF will be considerably extended: from telecom and internet access providers to service and hosting providers, chat forums and platforms, as well as all forms of other networks like hotels, hospitals, universities, public libraries and schools.⁶

Besides some modifications to the first contested draft (May 2010), its new version appears to various stakeholders like new wine in old wineskins – basically sticking to new surveillance techniques undermining civil rights and liberties. Critical voices did not become silent: in February 2014, Digital Society Switzerland, a small but active group specialised in net policy, together with six other civil society groupings including Member of Parliament Balthasar Glättli (Green Party), launched a complaint against data retention in Switzerland. The federal office in charge, the Service for Surveillance of Post and Telecommunication Traffic (ÜPF), rejected the complaint – as expected – by arguing that “high legal barriers would protect fundamental rights.” The complainants appealed to the Federal

Administrative Court.⁷ Meanwhile, in April 2014, the European Court of Justice (ECJ) declared the Data Retention Directive of the European Union “invalid” – a landmark ruling for many civil liberties groups all over Europe.⁸ The ECJ is backing key arguments of the Swiss complainants that existing practices for data retention “exceeded the limits imposed by compliance with the principle of proportionality” and calling it “a wide-ranging and particularly serious interference with the fundamental rights of respect for private life and of the protection of personal data.”⁹

Despite this revealing court ruling and broad opposition, the Swiss government and authorities drift between being unimpressed and stubborn. In March this year – just before the verdict – the Second Chamber of the Swiss Parliament (Ständerat), representing the cantons, gave its blessing to the BÜPF: 94% of the council’s members voted in favour, with only two votes against and four abstentions. Even some Ständeräte who had doubts caved in. Alexis Roussel, president of the Swiss Pirate Party, criticised the decision by concluding: “The Ständerat didn’t learn anything from the Snowden revelations.”¹⁰

Freedom or security – a common dilemma

However, parties and stakeholders opposing the planned BÜPF revision are broader than before. While most of the political parties (except the Greens) and the country’s political establishment of parliamentarians and party leaders support the new law or are indifferent at least, most of the party youngsters from all political spectrums have changed sides and joined the increasing ranks of opposition. Summer 2014 somehow looked like a showdown: at the end of May Switzerland saw its first net-political demonstration in front of the Federal Parliament in Bern, where several hundreds of people – digital natives mostly – expressed their common concerns against the BÜPF. They were supported by representatives from major business associations in the telecom and internet industry. Speakers from Asut, the Swiss Telecommunications Association, and Swico, the Association of ICT enterprises, besides others, expressed strong

1 Ludwig, W. (2011). Switzerland: Surveillance and security mania violating basic rights. In APC and Hivos, *Global Information Society Watch 2011: Internet rights and democratisation*. www.giswatch.org/en/country-report/freedom-expression/switzerland

2 Bundesamt für Justiz, Überwachung des Fernmeldeverkehrs, Totalrevision des Bundesgesetzes betreffend die Überwachung des Post- und Fernmeldeverkehrs (BÜPF). www.ejpd.admin.ch/content/ejpd/de/home/themen/sicherheit/ref_gesetzgebung/ref_fernmeldeueberwachung.html

3 Ludwig, W. (2011). Op. cit.

4 Bundesamt für Justiz, Post- und Fernmeldeüberwachung: Klare und restriktive Rechtsgrundlagen, press release, November 2011. www.ejpd.admin.ch/content/ejpd/de/home/dokumentation/mi/2011/2011-11-23.html

5 Ibid.

6 Bundesamt für Justiz, Post- und Fernmeldeüberwachung: Klare und restriktive Rechtsgrundlagen, press release, February 2013. www.ejpd.admin.ch/content/ejpd/de/home/dokumentation/mi/2013/2013-02-27.html

7 Steiger Legal, Urteil pro Vorratsdatenspeicherung in der Schweiz, July 2014. https://www.steigerlegal.ch/2014/07/01/urteil-pro-vorratsdatenspeicherung-in-der-schweiz

8 Court of Justice of the European Union, The Court of Justice declares the Data Retention Directive to be invalid, press release No 54/14, April 2014. curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf

9 See footnote 7.

10 Ständerat segnet BÜPF-Revision ab, Computerworld.ch, March 2014. www.computerworld.ch/news/it-branche/artikel/staenderat-segnet-buepf-revision-ab-65429

reservations. Jean-Marc Hensch (Swico) welcomed the demonstrators: “Dear potential criminals, dear possible suspects” – referring to broad-scale surveillance and the storage of personal data without concrete facts supporting suspicion of a crime.¹¹ A speaker from the young social democrats (Juso) accused the Federal Council and his party elders of “historical amnesia”, pointing to the revelations of the second Secret Files Scandal in summer 2010 (and the early 1990s) or similar incidents that had shattered people’s confidence in its secret services before.¹²

The Federal Parliament (Nationalrat) was supposed to deal with the BÜPF bill in June, but the debate was postponed to its autumn or winter session. Observers predict more critical voices and substantial debates among parliamentarians, yet parliamentary opponents seem to be rather scarce. Ruedi Noser from the Liberal Party and a well-known ICT entrepreneur reflects: “Many MPs are not aware about the consequences of the BÜPF because they are digitally distant.” They obviously care more about banking secrecy than privacy. “I need to remind my party folks that privacy matters on the internet as well,” he said.¹³

Privacy as a privilege?

From the official side, it is Switzerland’s Data Protection and Information Commissioner Hanspeter Thür who expresses doubts about private and state actors that need to be better controlled whenever collecting data. “Consumers have almost no options any more to protect their private sphere – privacy becomes a privilege,” he feels.¹⁴ According to a recent study conducted in nine countries on behalf of the European Commission, public awareness and wariness about state surveillance is on the rise. The survey sample in Switzerland (75 to 90 people in all language regions) indicated that Swiss citizens are rather anxious about surveillance of the public for security reasons: 38% only were in favour of it (citizens are more critical in Germany only).¹⁵

A referendum on surveillance seems predictable

Political prognoses are usually difficult, depending on various factors (not only in Switzerland). However, if the contested BÜPF passes the Federal Parliament in the autumn or winter session (like the second Chamber Ständerat in March before) – which seems to be predictable – a referendum will be called for by various actors in the country. A Referendum Committee was already created at the end of May.¹⁶ Such referendums are instrumental to direct democracy and an essential part of the political system in Switzerland. Whenever the two Chambers of the Parliament pass a law, a public referendum can be announced and organised by any stakeholder groups in the country (usually political parties, unions, business or other associations or any initiatives). They usually create an alliance of opponents called a Referendum Committee. Such committees need to collect 40,000 signatures (practically, around 50,000 are necessary) from all over the country during a limited period of several months. Once this number is achieved, large packages of signatures are delivered – usually in a public action – to the Federal Chancellery in Bern. The office in charge will review and check the validity of the collected signatures before a referendum is officially approved. Upon approval of a referendum, the respective law is suspended until public voting – dates are fixed by the Federal Council in the course of the next federal voting schedule (usually in spring, summer or autumn every year).

The biggest challenge for any Referendum Committee is to organise broader alliances of supporters among opponents and to raise funds (a minimum of one million Swiss francs, roughly USD 110 million) for a voting campaign. In the given case of an anticipated Anti-BÜPF campaign, the prospects are not bad, with strong business actors on board (not only for money, but also for networking). Another decisive success factor for any such campaign is media coverage and support by influential media titles all over the country. As it looks now, the mixture of the Anti-BÜPF coalition is rather unique and heterogeneous, and has considerable potential to mobilise support from various spheres of Swiss society – particularly among youngsters and digital natives. However, a well-known risk factor is voting discipline – usually elder and conservative people use the opportunities of direct democracy while younger generations tend to abstain. And usually the level of participation in Swiss voting is rather

low, at around 50% or less. Nevertheless, an Anti-BÜPF campaign (depending on the final decision of the parliament) offers great opportunities for broader public discourse about state and other forms of surveillance in the digital age. The colourful coalition of critical voices and pronounced opponents of this law looks promising at least. What appears like a conflict of generations – digital natives versus immigrants – could be a next step into an open Swiss information society.¹⁷

Action steps

The topic of advancing the information society in Switzerland is so far mostly limited to some specialists, academia or a few informed circles. A high percentage of the population (close to 80%) use computers, mobile devices and the internet on a daily basis, but do not care so much about related issues, problems or challenges – as long as access to infrastructure and content is provided and everything works well. Even those using social networks

like Facebook, etc., generally do not care about privacy that much. Compared to Germany, net politics and related matters is still a playground for a few nerds, and media and internet literacy is often demanded but continuously underserved. More initiatives in this respect are needed on various levels of society (particularly schools). To work against the idea that “privacy becomes a privilege”, more awareness raising and discussion is needed – from the family up to the political levels (parties and parliament).

The anticipated Anti-BÜPF campaign (after the law is presumably adopted later this year) offers a great chance for broader public dispute and contestation on limits of state interference into and surveillance of private spheres. As the political establishment of the country has not yet arrived in the digital age, other parts of society – like the Anti-BÜPF coalition – need to step in and take the lead for an appropriate debate about the dangers and limits of surveillance.¹⁸

11 STOP BÜPF, Medienecho zur Stop-Büpf-Demo vom 31. Mai 2014 and Testimonials. stopbuepf.ch/medienecho-zur-stopbuepf-demo-vom-31-mai-2014

12 Die Fichenaaffäre – eine Geschichte von Lug und Trug, Tagesanzeiger, 5 July 2010. www.tagesanzeiger.ch/schweiz/standard/Die-Fichenaaffaere--eine-Geschichte-von-Lug-und-Trug/story/16223362

13 Überwachung: Der Streit um Staatstrojaner spaltet die Parteien, TagesWoche, July 2014. www.tageswoche.ch/de/2014_30/schweiz/664229

14 Datenschutz: „Privatsphäre wird zu einem Privileg“, Interview with the FDPIC, March 2014. www.nzz.ch/aktuell/schweiz/privatsphaere-wird-zu-einem-privileg-1.18256915

15 Schweizer lehnen Staatsüberwachung ab, NZZ am Sonntag, May 2014. www.nzz.ch/aktuell/schweiz/schweizer-lehnen-staatsueberwachung-ab-1.18309315

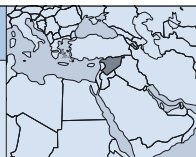
16 Ibid.

17 Petition STOP BÜPF, Nein zum Überwachungsstaat, July 2014. buepf.ch

18 Balthasar Glättli, Dossier BÜPF (13.025 Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs). www.balthasar-glaettli.ch/dossier/dossier-buepf-bundesgesetz-betreffend-die-ueberwachung-des-post-und-fernmeldeverkehrs

SYRIA

Circumventing surveillance of internet communications



Karim Bitar

Introduction

Hardly a day passes without news about the conflict in Syria making headlines. After more than three years of clashes, the death toll is estimated to have exceeded 150,000.¹ Since the early days of the uprising, the government has imposed strong restrictions on foreign media coverage of the events, granting access only to reporters who share its side of the story.

Under such restrictions, it would be expected that the opposition would turn to citizen journalism to provide coverage of the events from its perspective. Many initiatives were started for this purpose, using mobile phone cameras to record and document events, and broadcast this footage to the world through the internet.

With the internet becoming the only viable medium for communication, the issue of the government's ability to intercept, block and exploit the communications of the opposition becomes a major challenge. Citizen journalists and activists had to find creative measures to circumvent government surveillance and protect their communications.

In the following sections of this report, I investigate a major project implemented by the Syrian government to intercept and trace all the digital activities and communications of its citizens. I also explore the tools and techniques developed by Syrian citizens to bypass the government's intrusive eye, and regain their privacy.

Policy and political background

Surveillance of citizens' communications is not new in Syria. While it has certainly intensified in scale and scope over the past four years, government surveillance has been a dominant theme in the country for decades, pre-dating the internet and digital communications. While the Syrian Constitution protects freedom of expression, and guarantees the privacy

of all communications of the country's citizens, the government does not seem to be too concerned about that.

Syria was ruled by a state of emergency law from 1963 to 2011.² This law severely restricted personal liberty and freedom of expression. The massive secret services organisation established shortly after ensured that the red lines were clearly drawn, and those who crossed them were duly punished. As a result, Syria became the 177th country (out of 179) on the Reporters Without Borders' 2014 Press Freedom Index,³ and was given the "worst of the worst" title by Freedom House in 2014 for achieving the lowest possible ratings on all criteria in political rights and civil liberties.⁴

This explains the internet's delayed entry into the country, since an open, international and difficult-to-control communication medium could undermine the establishment and lead to situations the government may not tolerate. Over time, the government realised that it could use the exact same technology to expand the scale and scope of its traditional surveillance activities, and it soon acted to make mass surveillance of digital communications the new reality.

Pervasive surveillance in the digital age

In late 2011, an Italian telecommunications company, Idea SpA, was caught in the midst of an unsettling controversy: the company was installing surveillance equipment in Syria that would enable the government to intercept every single email and internet communication that flows through the country.⁵

The leaked details of the deal, which are highly credible given the details they cite, indicate that the installed system would use deep packet inspection

to analyse the content of all traffic that travels through the country's national public data network (PDN). The national PDN constitutes the digital communications backbone for the whole country, and all traffic – for internet service providers (ISPs), banks, voice over IP (VoIP), etc. – passes through its infrastructure. This would give the installed surveillance system comprehensive access to all digital communications in the country, and the leaks of the deal confirm that Idea SpA was training local personnel on operating the system's monitoring and tracing capabilities.

While Idea SpA used some of its own technology to integrate the system, it also implemented several components from other hardware and software vendors, including US company NetApp Inc., French company Qosmos SA, and German company Utimaco Safeware AG. These companies were quick to announce that they were unaware that their products were shipped to Syria, and that they were acquired locally in Italy. This raises serious questions about the effectiveness of export control regulations for surveillance gear, and how easily such regulations can be circumvented.

A primary concern for surveillance projects like this is the argument that the government can use them to hide its intrusive surveillance activities under the "lawful interception" of citizens' communications for law enforcement purposes. In fact, that is precisely the claim stated by Idea SpA's CEO in responding to the criticisms of his firm's involvement in the project.

What those who adopt this argument fail to mention, however, is that "lawful interception" is tightly governed by checks and balances to ensure all activities are performed in accordance with the country's constitution and applicable laws. This includes, for example, the need for a court warrant that is only issued after due legal process. The secrecy surrounding this project, and many similar others, makes it impossible to verify its compliance with these requirements.

Another argument used to justify mass surveillance is that "everybody else does it". With the recent revelations on mass surveillance programmes in the United States, the United Kingdom and other countries, even established democracies were caught in the act of invading the privacy of their citizens and those of other countries, despite long traditions of freedom of expression and privacy protection. If it is so easy to bypass the constitutional guarantees and secretly intercept citizens' communications in these countries, how can much less democratically developed countries be expected to set a better example?

The problem is actually compounded for citizens of the latter, since they are subjected to several layers of spying and surveillance. At one level, their governments are engaging in intrusive, large-scale interception and surveillance of their communications. On another, they are subjected to foreign surveillance from countries other than their own. It is not unrealistic to imagine this turning into a global overlapping "spaghetti" of surveillance programmes where everyone is spying on everyone else.

In such a distrustful environment, it can be very difficult to even track who is doing what. For example, the recent story of the US National Security Agency (NSA) bugging telecommunications equipment while in transit to its users without the knowledge of the equipment's vendors themselves is a startling example. That story sparked global outrage among customers of US technology companies, and prompted John Chambers, CEO of Cisco Systems Inc., to send a carefully worded letter to President Barack Obama complaining against these acts.⁶

So how are people in Syria dealing with this ubiquitous surveillance of their everyday digital activities? History has taught us that humans have an amazing ability to adapt to their environment and develop creative solutions to overcome the challenges that come their way. Syrians are no exception.

In addition to many awareness raising campaigns and educational activities, such as the Amenny (Secure Me) Digital Awareness Week⁷ (which includes training courses on securing digital communications, erasing trails, awareness videos, and tips on how to use online security tools), a team of Syrian technology professionals developed a specifically designed distribution of the Linux operating system called Virtus Linux to enable users to easily hide their tracks and communicate without fear of the eyes of the person-in-the-middle (or, probably more accurately, people-in-the-middle).⁸

Another approach usually used by Syrian citizens to avoid surveillance is to develop "code language", using agreed upon substitutes for suspicious words and sentences in daily communication. Actually this practice was so widespread that some substitute phrases became famously known for their concealed synonyms. For example, most Syr-

¹ Evans, D. (2014, April 1). Death toll in Syria's civil war above 150,000: monitor. *Reuters*. www.reuters.com/article/2014/04/01/us-syria-crisis-toll-idUSBREA300YX20140401

² Marsh, K., & Black, I. (2011, April 19). Syria to lift emergency rule after 48 years – but violence continues. *The Guardian*. www.theguardian.com/world/2011/apr/19/syria-lift-emergency-rule-violence

³ Reporters Without Borders. (2014). World Press Freedom Index 2014. rsf.org/index2014/data/index2014_en.pdf

⁴ Freedom House. (2014). Freedom in the World 2014. freedomhouse.org/report/freedom-world/freedom-world-2014

⁵ Elgin, B., & Silver, V. (2001, November 3). Syria Crackdown Gets Italy Firm's Aid With U.S.-Europe Spy Gear. *Bloomberg*. www.bloomberg.com/news/2011-11-03/syria-crackdown-gets-italy-firm-s-aid-with-u-s-europe-spy-gear.html

⁶ Bort, J. (2014, May 19). Cisco CEO Writes Letter To Obama Asking Him To Stop The NSA Hacking Into His Equipment. *Business Insider*. www.businessinsider.com/cisco-ceo-letter-to-obama-about-nsa-2014-5

⁷ https://www.facebook.com/events/305539792943989/?ref_newsfeed_story_type=regular

⁸ internetfreedomfh.strutta.com/entry/426472

ians understand that “he is visiting his aunt” refers to someone who has been arrested or put in prison.⁹

While this code language started offline, aiming mainly to disguise information from “the guy next door”, it quickly integrated in the digital communications fabric, now hiding information from “the guy on the wire”.

On top of the code language, and several layers of encryption and secure communications, Syrian activists became masters in the art of concealment. They skilfully separated their online identities from their actual selves, using techniques such as pseudonyms and fake friend lists on social networking sites like Facebook and Twitter. These techniques were constantly updated as activists learned about the government’s methods for tracking them.

By using such techniques, many activists have successfully overcome the government’s elaborate surveillance efforts, limiting their effectiveness to tracking the “naïve” who have not yet acquired the skills to hide their communications. Interestingly, as awareness increases and privacy and security knowledge and tools become widely available and easily accessible, the “naïve” group has started to shrink, as everyone wants to feel in control of their privacy.

But increasing awareness of the privacy violation of mass surveillance activities does not only lead to higher adoption of security tools and techniques; it can also bring about dramatic policy change. For example, following the sustained media focus and reporting on leaks exposing details of some of the US government surveillance programmes, the US Congress moved to limit the NSA’s mass surveillance programme.¹⁰ The fact that many US-based companies took swift action to tighten privacy and security controls in their systems, fearing for their market share both locally and internationally, was undoubtedly a factor that was taken into consideration.

While such policy change is possible in established democracies, it would be much more difficult in totalitarian countries. So how could awareness and grassroots movements affect change in countries like Syria? For one, they can lead to tighter export regulations for surveillance solutions so that they are only imported to countries where rule of

law is respected. Export regulations can also require assurances that such systems will be solely used under the responsibility of appropriate judicial process.

Conclusions

Information and communications technologies (ICTs) have been a transforming power for the economy, education, development and politics. While many benefits can be cited for ICTs, they have had a major unfortunate consequence: they made it much easier for governments and other agencies to spy on people’s communications and activities, both inside and outside their state borders.

While some governments tried hard to resist the adoption of ICTs in their countries, fearing their powerful transforming powers, they eventually realised that these technologies can be used to counter their very own effects in facilitating the free flow of information.

Syria was very late in adopting most new ICTs, mostly because of the fears cited above. However, the government later realised that instead of pushing back, it can actually utilise these technologies to both deepen and widen its surveillance programmes. The project mentioned in this report is but one example that was leaked to the public, and it would be difficult to assert that it is the only existing project. In fact, some reports suggest that other Western companies may have been providing similar equipment to the Syrian government.¹¹

There is a difference, though, between offline and online surveillance: while avoiding offline surveillance usually forced people to stay silent or talk in very small circles, online surveillance can be circumvented with some awareness, techniques and accessible tools. That is precisely what happened in Syria, where the citizens’ response to the massive surveillance programmes was to intensify awareness campaigns and develop technical tools to ensure that people can still communicate and express their opinions without being caught by the government’s expensive surveillance and tracking systems.

But technical approaches are only part of the solution. Policy making is also an important factor. Unfortunately, advocacy efforts for policy change on such sensitive topics in Syria are doomed to yield limited results. Despite the protections afforded by the constitution, several laws were enacted

to restrict privacy and grant several government agencies the right to intercept, track and monitor citizens’ communications. Still, activists and human rights organisations can advocate for higher accountability for companies providing mass surveillance systems, and for better enforcement of export regulations for these systems. However, under what appears to be a global government attack on personal privacy, seeing the fruits of these efforts seems to be a rather long shot. In fact, the failure of the Global Online Freedom Bill, proposed to the US Congress in 2011 to ban sales of US surveillance gear to undemocratic countries, is a recent testament.¹²

Action steps

Despite the increasing efforts to invade privacy and deprive people of personal liberties, several mitigation approaches exist to counter these efforts and reduce their effectiveness. The first step is increasing awareness of the extent of such mass

surveillance efforts and their subsequent risks. Sufficient awareness among global citizens will lead to higher adoption of readily available technical tools that circumvent most of these surveillance efforts and restore confidence in the privacy of digital communications.

Advocacy for policy changes will certainly be needed to create a lasting effect and reduce the need to take sometimes cumbersome technical measures. Policy change is mostly possible in countries with established democracies with a history of relative response to public opinion. Unfortunately, such change is unlikely to happen in countries with less democratic governments. However, the moral responsibility towards citizens in these countries mandates that other options be pursued on the international stage, such as imposing and enforcing appropriate trade sanctions to ensure that capable mass surveillance systems will not be unlawfully abused by governments with a known track record in human rights abuse.

⁹ Friedman, J. J. (2013, October 6). In Syria, code language defies surveillance. The Boston Globe. www.bostonglobe.com/ideas/2013/10/06/syria-code-language-defies-surveillance/1c18bNgxllkqoCElIzeYM/story.html

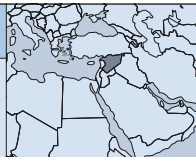
¹⁰ Roberts, D., & McVeigh, K. (2014, May 22). NSA surveillance reform bill passes House by 303 votes to 121. The Guardian. www.theguardian.com/world/2014/may/22/nsa-reform-bill-usa-freedom-act-passes-house

¹¹ Spiegel Online. (2012, April 11). Monitoring the Opposition: Siemens Allegedly Sold Surveillance Gear to Syria. Spiegel Online. www.spiegel.de/international/business/ard-reports-siemens-sold-surveillance-technology-to-syria-a-826860.html

¹² beta.congress.gov/bill/113th-congress/house-bill/491

THAILAND

When elephants fight: Communications surveillance on the rise in Thailand



Thai Netizen Network

Mishari Muqbil and Arthit Suriyawongkul
thainetizen.org

Introduction

Thailand is presently going through a period of upheaval with the population split between two strong ideologies and those in power playing a zero sum game. Surveillance of the internet and other communication mediums has in the last decade been shown to have progressively greater importance to those in power. This can be seen by the 2007 Computer-related Crimes Act (CCA), brought into law by the previous junta; but more telling is the second version of the law, worked on by the subsequently elected civilian government, which focuses on criminal aspects but offers no safeguards to privacy and civil liberties.

The major application for mass surveillance has been in the form of logging internet use and blocking websites, but there have also been cases where law enforcement has requested cooperation from companies such as the social network company LINE in order to acquire chat transcripts to help them prosecute (non-political) criminal cases. However, recently, with the military takeover of the caretaker civilian government on 22 May 2014, surveillance has taken a more totalitarian form.

At 3:00 p.m. on 28 May 2014, people across Thailand could not use Facebook for about 55 minutes. At first it was announced by the National Council for Peace and Order (NCPO) spokesman that there was an issue with Facebook's own internet gateway.¹ But later it was revealed by the vice president and head of communications of Telenor Asia that its local subsidiary DTAC, the second-largest GSM operator in the country, "received a notification at 15:00 local time from the National Broadcasting and Telecommunications Commission of Thailand to restrict access to Facebook

temporarily."² This incident would serve as a warning of things to come.

Policy and political background

The CCA³ stipulates penalties for various computer crimes including unauthorised access and spamming, but the clauses relevant to this report are Section 13, which penalises anyone who "disseminates sets of instructions developed as a tool used in committing an offence;"⁴ Section 14, which penalises the spreading of vaguely defined "false computer data" (often interpreted to use for defamation charges), pornography and information that goes against national security (most notably defamation of members of the royal family); and "intermediary liability" in Section 15, which holds accountable the service provider who "supports or consents" to the crimes committed under Section 14. A service provider is broadly defined and can be anything from a satellite link provider to a coffee shop with free Wi-Fi access. Section 18 allows the authorities to demand traffic data from service providers without a court warrant. Article 25 of the Special Case Investigation Act (2004, amended 2008) also allows communication interception without notification.⁵ Since 2012, every computer-related crime case is a special case under this Special Case Investigation Act.⁶

The new junta has chosen to act slightly differently. Their *modus operandi* seems to be the direct command of ministries and semi-governmental organisations to carry out tasks irrespective of existing legislation.

Compliance with international benchmarks on surveillance

Since the military junta has taken power, there has been one high-profile arrest based on computer evidence. Sombat Boonngamanong, an activist who defied the junta, was tracked through his IP address.⁷ It is of concern how this happened exactly, as Sombat's primary visible form of expression is through Twitter and Facebook. Both are HTTP Secure-enabled,⁸ which should prevent any agents monitoring Thai internet traffic from tracing his account back to his address. We can only speculate that he made an error in operations security which resulted in his IP address being revealed, but we also cannot rule out the possibility of Facebook's cooperation with the junta or the existence of highly advanced surveillance capabilities.

If we look at this evolving situation in the context of the 13 International Principles on the Application of Human Rights to Communications Surveillance,⁹ we see that Thailand has entered a precarious situation:

1. Legality – It can be argued that surveillance and intercepts are in effect legal, as laws have been written to give the state power to intercept. However, if it is implemented in such a way that citizens cannot foresee its application, then we fall short on this principle. Specifically in the case of DTAC above, the junta denied that such a block was ordered, and when Telenor's executive said otherwise,¹⁰ the company felt threatened.¹¹
2. Legitimate aim – It is arguable whether retaining logs of all internet traffic complies with a legitimate aim or not. One thing is certain: Sombat has been charged with "cyber crime as well as of inciting unrest and violating junta orders"¹² for not reporting to the junta when summoned, and

for organising a flashmob.¹³ This is definitely not a "legal interest that is necessary in a democratic society."¹⁴

3. Necessity – The provisions in the CCA require internet service providers (ISPs) to retain traffic data logs for up to three months to make them available for scrutiny by the state. The information, if requested, must be handed over to a competent officer without the requirement of any judicial oversight. Since the coup, however, it is unclear whether this applies anymore, as seen by the shutting down of Facebook with no reason provided nor an acknowledgement of the shutdown order.
4. Adequacy – Despite the blanket provisions and data logging requirements of the CCA, it does not seem to adequately fulfil all legal requirements. In 2013 Thai authorities reached out to LINE for access to online chat records.¹⁵
5. Proportionality – Here, it is enough to quote one analyst: "The Computer Crime Act has been criticised for its unclear provisions and harsh penalties."¹⁶ This is by virtue of the fact that the language of the act is open to very broad interpretations, and some provisions prescribe a harsher penalty for a crime using a computer, compared to the same crime conducted without a computer.
6. Competent judicial authority – This is split into two parts: regular criminal and civil cases under the CCA, which are handled by the respective civilian courts, and national security cases, which are now handled by military courts.¹⁷ The civilian courts have had some training and experience dealing with such cases (even though this is questionable).¹⁸ However, it is certain that the military courts have had no experience dealing with CCA-related issues and are unlikely to base their judgements on human rights considerations.
7. Due process – Human Rights Watch (HRW) says it best: "The May 25 order [to try civilians in

1 The Nation. (2014, May 29). No policy to block fBFB. (2014, May). Retrieved June 13, 2014, from [The Nation](http://www.nationmultimedia.com/politics/%5CNo-policy-to-block-FB%5C-30234896.html).

2 Vals, M. (2014, June 9). Telenor says Thailand's recent Facebook outage was ordered by the government. *The Next Web*. thenextweb.com/asia/2014/06/09/operator-dtac-says-thailands-government-forced-shut-access-facebook

3 <https://thainetizen.org/docs/thailand-computer-crime-act-2550> (original); <https://thainetizen.org/docs/thailand-computer-crime-act-2550-en> (English translation).

4 Under the previous section which can penalise security research as well as make dual use software illegal because the same set of computer tools that can be used to test for security flaws can also, by their very nature, be used to gain unauthorised entry.

5 Special Case Investigation Act (No. 2, amended February 2008). bit.ly/thaispecialcaseinvestigationact2008 (Thai and English translation)

6 Ministerial Regulation on Additional Special Cases according to Special Case Investigation Act (No. 2). bit.ly/morespecialcases2 (in Thai)

7 Sawitta Lefevre, A. (2014, June 6). Thai junta tracks internet posting to capture protest leader. *Reuters*. uk.reuters.com/article/2014/06/06/uk-thailand-politics-idUKKBN0EHOX20140606

8 HTTP Secure (HTTPS) is a standard for protecting internet traffic from intercepts, by encrypted communications using Transport Layer Security (TLS) or its predecessor, Secure Sockets Layer protocol. More technical information can be found at www.tldp.org/HOWTO/SSL-Certificates-HOWTO/x64.html; for more information in plain English, watch this animation: youtu.be/DPYYwocrbFE

9 <https://en.necessaryandproportionate.org/text>

10 Vals, M. (2014, June 9). Op. cit.

11 Woodgate, E. (2014, June 11). Telenor threatened by Thai junta. *News in English.no*. www.newsinenglish.no/2014/06/11/telenor-threatened-by-thai-junta

12 Ngamkham, W., & Sattaburuth, A. (2014, June 11). Sombat now faces cyber-crime charge. *Bangkok Post*. www.bangkokpost.com/news/politics/414655/sombat-now-faces-cyber-crime-charge

13 Purnell, N. (2014, June). How Thai flash mobs avoid capture. *Wall Street Journal*. blogs.wsj.com/searealtime/2014/06/01/how-the-thai-flash-mobs-avoid-capture

14 <https://en.necessaryandproportionate.org/text>

15 Doksono, T. (2013, August 13). Thai police seek to monitor chat app for crimes. *AP*. bigstory.ap.org/article/thai-police-seek-monitor-chat-app-crimes

16 Charoen, D. (2012). The analysis of the Computer Crime Act in Thailand. *International Journal of Information and Communication Technology Research*, 2(6). esjournals.org/journaloftechnology/archive/vol2no6/vol2no6_7.pdf

17 Thai PBS. (2014, May 25). NCPO announces cases to be tried by military court. *Thai PBS*. englishnews.thaipbs.or.th/ncpo-announces-cases-tried-military-court

18 Panananda, A. (2012, May 15). Oddities abound in Amphon's trial and jailing. *The Nation*. www.nationmultimedia.com/politics/Oddities-abound-in-Amphons-trial-and-jailing-30181989.html



Landing page that says: "This website contains content and information that is not appropriate and has been suspended by the Ministry of ICT."

military courts] grants the military wide-ranging powers to prosecute civilians without basic due process protections, and prohibits defense counsel and rights to appeal.¹⁹

8. User notification – Passive surveillance happens without any indication to the user that it is happening. However, if users try to access a blocked URL, they are greeted with a landing page. There are several different landing pages depending on which state authority is responsible for the URL being blocked. A landing page by the Ministry of ICT is shown in Figure 1. In June 2014, the Thai Netizen Network found that the blocked URL landing page that is run by the Technology Crime Suppression Division (TCSD) is trying to imitate the Facebook login screen and collecting visitors' personal information. The TCSD block page has two graphics: one is a blue "Close" button, and the other is a "Login with Facebook" icon. If the second is clicked, visitors will be redirected to a TCSD Facebook application named "Login" and asked for permission to access their personal information stored in their Facebook profile – without any indication of where that data is being sent, or for what purpose.²⁰

9. Transparency – There is no official list available of websites being blocked. In the past, after the 2006 coup, Freedom Against Censorship Thailand (FACT) made the block list available by leaking information from the official list given out to ISPs.²¹ In 2007, FACT and the Campaign for Popular Media Reform petitioned for the block list using the 1997 Official Information Act^{22,23} but eventually failed. The Official Information Commission said that revealing the block list could harm the website owners' reputations,²⁴ citing the "privacy" exemption of the Act. There are also no lists available of the number of requests to share data that an ISP has received, and when DTAC acknowledged being asked by the junta to block Facebook, it was threatened with punitive measures.²⁵
10. Public oversight – There is little or no public oversight. Law enforcement officials are empowered to act on their own.
11. Integrity of communications and systems – Interception can put users in danger by creating a

21 facthai.wordpress.com/data

22 FACT. (2007, February 11). Information Request Letter to MICT. *FACT*. facthai.wordpress.com/2007/02/11/info-request-letter-to-mict-eng

23 FACT. (2007, April 3). FACT files Freedom of Information complaint. *FACT*. facthai.wordpress.com/2007/04/03/fact-files-freedom-of-information-complaint

24 Freedom House. (2011). *Freedom on the Net 2011: Thailand country report*. www.freedomhouse.org/report/freedom-net/2011/thailand

25 Woodgate, E. (2014, June 11). Op cit.

19 Human Rights Watch. (2014, May 28). Thailand: Halt military trials, end arbitrary arrests. *Human Rights Watch*. www.hrw.org/news/2014/05/28/thailand-halt-military-trials-end-arbitrary-arrests

20 O'Brien, D. (2014, June 24). Thai junta used Facebook app to harvest email addresses. *Electronic Frontier Foundation*. https://www.eff.org/deeplinks/2014/06/thai-junta-used-facebook-app-harvest-email-addresses

convenient attack point. For example, for a while the proxy for True (a major ISP) was compromised, serving pop-up ads.²⁶ Since the attacker could wilfully manipulate web traffic data, it is unknown what else they may have done during this period. There is also little transparency on the side of the ISPs on the issue of who has access to the traffic information and how interception is happening. There is no consideration of whether the state would refrain from compelling the identification of users. Internet usage at internet cafés requires users to provide identification, which is recorded, before access is granted and, since the coup, it has been reported that vendors have been consulted to find a way where "[e]very Thai citizen will need to authenticate an internet log-on session with a smart ID card."²⁷

12. Safeguards for international cooperation – When the Thai authorities were getting in touch with the LINE corporation, there did not seem to be any resistance from the Thai division of the company. In Japan, where LINE's HQ is based, they were clear that a Japanese court order is required to comply in any way with state requests.²⁸ More telling is a recent incident where authorities decided to seek cooperation with social media providers to block content.²⁹ A trip was planned to Singapore to pursue the matter, but then was abruptly cancelled.³⁰
13. Safeguards against illegitimate access – The CCA stipulates in Article 24 that if information gathered by a competent official is leaked by anyone, they can face a jail term of up to two years or be fined up to 40,000 baht (about USD 1,200), which could help deter neglect on the part of the officer. However, it is unclear how many safeguards apply under the coup administration.

Conclusions

There is an African proverb that says, "When elephants fight, the grass gets trampled." The proverbial

grass in this case is the right to access and distribute information, which is the scenario that is unfolding now in Thailand. It is doubtful that the situation will get better any time soon as this conflict intensifies; and if the current trend is any indication, it has the potential to get worse.

Based on the pattern of the junta making regular announcements for key individuals to report to them,³¹ in combination with "Big Data's" ability to combine cross-referenced usage data from the logs retained from ISPs under the CCA, Prime Minister Yingluck's one million CCTV cameras in Bangkok,³² and some form of Wi-Fi tracking³³ (possibly using government-sponsored free Wi-Fi access points),³⁴ it is not difficult to see how if left unchecked, Thailand can turn into a pervasive surveillance society.

Action steps

The best strategy is to have a three-pronged approach:

- Educate – Inform the public about what criminal laws such as the CCA and surveillance mean for them. Give examples so that they can see what they stand to gain and lose from a surveillance society; then give them tools to protect their privacy and train them how to use them so that they may preserve their privacy if they choose to. This, however, should be done with care, as it is uncertain if the junta will consider such actions to be illegal in the future.
- Collaborate – At present there is no end in sight to the political conflict. However, it may be possible to convince the junta that if they had publicly released block lists and block orders, then their denial of the Facebook block would have been much more credible.
- Advocate – Activists must continue to advocate for strict controls over surveillance in Thailand and in the region, but it is unlikely that there will be the political will to do so any time in the near future.

26 Sambandaraksa, D. (2014, January 13). True Internet's proxy compromised. *Telecom Asia*. www.telecomasia.net/content/true-internets-proxy-compromised

27 Sambandaraksa, D. (2014, June 10). Thai junta holding the mother of all garage sales. *Telecom Asia*. www.telecomasia.net/blog/content/thai-junta-holding-mother-all-garage-sales

28 Leesa-nguansuk, S. (2014, May 31). LINE data request faces legal hurdles. *Bangkok Post*. www.bangkokpost.com/news/local/412749/line-data-request-faces-legal-hurdles

29 The Nation. (2014, May 29). Junta to seek cooperation from Facebook, LINE, YouTube to block 'inappropriate content'. *The Nation*. www.nationmultimedia.com/breakingnews/junta-to-seek-cooperation-from-facebook-LINE-YouTube-30234955.html

30 Purnell, N., & Chaichalearmmongkol, N. (2014, June 2). Thai junta says Facebook, Google meetings called off. *Wall Street Journal*. online.wsj.com/articles/thai-junta-says-facebook-google-meetings-called-off-1401689775

31 The Nation. (2014, May 24). Military junta summons 114 more to report today. *The Nation*. englishnews.thaipbs.or.th/military-junta-summons-114-report-today; The Nation. (2014, May 24). Junta summons 35 more figures. *The Nation*. www.nationmultimedia.com/breakingnews/junta-summons-35-more-figures-30234505.html; Prachatai. (2014, June 5). Junta summons activists-lèse majesté suspects in exile. *Prachatai*. www.prachatai.com/english/node/4092

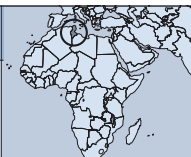
32 Thai PBS. (2013, November 5). Yingluck to open Miracle Eye project in Bangkok today. *Thai PBS*. englishnews.thaipbs.or.th/yingluck-open-miracle-eye-project-bangkok-today

33 Cunche, M. (2013). I know your MAC address: Targeted tracking of individual using Wi-Fi. *International Symposium on Research in Grey-Hat Hacking - GreHack (2013)*. hal.archives-ouvertes.fr/docs/00/85/83/24/PDF/Wi-Fi_Stalking.pdf

34 Government Public Relations Department. (2012, September 1). Opening over 20,000 free WiFi hotspots in Bangkok. Press release. thailand.prd.go.th/view_news.php?id=6070&a=4

TUNISIA

New Big Brother, non-existent reforms



Afef Abrougui
afef_abrougui@live.fr

Introduction

The shadows of the mass surveillance state still chase Tunisians, as the northernmost African country adopts a new constitution enshrining privacy rights three years after the ouster of former autocratic President Zine el Abidine Ben Ali.

To keep a tight grip on political dissent, authorities under the Ben Ali rule practised unchecked and indiscriminate surveillance of citizens' communications. Spying agents at the Interior Ministry and the Presidential Palace tapped into phones and through deep-packet inspection (DPI) intercepted and altered emails.¹

Tunisia's successive interim governments repeatedly spoke out to reassure citizens that the spying practices of the past had dissipated and that surveillance in the post-Ben Ali era is conducted only after obtaining judicial orders. However, steps taken by the authorities to set up a new telecommunications surveillance entity, the Technical Telecommunications Agency (better known by its French acronym the ATT), raised eyebrows.

While the Tunisian authorities argue that the creation of the agency is needed for its counter-terrorism efforts, privacy advocates and human rights groups worry that the lack of independent oversight mechanisms will only imperil user rights.

Policy and political background

Throughout 2013 and 2014, armed groups believed to be affiliated with Al-Qaeda in the Islamic Maghreb (AQIM) waged several attacks on security and armed forces in different regions of the country, leaving dozens of deaths and injuries among soldiers and police officers. In the wake of these attacks, the Interior Ministry reiterated calls for the filtering and monitoring of the internet. Indeed, the scrapping of the former regime's internet filtering

practices in 2011 allowed for the flourishing and unrestricted dissemination of local content on the web, including extremist religious discourses that incite to violence.

Speaking to the Arabic-language newspaper *Alchourouk*² in February 2014, Interior Minister Lotfi Ben Jeddou said that there are at least two platforms used to subvert and impede security action: "cyberspace and mosques". "The internet is being deployed as a tool to incite terrorism," he added.

"These internet sites represent a threat (...) they nurture terrorism and extremism," said Interior Ministry spokesman Mohamed Ali Aroui during a news show³ broadcast on 28 February 2014 on the privately-owned Ettounsiya TV.

The authorities also blamed the use of online platforms to recruit hundreds⁴ of young Tunisian jihadists to fight the Syrian regime of Bashar al-Assad.

New Big Brother, non-existent reforms

On 6 November 2013, the government of former Prime Minister Ali Laarayedh issued Decree No. 2013-4506⁵ providing for "the creation of the Technical Telecommunications Agency (ATT) and determining its administrative and financial organisation and methods of functioning". Article 2 of the decree tasks the agency with "providing technical support for judicial investigations into information and communication crimes."

The ATT is set to fill a legal and institutional vacuum that characterised communications surveillance in post-Ben Ali Tunisia. With the creation of the ATT, communications surveillance in Tunisia is

now the responsibility of one single agency known to the public.

Under the Ben Ali regime, different organs were believed to be involved in monitoring citizens' communications, including the disbanded secret police,⁶ the Tunisian Internet Agency (ATI), which hosted internet surveillance and censorship equipment, and the Presidential Palace.

"Lawful interception will [now] be based on institutions worthy of a democracy," Mongi Marzouk, the former information and communications technology (ICT) minister, told the local technology news site *Tunisie Haut Débit* in January 2014,⁷ in defence of the setting up of the new surveillance body.

With the creation of the ATT, "the process of [providing] the judiciary with technical support will be institutionalised to end non-transparent phone-tapping," he added.

"The benefits, if they exist, are about the fact that for the first time surveillance has a form, an agency, and we are no longer in the era of Ben Ali where monitoring was done without anyone knowing who practised it," Moez Chakchouk, head of the Tunisian ATI, told IBTimes⁸ in late February.

Following the ousting of Ben Ali, the ATI has been assisting the judiciary in investigating internet-based crimes, after receiving court requests.⁹ This is despite the fact that there is no legal text that requires the ATI to do so. "We don't have any constraints but we try to help the court solve some cases, keeping a minimum surveillance," the ATI's chief said at the Freedom Online Conference in Tunis in June 2013.

On the other hand, the Interior Ministry has carried on with its phone tapping practices, though on a lesser scale.¹⁰ Today, surveillance of phone

communications takes place only "after receiving written orders from investigative judges or the State prosecutor" and previous practices of tapping into activists and politicians' phones were scrapped, the ministry was quoted as saying by *African Manager* in May 2013.

Despite the entry into force of Decree 4506 and the establishment of the ATT, the ministry's monitoring of telephone communications is not coming to an end soon.

"Under the decree, telephone tapping lies in the ATT's field of intervention," Jamel Zenkri, ATT's general director, told the local magazine Webdo. "However, right now, at least for this year, we cannot do it" due to "equipment problems," he explained.¹¹

The ATT may well indeed fill a legal and institutional vacuum. However, with its multiple loopholes, Decree 4506 fails to uphold international standards and principles on the application of human rights to communications surveillance,¹² in doing so threatening user rights.

- The decree does not make any reference to the principles of *legality*, *legitimacy*, *necessity*, *adequacy* and *proportionality* on communications surveillance.
- At no point does the decree state that individuals should be *notified* of the surveillance of their communications. In addition, there is no independent authority to which data subjects may resort whenever they fear that processing of their personal data is overriding their fundamental rights and freedoms. The decree also does not state that data subjects may be able to file complaints against the ATT.
- The decree's vague language represents a threat to citizens' rights to privacy and free expression. For instance, article 2 tasks the ATT with "providing technical support for judicial investigations into ICT-related crimes" without defining these crimes. The decree further mentions the "legislation in effect" on several occasions, without specifying the legislation in question. With Tunisia's numerous repressive laws which criminalise certain types of free speech, such as "defamation" and content "harming good morals and public order", there are concerns that users might risk being put under surveillance for merely expressing themselves.

¹ Silver, B. (2011, December 13). Post-Revolt Tunisia Can Alter E-Mail With 'Big Brother' Software. *Bloomberg*. www.bloomberg.com/news/2011-12-12/tunisia-after-revolt-can-alter-e-mails-with-big-brother-software.html

² Alchourouk. (2013, February 23). Interior Minister Lotfi Ben Jeddou in a long interview with Alchourouk: We defeated terrorism and a soonish resolution in Chaambi. *Alchourouk.com*. bit.ly/1eKVuhs

³ youtu.be/ZE6HQXmDTGY?t=23m49s

⁴ Sfaki, B. (2014, April 4). 1,800 Tunisians Fighting in Syria, Says Ministry of Interior. *Tunisia Live*. www.tunisia-live.net/2014/04/04/1800-tunisians-fighting-in-syria-says-ministry-of-interior

⁵ Ministry of Information and Communications Technologies. (2013). Décret n°2013-4506 du 6 novembre 2013, relatif à la création de l'agence technique des télécommunications et fixant son organisation administrative, financière et les modalités de son fonctionnement. [Decree n°2013-4506 related to the creation of the Technical Telecommunications Agency and determining its administrative and financial organization and methods of functioning]. www.mincom.tn/fileadmin/templates/PDF/juridiques/D2013-4506.pdf

⁶ Amara, T., & Karouny, M. (2011, March 7). Tunisia names new government, scraps secret police. *Reuters*. www.reuters.com/article/2011/03/07/us-tunisia-government-idUSTRE7264A220110307

⁷ Naffati, W. (2014, January 3). Le ministère de l'Intérieur n'aura plus l'accès direct aux réseaux pour les écoutes téléphoniques. [The Interior Ministry will no longer have direct access to networks for phone-tapping]. *Tunisie Haut Débit*. www.thd.tn/index.php?option=com_content&view=article&id=3777:le-ministere-de-l-interieur-n-aura-plus-l-acces-direct-aux-reseaux-pour-les-ecoutes-telephoniques&catid=64:fixanmobile&Itemid=361

⁸ Stevenson, T. (2014, February 26). NSA-Style: Tunisia Setting Up Counterterrorism Unit That Will Also Spy On Citizens. *International Business Times*. www.ibtimes.com/nsa-style-tunisia-setting-counterterrorism-unit-will-also-spy-citizens-1558013

⁹ Khelifi, R. (2013, June 18). Tunisian Internet Agency CEO: Lack of Legal Reforms Imperils Internet Freedom in Tunisia. *Tunisia Live*. www.tunisia-live.net/2013/06/18/chakchouk-lack-of-legal-reforms-imperils-internet-freedom-in-tunisia

¹⁰ African Manager. (2013, May 12). Tunis : Les écoutes téléphoniques existent toujours, juste derrière le ministère de l'intérieur. [Phone-tapping still exists, just at the interior ministry]. *africanmanager.com*. www.africanmanager.com/150744.html

¹¹ Webdo. (2014, June 4). Jamel Zenkri, DG de l'AT des Télécommunications: "la censure n'est nullement envisagée" (3/3) [Jamel Zenkri, general director of ATT: "Censorship is by no means an intention"]. *webdo.tn*. www.webdo.tn/2014/06/09/jamel-zenkri-dg-lat-telecommunications-censure-nest-nullement-envisagee-33/

¹² en.necessaryandproportionate.org/text

- Decree 4506 states that the ATT provides “technical support for judicial investigations” into ICT crimes. It is also tasked with “receiving and treating orders from the judicial authority to investigate and record ICT-related crimes in accordance with the legislation in effect.” However, the decree’s language does not ensure *independent judicial control of communications surveillance* but rather attributes too many prerogatives to the Ministry of Information and Communications Technologies. The decree establishes the ATT as a “public entity of an administrative nature” under the aegis of the Ministry of ICTs. Under article 12, the ministry is tasked with appointing the agency’s general-director and department directors. Besides this, the agency is required to carry out “any other mission linked to its activity that it is assigned by the Ministry of Information and Communications Technology” (article 5). This means that the ICT ministry could be involved in issuing surveillance requests.
- The lack of *independent oversight mechanisms* is also a cause for concern. Decree 4506 establishes an “oversight committee” to “ensure the proper functioning of the national systems for controlling telecommunications traffic in the framework of the protection of personal data and civil liberties.” However, the role of this committee remains unclear. Its board is presided by the ATT’s general-director and dominated by representatives from the government ministries of defence, interior, ICTs, justice and human rights, which strips it of the required neutrality to carry out any supervisory role.
- Decree 4506 does not put in place *transparency mechanisms* which would reveal to the public the scope of the agency’s activities. Article 5 only tasks the agency’s general-director with drafting annual reports to be submitted to the ICT ministry.

With so many loopholes, the ATT could easily violate citizens’ rights, especially without an independent data protection authority which could act as a guarantee against unchecked and indiscriminate surveillance.

Tunisia does have a data protection authority, the National Authority for the Protection of Personal Data (INPDP), established under the Personal Data Protection Law of 26 July 2004. Established in an era of mass surveillance, the authority was marginalised and its role was only nominal. As interim authorities continue to disregard legal reforms which would guarantee the authority’s

independence from government interference and consolidate its prerogatives, the INPDP remains powerless.

Under article 78 of the 2004 Personal Data Protection Law, the INPDP is made up of two members of parliament and government representatives from the prime minister’s office and the defence, interior, scientific research, health and ICT ministries.

The same law makes state authorities exempt from the supervision of and accountability to the INPDP. For instance, state bodies are not required to notify the INPDP or obtain the “explicit and written approval” of data subjects before processing their personal data. Data subjects also cannot file objections on state authorities’ processing of their data to the INPDP.

In 2012 the INPDP announced that it was planning to submit draft amendments¹³ to the 2004 privacy law to the National Constituent Assembly (NCA). To date, the assembly is yet to debate, let alone adopt, these amendments, which the government does not consider as “an urgent priority,”¹⁴ the authority’s head told Index on Censorship last January.

In addition to a powerless data protection authority incapable of supervising the country’s new Big Brother, the surveillance laws¹⁵ inherited from the dictatorship era, which to this date remain on the books, are worrisome. For instance, Decree 97-501 of 14 March 1997 concerning value-added telecommunications services and the Regulations of 22 March 1997 concerning the specifications for setting up and operating value-added internet telecommunications services make internet service providers (ISPs) liable for third-party content, binding them to monitor and take down objectionable content.

Under articles 8 and 9 of the Internet Regulations, ISPs are further required to submit lists of their subscribers to the authorities on a monthly basis and to retain archives of content for up to one year. Article 14 of the 2001 Telecommunications Code requires telecom networks operators to submit a list containing the names, phone numbers and addresses of their subscribers with the exception of those “explicitly refusing the publication” of their

details. Article 87 of the same code bans the use of encryption technologies without the authorities’ authorisation.

Conclusions

There is no doubt that a cyber-crime surveillance body is needed for any country to fight serious crimes such as child pornography, fraud and cyber terrorism. However, the creation of such an agency requires deep reflection and the participation of all stakeholders, in particular civil society.

Tunisia’s setting up of the ATT was a hasty step. The government created the agency by decree and not by law, which would require a debate at and the approval of the constituent assembly.

In addition, the authorities did not put in place effective and sufficient mechanisms and measures to ensure that any interference with citizens’ communications upholds international standards and does not infringe on their rights. “Communications surveillance should be regarded as a highly intrusive act that potentially interferes with the rights to freedom of expression and privacy and threatens the foundations of a democratic society,”¹⁶ states a report delivered last year by the United Nations Special Rapporteur on freedom of expression and opinion in the wake of the revelations about the US National Security Agency (NSA).

In a statement published on 20 November 2013, the ICT ministry asserted that Decree 4506 does include a “set of guarantees” to “consolidate respect for human rights, personal data protection, freedom of expression on the internet and the right to access information.” Yet an analysis¹⁷ of the decree proves the exact opposite. Vague language and a lack of oversight mechanisms, transparency and independent judicial control are all menacing Tunisians’ rights to privacy and free expression.

Action steps

In late January 2014, Tunisia’s National Constituent Assembly adopted a constitution guaranteeing privacy rights. Article 24 of the document states that “the state protects the right to privacy, the sanctity of domiciles, the confidentiality of correspondence and communications, and personal data.”

However, these constitutional provisions are pointless as long as the authorities do not initiate serious reforms on communications surveillance.

Before rushing to establish a new spying agency, Tunisia’s authorities should have first enacted much-needed privacy reforms including:

- Amending the 2004 privacy law to consolidate the role of the INPDP as the country’s data protection authority and ensure that the processing and collection of personal data by state authorities does not go unchecked and unaccountable.
- Abolishing or amending Ben Ali-era surveillance laws.
- Abolishing all laws that criminalise free speech, in particular those that criminalise free speech through ICTs, namely article 86 of the Telecommunication Code, which punishes by up to two years imprisonment anyone convicted of “insulting and disrupting the lives of others through public communications networks.”
- Signing the Council of Europe’s Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.¹⁸

Though most of the reforms suggested above can only see daylight after a constitutional court is in place and only once legislative and presidential elections due later this year are held, to cut with the abuses of the past, political willingness is equally essential.

¹³ Abrougui, A. (2012, August 15). New-era privacy law drafted to protect Tunisians from the surveillance state. *Index on Censorship*. uncut.indexoncensorship.org/2012/08/tunisia-drafts-new-era-privacy-law

¹⁴ Abrougui, A. (2014, January 2). Tunisians cast a wary eye on new crime agency. *Index on Censorship*. www.indexoncensorship.org/2014/01/tunisians-cast-a-wary-eye-on-att/

¹⁵ Article 19. (2013). *Tunisia: Background paper on Internet regulation*. www.article19.org/resources.php/resource/37135/en/tunisia-background-paper-on-internet-regulation

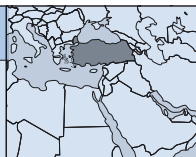
¹⁶ Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, to the 23rd session of the UN Human Rights Council, 17 April 2013. www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf

¹⁷ Reporters Without Borders. (2013, December 2). Authorities urged to rescind decree creating communications surveillance agency. *Reporters Without Borders*. en.rsf.org/tunisia-authorities-urged-to-rescind-02-12-2013,45531.html

¹⁸ Council of Europe. (2008). Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. conventions.coe.int/Treaty/en/Treaties/Html/108.htm

TURKEY

So you want a surveillance state?



Evin Barış Altıntaş

Introduction

In May 2010, the leader of Turkey's main opposition party, the Republican People's Party (CHP), resigned after footage showing him intimately involved with a deputy of his party was published.¹ One year later, in May 2011, there was another sex-tape scandal, at the end of which ten deputies of the Nationalist Movement Party (MHP) had to resign.² No serious investigation was carried out into who was responsible for the recordings, and Turkish politics has since been shaped by legally or illegally obtained recordings, wiretapped phone conversations or intercepted electronic communications. Four years after Deniz Baykal's resignation, a model gave an interview to a government-friendly newspaper³ regarding allegations that a gang that eavesdropped on the country's prime minister also monitored her communications. She was furious, but not because she felt violated; rather, because the violation had come from what she believed to be an unauthorised authority. She said: "Only official agencies can eavesdrop on me when they deem necessary." She was reciting the Turkish government's newest narrative.

Policy and political background

"If you do nothing wrong, if you have no illegal business, don't be afraid of wiretapping," Binali Yıldırım, who was at the time minister of transportation and communication, told Parliament in 2009.⁴

Five years later, the Justice and Development Party (AKP) government would pass law after law to grant state intelligence units nearly unlimited powers of surveillance with little accountability or oversight over how they are used.⁵ Ironically, the AKP government has become the victim of a major wiretapping scandal⁶ itself, which has revealed alleged government corruption. What makes the issue even more convoluted is that some in the overly polarised country claim that the voice recordings on AKP were obtained through court warrants, although the government alleges their illegality. Against this political backdrop, the citizenry remains mainly apathetic to, if not supportive of, the creation of what has been described as a "complete security apparatus" to control the population.⁷

A tale of many surveillance centres

Turkey's recent political history makes it clear there is a tape on everyone that can be leaked at the opportune moment, and the perpetrators usually do not have to suffer any legal consequences regarding privacy violations. Turkey's recent attempted coup trials, publicly known as the Sledgehammer and Ergenekon trials,⁸ in which hundreds of high-ranking military officials as well as civilians stood trial on charges of attempting to overthrow the AKP government, have shown that there are no secrets in this new era; not even personal ones. During the course of the investigation some of their highly private conversations were also leaked to the media. However, these cases have not led to a public debate over the current legislation on privacy and rights violations.

Another major wiretapping scandal broke after 17 December 2013 when prosecutors made public a major graft investigation that reached the government and Prime Minister Recep Tayyip Erdoğan's inner circle.⁹ In March of this year, voice recordings purportedly obtained during the course of the graft investigation were released on Twitter by a user account, which has since been withheld in Turkey by Twitter.¹⁰ The recordings allegedly featured the voices of some ministers, businessmen close to the AKP government, as well as several alleged conversations between Erdoğan and his son Bilal Erdoğan, in which the two spoke about hiding large amounts of cash in their home.¹¹ In response to the corruption investigation and the leaks, the government has carried out purges in the police force and the judiciary and public agencies.¹² It has claimed that what Erdoğan calls a "parallel organisation" – which it associates with its former political ally, the religious-minded social movement Hizmet, inspired by the Islamic preacher Fethullah Gülen, and which has been able to expand its presence in the country's police force and other state agencies with the support of the AKP – was behind the corruption allegations in a plot against his government. Later on, it emerged that some of the recordings leaked were based on court warrants, but the government so far has been able to effectively stonewall the graft probe.

As part of its efforts to exert more control over the internet, the AKP government has also amended Turkey's Law No. 5651 on the Regulation of Internet Publications and Prevention of Crimes Committed through these Publications.¹³ The amendments were found to be a violation of free speech, and criticised both domestically and internationally.¹⁴

Initially, the amendments had sought to oblige all access providers to form a union in order to be able to operate in the country, and to store the traffic and browsing data of users for a two-year period, to be shared with state authorities upon court orders or administrative requests. However, this was later repealed and the law was amended to limit data storage by access providers strictly to communications traffic when there are street protests.

However, more internet restrictions were to follow. In response to the graft scandal, the AKP banned Twitter in March 2014. Twitter had already angered Prime Minister Erdoğan, who has publicly expressed his dislike of the social media platform many times for its role during the 2013 anti-government Gezi protests. In fact, several Gezi protesters were detained over posts shared on their personal Twitter or Facebook accounts.¹⁵ Some analysts said the amendments followed by the Twitter ban are indicative of further rights violations to come.¹⁶ And they were proven right. In less than a month after the Twitter ban, the government banned access to YouTube through the Telecommunications Authority (TİB). YouTube was banned after another leak, this time of a high-level secret meeting between the state's top security officials recorded at the Foreign Ministry building, in which the speakers spoke about starting a war with Syria. The access ban could only be lifted through a Constitutional Court order,¹⁷ an action which Erdoğan criticised as being "unpatriotic". Lower court orders to lift both the Twitter and YouTube bans were earlier ignored by TİB. To date, the perpetrator of the security summit leak still has not been found, although the government has accused, with no evidence, the aforementioned parallel structure of being behind it.

Users were able to circumvent the YouTube and Twitter bans through DNS server changes, and later via virtual private networks (VPNs), as there were reports that the user-changed DNS servers were intercepted by Turkish internet service providers

1 (2010, May 11). CHP leader Baykal resigns. *Today's Zaman*. www.todayszaman.com/tz-web/news-209896-103-chp-leader-baykal-resigns-puts-blame-on-ruling-party.html

2 Hurriyet Daily News. (2011, May 22). Turkish politics tainted by sex tape conspiracy. *Hurriyet Daily News*. www.hurriyetdailynews.com/default.aspx?pageid=438&n=turkish-politics-tainted-by-sex-tape-conspiracy-2011-05-22

3 Yazdir, H. (2014, June 15). Turkiye baronlar tarafından hortulanacakti (Barons were going to drain out Turkey's wealth). *Yeni Şafak*. yenisafak.com.tr/pazar-haber/turkiye-baronlar-tarafindan-hortulanacakti-15.06.2014-658542

4 Korkmaz, O. (2014, February 27). Why fear wiretapping if you have no illegal business? *Hurriyet Daily News*. www.hurriyetdailynews.com/why-fear-wiretapping-if-you-have-no-illegal-business.aspx?pageID=449&nID=62975&NewsCatID=497

5 Jones, D. (2014, April 18). Turkish law gives spy agency controversial powers. *Voice of America*. www.voanews.com/content/turkish-law-gives-spy-agency-controversial-powers/1896418.html

6 DW. (2014, March 21). Erdogan defies quagmire of scandal in Turkey. *DW*. www.dw.de/erdogan-defies-quagmire-of-scandal-in-turkey/a-17511672

7 Smith, D. (2014, April 26). New Law In Turkey Expands Surveillance State And Cracks Down On Journalists. *Jonathon Turley*. jonathanturley.org/2014/04/26/new-law-in-turkey-expands-surveillance-state-and-cracks-down-on-journalists/

8 Tisdall, S. (2012, September 25). Turkey's Sledgehammer Coup verdict: justice or Soviet-style show trial? *The Guardian*. www.theguardian.com/world/2012/sep/25/turkey-sledgehammer-coup-trial-verdict

9 Today's Zaman (2014, February 16). Chronology of Dec. 17: The stones are settling into place... *Today's Zaman*. www.todayszaman.com/news-339508-chronology-of-dec-17-the-stones-are-settling-into-place-.html

10 Today's Zaman. (2014, April 20). Twitter freezes two accounts. *Today's Zaman*. www.todayszaman.com/news-345673-twitter-freezes-two-accounts-after-meeting-with-officials.html

11 An English translation of the transcript can be found at: www.liveleak.com/view?i=9f6_1393289511

12 Üstütağ, G. (2014, June 14). Erdoğan's witch hunt turns key state institutions upside down. *Today's Zaman*. www.todayszaman.com/news-350367-erdogans-witch-hunt-turns-key-state-institutions-upside-down.html

13 Euronews. (2014, February 18). Turkey's controversial internet law gets presidential approval. *Euronews*. www.euronews.com/2014/02/19/turkey-s-controversial-internet-law-gets-presidential-approval

14 Today's Zaman. (2014, February 25). Amnesty criticizes internet law, treatment of journalists in Turkey. *Today's Zaman*. www.todayszaman.com/news-339334-amnesty-international-criticizes-internet-law-treatment-of-journalists-in-turkey.html; Uras, U. (2014, February 25). New internet law in Turkey sparks outrage. *Al-Jazeera*. www.aljazeera.com/indepth/features/2014/02/new-internet-law-turkey-sparks-outrage-201422312144687859.html. For a legal analysis on the potential dangers of the law, see: www.thelawyer.com/analysis/opinion/turkeys-new-internet-law-increases-state-control/3016906.article

15 Today's Zaman. (2014, February 24). Gezi protests' Twitter suspects demand Erdoğan testify as victim. *Today's Zaman*. www.todayszaman.com/news-340332-gezi-protests-twitter-suspects-demand-erdogan-testify-as-victim.html

16 Andrew Gardner, Amnesty International (AI) researcher on Turkey, has said of the Twitter ban: "It is very indicative of how policy is made in Turkey and how rights are violated. I think this is going to have long-term implications." Today's Zaman. (2014, March 25). Government toughens war on Twitter, bans more sites. *Today's Zaman*. www.todayszaman.com/news-343039-government-toughens-war-on-twitter-bans-more-sites.html

17 Al-Jazeera. (2014, May 29). Turkey's top court rejects YouTube ban. *Al-Jazeera*. www.aljazeera.com/news/middleeast/2014/05/turkey-top-court-rejects-youtube-ban-2014529195032711672.html

(ISPs),¹⁸ a further rights violation, if the allegations are true.

Recently, hundreds of police officers who have participated in the graft investigation into the government have also been detained on espionage charges.¹⁹

These developments have deepened polarisation in society, making it easier for the increasingly draconian surveillance laws to find acceptance. The AKP has also been able to retain its votes in the 30 March local elections²⁰ and later have its presidential candidate, none other than Prime Minister Erdoğan himself, get elected in the first round of the country's first-ever popular presidential election on 10 August, in spite of serious graft allegations, harsher internet controls, and Orwellian powers being granted to the country's spy agency.

Conclusions

Internet users and the global public are increasingly more sensitive about unchecked government surveillance, particularly following Edward Snowden's revelations about the extent of US National Security Agency (NSA) surveillance – which was not a secret for many concerned with surveillance²¹ prior to Snowden's leaks. Now world governments seem to be finding ever more intrusive ways of intercepting communications. Globally, we can forget about privacy.

However, the situation in Turkey seems to be more alarming, as there is little public discussion on the effects of unchecked surveillance. To the contrary, an overwhelming majority of the public seems to be content with the stricter powers of the government, if the outcomes of the two recent elections are any indication. Debate on how to protect citizens from unnecessary and unchecked government surveillance has taken place in Turkey, but only among civil society groups, rights organisations and academics. International bodies, including the European Union (EU), have reacted to Turkey's stricter surveillance laws, but these have had little effect on the government's plans to centralise surveillance powers.

In addition to this depressing milieu, it should be noted that in some of the ongoing wiretapping cases, it is not yet clear who has done the eavesdropping. Although legally the telecoms body TİB has the right to wiretap phone lines based on court orders, intelligence units of the police force and the gendarmerie also have some technical capabilities to monitor communications, although the extent of these capabilities is debated.²² Jurists and lawyers have offered different interpretations as to what is legal, usually depending on their political stance and level of partisanship. Ambiguity concerning who is authorised to monitor real-life or electronic communications in Turkey is a direct consequence of the increasing polarisation, which helps the administration justify and acquire consent for going after “parallel structures”, or other imagined enemies, to consolidate Erdoğan's supporters.

History has shown time and again that even the most democratic government will abuse widespread surveillance powers if it has them. In the Turkish case, the unchecked access to the personal data of citizens for what some say are “warring factions” nested within the state hierarchy makes the issue even more complicated. It is very difficult at this time to pinpoint the perpetrators of warrantless wiretapping. Certainly, there are many challenges of attempting to maintain control over the population;²³ however, there is no indication as of yet that challenges from political groups might actually work against the government in the end. Currently, political opposition, human rights groups and generally disadvantaged groups are extremely distressed about Turkey's descent into a police or surveillance state. However, systematic rights violations are undeniably a major threat to everyone, including the members of the majority. Another potential victim of unchecked state surveillance are the power holders, a fact that the AKP government has seen first-hand already.

Action steps

Turkish civil society organisations have been even more active than before about reminding users of their rights to privacy and raising their voices against internet surveillance and monitoring. For example, in 2012, the Chamber of Computer Engineers (BMO) released a comprehensive User Rights Manifesto²⁴ backed by eight organisations including professional chambers, anti-censorship and internet rights groups. However, these efforts have had little outreach, given the politically tense situation in the country. Activists should continue their efforts in creating awareness on state surveillance, but perhaps make certain modifications:

- Street protests against internet censorship are increasingly seen as anti-government actions in Turkey. Organisations should find ways to communicate with parts of society that are sceptical of groups that they associate with the Gezi protests.
- All civil society organisations must find a way to convince the AKP administration to reduce the political polarisation in the country. Hostility among a divided public breeds less transparency, which in turn facilitates unlawful or legal but unnecessary state surveillance.
- Educational institutions at all levels should make internet freedoms a part of their curricula and teaching programmes.

- All civil society organisations, even if they are not in the field of technology or communications freedoms, should treat internet liberties as a basic human right and include this freedom in their wider agenda. Rights activists should focus on communicating with civil society groups from other fields.
- Although independent media and journalist freedoms are increasingly threatened in Turkey,²⁵ journalists should be braver and more outspoken on the subject of state surveillance.
- The international community has been extremely critical of Turkey's increasingly dictatorial expansion of surveillance laws. It might be helpful if international bodies and organisations such as the Organization for Security and Co-operation in Europe (OSCE), the UN or the EU also concentrated on reaching out to the majority that seems to approve of the government's surveillance policies.

Fighting for democracy and transparency in times of political repression takes not only courage but innovation and reinventing ideas to make sure that the public understands that dissenters and government critics are not the country's enemies. Populist authoritarianism can be defeated only by gaining the support of government supporters, not antagonising them.

¹⁸ Statement from Google: Turkish ISPs block access to Google DNS servers (in Turkish), T24 website, 31 March 2014. t24.com.tr/haber/google-dnsleri-turk-servis-saglayicilar-engelliyor,254845

¹⁹ AP story on what is known as the “July 22 Operation” in Turkey: Fraser, S. (2014, July 22). Turkey detains police for ‘spying’ and wiretaps. *AP*. bigstory.ap.org/article/turkey-police-involved-graft-probe-detained

²⁰ The Economist. (2014, April 5). Erdoğan on a roll. *The Economist*. www.economist.com/news/europe/21600161-ak-party-wins-convincingly-what-next-erdogan-roll

²¹ Unseen.org founder Chris Kitze interview with RT: https://www.youtube.com/watch?v=CvMiKT4R_Fo#t=20

²² One of the former police chiefs accused of spying on the government claims it is technically impossible for the police force to eavesdrop on the encrypted phone lines of the prime ministry, although the prosecution – which has the blessing of the AKP government – claims that this was exactly what the police officers have done. Interview with Yakub Saygılı: Akman, N. (2014, August 11). ‘I’m ready to serve many years in prison if what I did was illegal’. *Today's Zaman*. www.todayszaman.com/interviews_im-ready-to-serve-many-years-in-prison-if-what-i-did-was-illegal_355343.html

²³ Darren Smith notes that “maintaining a complete security apparatus in controlling a population is expensive in terms of resources, money, and political backing.” Smith, D. (2014, April 26). Op. cit.

²⁴ BMO Manifesto, in Turkish: www.bmo.org.tr/2012/04/18/internet-kullanici-haklari-bildirgesi-yayinlandi

²⁵ Kramer, D., Robbins, C., & Schenkkan, N. (2014). *Democracy in Crisis: Corruption, Media, and Power in Turkey*. Washington, DC: Freedom House. www.freedomhouse.org/sites/default/files/Turkey%20Report%20-%20Feb%202014.pdf

UGANDA

Gender dynamics need to be addressed in communications surveillance in Uganda



Women of Uganda Network (WOUGNET)

Dorothy Okello, Cleopatra Kanyunyuzi
and Winnie Mbabazi
www.wougnet.org

Introduction

In 2000, Uganda was recognised as one of the most liberal telecommunications markets in Africa and one in which the number of mobile subscribers exceeded fixed-line subscribers.¹ By 2013, it was estimated that 39% of Ugandans were using mobile phones, and 17% were daily users of the internet – primarily accessing the internet via mobile devices.²

Uganda is a landlocked country in East Africa with an estimated population of 35.4 million.³ Females represent 49.9% of the population, while 49% of the population is 14 years old or younger.⁴ This means that while Uganda's population is fairly balanced by gender, it is also a very young population with a potential affinity for the use of information and communications technologies (ICTs). Uganda has an ICT Development Index (IDI) score of 1.81, which is below the world average IDI of 4.35.⁵ IDI is a reflection of three ICT development drivers, namely, infrastructure and access to ICTs, level of ICT use in the society, and impact resulting from efficient and effective ICT use.

Policy and political background

Uganda has witnessed tremendous growth in the ICT sector, with the expansion of ICT applications and services including information generation and dissemination, mobile money, and innovative mobile apps – particularly in the agriculture and health sectors. The ICT policy and regulatory environment has also evolved from a focus on promoting widespread

access of ICTs to a focus on management of computer/mobile usage and internet freedoms. Examples of Uganda's ICT policies and regulations include the National ICT Policy (2003), Access to Information Act (2005), National Information Technology Authority Uganda Act (2009), Regulation of Interception of Communications Act (2010), Electronic Signatures Act (2010), Computer Misuse Act (2011), Electronic Transactions Act (2011), and Uganda Communications Commission Act (2013).

Other acts that have implications on ICT usage and surveillance include the Anti-Terrorism Act (2002), which gives security officers powers to intercept the communications of a person suspected of terrorist activities and to keep such persons under surveillance; the Anti-Homosexuality Act (2014), which outlaws the use of “electronic devices which include internet, films, and mobile phones for purposes of homosexuality or promoting homosexuality”; and the Anti-Pornography Act (2014), which mandates a Pornography Control Committee to “expedite the development or acquisition and installation of effective protective software in electronic equipment such as computers, mobile phones and televisions for the detection and suppression of pornography.”⁶ The Uganda Communications Commission is also to conduct a study with a view to ensuring “responsible use of social media and the internet” through regulation of social media content and internet usage.⁷

Communications surveillance in Uganda: Cause for concern?

In March 2014, the media in Uganda were flooded with stories of the fate of the country's prime minister, Amama Mbabazi. According to one newspaper, an opposition politician was noted as having remarked how the prime minister “seems to be the first victim of a repressive law that clearly violated the right to privacy.”⁸ The comments arose when pri-

vate conversations between the prime minister and his wife that had been allegedly secretly recorded were played back at a caucus meeting of the ruling party to which the prime minister belongs. The “repressive law” was the Regulation of Interception of Communications Act (RIC Act, 2010) which had been tabled as a bill to the ruling party caucus by Mbabazi himself while he was security minister in 2007. The RIC Act provides for “lawful interception and monitoring of certain communications in the course of their transmission through a telecommunication, postal or any other related service or system in Uganda.”⁹

It should be noted that the Constitution of the Republic of Uganda 1995 under Article 27 states that “[n]o person shall be subjected to unlawful search of the person, home or other property of that person; or unlawful entry by others of the premises of that person,” and that “[n]o person shall be subjected to interference with the privacy of his home, correspondence, communications or other property.”¹⁰ Furthermore, Article 29(1)(a) states that “every person shall have the right to freedom of expression and speech which includes freedom of the press and other media.” In the absence of a data protection authority, complaints that arise out of issues concerning the abuse of privacy are currently handled by the Uganda Human Rights Commission (UHRC).¹¹

The incident involving the prime minister highlights why there is growing concern over the governance and regulation of communication surveillance, and how it is being used to infringe on one's right to privacy in Uganda. Because this case affected a high-ranking Ugandan official, the question is, how safe is the ordinary Ugandan? And from a gender activist perspective, what are the gender concerns in the emerging policy and regulatory environment? Two recent studies on internet freedoms in Uganda were conducted by Unwanted Witness and Collaboration on International ICT Policy in East and Southern Africa (CIPESA). While both studies review the communications surveillance environment in Uganda, there is no specific focus on issues of concern by gender. However, both studies did raise various concerns that are relevant to women's use of the internet and social media.

Enforced under the RIC Act, the mandatory subscriber identity module (SIM) card registration, with a deadline of August 2013, is reported to have increased the opportunity for citizens to be subject to secret surveillance and had a chilling effect on free speech online.¹² In May 2014, an official from the Ugandan police's Electronic Counter Measures Department noted that while collection, storage and sharing of users' data through lawful means is for ensuring citizens' safety, the use of the SIM card registration records had not been that effective.¹³ This was because some SIMs are not yet registered or are only partially registered with alias names such as “gxp”. As such, it makes it hard for the Ugandan police to track down some offenders using SIM card records.

As noted by the media platform Unwanted Witness, without a data protection law in place, Ugandans are not only exposed to surveillance by the state but by anyone who can influence workers at telecom companies.¹⁴ This was evident in the number of reported court hearings where phone call printouts have been presented as criminalising evidence to convict alleged offenders without questioning the processes under which such information was acquired. In addition, anecdotal evidence seems to suggest that it is easier for males to obtain call records when tracking suspected infidelity of their spouses. This would be in line with cultural traditions that permit polygamy, but absolutely object to any “infidelity” on the part of females.

Another key issue, raised by the CIPESA report, was that knowledge and skills about threats to online safety appeared to be widely lacking, including amongst bloggers, journalists and activists that regularly used the internet.¹⁵ As stated in the report, “many online users were prone to attacks and hacks into their private communication due to the lack of requisite skills to secure their communication and information. Similarly, there seemed to be a general lack of knowledge on what constituted online freedoms and what was needed to protect and to promote them. This partly explained why there were few conversations on internet freedoms in the East Africa region. A final plank in the deficiency in knowledge and skills was related to online ethics among internet users.” It is widely known that women's ICT skills significantly lag behind those of men,

1 International Telecommunication Union. (2001). *The Internet in an African LDC: Uganda Case Study*. www.itu.int/ITU-D/ict/cs/uganda/uganda.html

2 Unwanted Witness. (2014). *The Internet: They are coming for it too!* www.unwantedwitness.or.ug/wp-content/uploads/2014/01/internet-they-are-coming-for-it-too.pdf

3 Uganda Bureau of Statistics. (2013). 2013 Statistical Abstract. www.ubos.org/onlinefiles/uploads/ubos/pdf%20documents/abstracts/Statistical%20Abstract%202013.pdf

4 World Bank Database: Uganda. www.worldbank.org/en/country/uganda

5 International Telecommunication Union. (2013). *Measuring the Information Society 2013*. www.itu.int/en/ITU-D/Statistics/Pages/publications/mis2013.aspx

6 CIPESA. (2014). *State of Internet Freedoms in East Africa 2014: An Investigation Into The Policies And Practices Defining Internet Freedom in East Africa*. www.cipesa.org/?wpfb_dl=76

7 Lule, J. A. (2014, May 12). UCC to control internet, social media content. *New Vision*. www.newvision.co.ug/news/655459-ucc-to-control-internet-social-media-content.html

8 Kizza, B. (2014, March 5). Is Amama Mbabazi falling on his own sword? *The Observer*. www.facebook.com/ugandaobserver/posts/479565065499306

9 The Regulation of Interception of Communications Act, 2010. www.ulii.org/files/Regulations%20of%20Interception%20of%20Communications%20Act,%202010.pdf

10 Privacy International. (2006). *Legal Framework in Uganda: Constitutional privacy framework*. <https://www.privacyinternational.org/reports/uganda/i-legal-framework>

11 Ibid.

12 Unwanted Witness. (2014). Op. cit.

13 Remarks by an official from the Uganda Police's Electronic Counter Measures Department during the Internet Freedom Forum attended by WOUGNET on 23 May 2014, Kampala, Uganda.

14 Unwanted Witness. (2014). Op. cit.

15 CIPESA. (2014). Op. cit.

so a lack of knowledge and skills on online safety should be expected to follow a similar pattern.

While many Ugandans are not aware of the pending threats to the right to privacy, little if anything has been done to safeguard communication platforms to guarantee the freedoms of speech, expression, assembly and association online. For women in Uganda, these platforms are an essential tool to advocate for equality given the gender gap at the decision-making level. The internet is a vital resource offering a platform for women as well as men to express themselves and find valuable information.

As internet use continues to grow worldwide, the debate between greater cyber security and internet freedom is also expanding.¹⁶ Going online presents many opportunities and dangers because there are hackers, fraudsters and overzealous surveillance systems even while online forums present a place for people to express themselves, find useful information, and grow their businesses. Women are uniquely affected by ICT policy decisions as the internet presents a space and opportunity for women's greater involvement in society and the economy as a whole.¹⁷ Women are also distinctively at risk of abuse online. Because of this, women's organisations, especially those with expertise on ICT issues, need to be given an active role in national discussions regarding a balanced policy on cyber security and internet freedom.

It should also be acknowledged that the need for a balanced communications surveillance policy is within an environment where infrastructural, economic and cultural reasons also serve to constrain access to the internet for women. For instance, while 73% of Ugandans over the age of 15 can read or write at a basic level, 83% of men are literate compared to only 65% of women.¹⁸ Additional barriers include working infrastructure, physical mobility, and limited affordability.¹⁹ If women cannot access ICTs then they cannot utilise them. Indeed this situation typically attracts the question as to whether women should even be concerned about internet freedom matters given their limited access!

However, barriers to internet access coupled with excessive communication surveillance can only

serve to push women further away from inclusion when it comes to using ICTs. Anecdotal evidence reveals women who willingly give up access to ICTs so as to minimise potential domestic confrontations and violence. The small percentage of women who are able to access and utilise ICTs both online and offline have not been spared the negative effects of surveillance by the state or private individuals.

Currently, technology-related violence against women takes on a variety of forms such as cyber stalking, sexual harassment and unauthorised use, manipulation and dissemination of personal information – including photographs and videos.²⁰ Manipulation and intimidation of women through unauthorised use of personal information have been evident through leaked private photos in local tabloids, which is a clear violation of these women's rights to privacy as stated in the Access to Information Act. The Act contains the only statutory definition of privacy available in Uganda: “the right of a person to keep his or her matters and relationships secret.” This Act also provides that the right of access should not interfere with the right to privacy. Unfortunately, the fear of surveillance by either the state or private individuals further drives away or self-censors citizens from using ICTs online/offline to freely express themselves and be heard on issues that affect them politically, socially, economically and culturally.

Conclusions

Government agencies all over the world are increasing surveillance on their citizens due to perceived and real internal and external threats but, unfortunately, in the process they undeniably find themselves violating citizens' rights to privacy.²¹ Within the East African region, Uganda enacted its interception of communications law in 2010, Rwanda in 2013, and Ethiopia in 2009. Burundi's amended Code of Criminal Procedure 2013 provides for interception of communications, and Kenya's Intelligence Service Act 2010 also provides for interception.

At the same time, there is no question that the responsible development of communications surveillance and in general cyber security is necessary to protect women from cyber violence. However, the internet is also a useful tool for women to seek assistance and connect anonymously with various centres and organisations, for instance, those that assist survivors of violence against women (VAW). Anonymity is only achieved when users are confident that their actions are not being tracked, and that they can seek safety without fear of repudiation. Additionally, the

right to privacy online allows women to decide how they want to share their personal information through ICTs.²² Because of this there is a need for a balanced framework between communications surveillance and internet freedoms that protects women online, while not interfering with their ability to exercise their rights online. With a Gender Inequality Index score of 0.517 and ranked 110 out of 148 countries,²³ Uganda's rating is better than the sub-Saharan Africa average score of 0.577, but leaves plenty of room for concern on gender issues. Within the East African region, Rwanda fares best with an index score of 0.414 and a country ranking of 76.

For instance, without a data protection law to regulate the collection, storage and access to citizens' personal information, their security is endangered regardless if one is in public office or a private citizen, since this information can be accessed by anyone. A case in point is our key story in which a very high-profile public figure was not spared from surveillance that infringed upon his right to privacy. How much more, then, can be expected to happen to the ordinary Ugandan woman – with the aid of current cyber laws through which the government can control how digital freedoms should be exercised through surveillance?

As a topical issue, communications surveillance has attracted various reactions from different activists, stakeholders and experts at forums in Uganda, with some arguing that people give up their right to privacy once they go online. Others stress that self-censorship is the only way one can be assured of privacy and security online. Proponents for self-censorship argue that, even with data protection and privacy laws in place, it is difficult for the government to protect users once they enter cyber space due to the existence of third parties who also store users' information. However, others still insist that security/privacy, as ensured offline, should be available online. Proponents for online and offline privacy include those advocating for the amendment of oppressive sections in the laws that facilitate communications surveillance. Women's marginalisation in all these debates has also been discussed – notably at the national decision-making level. Even with fair gender representation, there is little or no input by women representatives in communications surveillance-related policies.

Action steps

Even while women may currently be limited in access to ICTs, they no less suffer various violations resulting from cyber crime and communications surveillance. There is a need for action steps to address the following:

- As civil society organisations advocate for government to uphold citizens' rights to freedom of expression, privacy and security, there is a need to acknowledge that in order to achieve a holistic approach to observing human rights offline and online, a balance between surveillance and freedom has to be achieved. If either is too extreme, it will lead to the abuse of human rights, in which women will be distinctly affected.
- There is a need for public sensitisation on privacy laws and citizen rights. The government, private sector and civil society should run awareness programmes so that when internet users come online they are aware of the pros and cons of the online environment.
- The right to freedom of expression should not be abused by ICT users online/offline. There is a need for public sensitisation on the rights and responsibilities that go along with internet freedoms.
- Individuals need to ensure that they stay safe online as much as they do offline. In particular, there is a need for awareness and capacity-building programmes for women on keeping safe online.
- There is a need for gender awareness and sensitisation for all actors in the communication surveillance space:
 - Civil society organisations need to advocate in a gender-sensitive manner for enactment of “safe” laws and amendment of laws that infringe on citizens' rights to privacy, freedom of expression and security both online and offline.
 - Publishers need to ensure that the information they post online and offline is factual, and that it does not perpetuate gender stereotypes or gender-based violence.
 - As the government enforces cyber security laws, the legitimate aim of protecting its citizens online and offline should be upheld with due consideration to gender concerns.
- There is a need for quantitative and qualitative research on women's knowledge, skills and reasons for going online in a context where communications surveillance is a reality. There is a need for studies on the effects and impacts of the prevailing online surveillance environment on women and their uptake of ICTs.

¹⁶ WOUUNET. (2014). *Cyber Infrastructure: A Women's Issue Too!*

¹⁷ Moawad, N. (2013). How does gender intersect with Internet governance. *Association for Progressive Communications*. <https://www.apc.org/en/node/18677>; Amuriat, G. Z., & Okello, D. (2005). Women on ICT Policy Making in Uganda. In F. Etta & L. Elder (Eds.), *At the Crossroads: ICT Policy Making in East Africa*. Kampala, Dar es Salaam and Ottawa: East African Educational Publishers Ltd., Ujuzi Educational Publishers Ltd. and the International Development Research Centre. web.idrc.ca/openbooks/219-8

¹⁸ UNESCO Institute of Statistics. Country Profiles: Uganda. www.uis.unesco.org/DataCentre/Pages/country-profile.aspx?regioncode=40540&code=UGA

¹⁹ WOUUNET. (2014). Op. cit.

²⁰ Moawad, N. (2013). Op. cit.

²¹ CIPEA. (2014). Op. cit.

²² Take Back the Tech! (2013, November 15). Public/private. *Define your line. Shape your space. Take Back the Tech! APCNews*. <https://www.apc.org/en/node/18739/>.

²³ UNDP. (2012). Gender Inequality Index. <https://data.undp.org/dataset/Table-4-Gender-Inequality-Index/pq34-nwq7>

UNITED KINGDOM

GCHQ: The NSA's Little Brother... not so little anymore



Open Rights Group

Javier Ruiz Diaz
www.openrightsgroup.org

Introduction

The documents leaked by the whistleblower Edward Snowden show that the United Kingdom (UK) is collecting information on millions of innocent citizens worldwide, in breach of human rights. British spies are also spreading malicious software, breaking internet security and carrying out attacks against protest groups, companies and other actors that are not terrorists or serious criminals.

So far the attention of most of the international media and public opinion has focused almost exclusively on the National Security Agency (NSA), the signals intelligence agency of the United States (US). But the NSA operates a global surveillance machine that relies on a network of key partners ranging from Israel to Sweden. First and foremost is its UK counterpart, the General Communications Headquarters (GCHQ).

It is important that civil society organisations throughout the world concerned about mass surveillance broaden the focus of their attention from the US and the NSA to include the UK and GCHQ.

Below we summarise some of the key activities of UK surveillance agencies exposed by Edward Snowden.

Beyond signals intelligence

Mastering the internet

But we are starting to “master” the Internet. And our current capability is quite impressive... We are in a Golden Age. (GCHQ internal document)¹

The activities of the UK's GCHQ are so inextricable from those of the NSA that from a certain perspective it makes little sense to treat them as separate entities. This cooperation started in earnest during the Second World War, and continued during the Cold War, with Britain providing forward listening stations in colonial outposts such as Hong Kong.

But the documents leaked by Snowden reveal many instances where the responsibilities of the UK can be clearly determined. For example, we know that GCHQ scoops the personal data of millions of innocent people around the world² by tapping into fibre optic cables that pass through Britain. This programme is called Tempora, and it is described in detail in the thematic report on the Five Eyes in this edition of GISWatch.

It is shocking that a private NSA contractor like Snowden had access to such an amount of information on British intelligence, and it is certainly not the full picture. Nevertheless, the leaks about GCHQ reveal an agency pursuing global domination of cyberspace by any means necessary.

Hacking private webcam conversations

Unfortunately ... it would appear that a surprising number of people use webcam conversations to show intimate parts of their body to the other person. (GCHQ internal document)³

The programme Optic Nerve involved tapping into the private webcam communications of innocent Yahoo subscribers and collecting millions of still images, including substantial amounts of explicitly sexual materials.⁴ The programme, apparently unknown to Yahoo, targeted 1.8 million unwitting users in a six-month period without any form of minimisation or filtering. The agency did this in order to improve their facial recognition capabilities, with the metadata and images being fed into the key NSA databases and its search engine, XKEYSCORE.

US senators have launched an investigation⁵ into Optic Nerve, accusing GCHQ of a “breathtaking lack of respect for privacy and civil liberties.” GCHQ

has simply provided a boilerplate response about compliance with UK laws.

Psychological operations against non-violent protest groups

[15:42] *“speakeasy” we’re being hit by a syn flood*⁶

[16:44] *“speakeasy” I didn’t know whether to quit last night, because of the ddos?* (Anonymous chat room log)⁸

GCHQ has moved from collecting “signals” and generating intelligence for other bodies, to proactive action,⁹ now representing 5% of GCHQ’s “business”.¹⁰ This action ranges¹¹ from psychological warfare, such as deleting a target’s online presence and spreading false information, to hacking and disabling target systems through denial of service (DOS) attacks.

A leaked catalogue of GCHQ hacking tools¹² shows that they built specific software for manipulating online communications and behaviour, not just collecting information. Among many others, these include tools to modify online polls, the popularity of YouTube videos, and traffic to specific websites.

It is particularly worrying that GCHQ considers as legitimate targets groups not involved in terrorism or serious crime, such as the “hacktivists” of Anonymous.¹³ Their chat rooms were shut down by GCHQ’s own hacking operations in 2011, called Rolling Thunder, with the effect of pushing away some 80% of visitors. GCHQ has also targeted supporters of Wikileaks,¹⁴ albeit in a less aggressive manner.

Industrial-scale hacking

GCHQ is a key partner in a joint system developed with the NSA capable of attacking millions of computers in a semi-automated process. Quantum¹⁵ is a collection of tools that turn the global listening apparatus of these agencies – dozens of both owned and hacked computers and routers in the heart of the internet backbone – into an active cyber weapon.

These are tools for hacking on an industrial scale. They analyse their target computers and automatically deliver tailored malware that allows the agencies to control computers, including the microphone and camera. These malware tools are sometimes distributed by creating fake Facebook or LinkedIn pages.

GCHQ’s own legal departments appear to have raised concerns about the legality of these techniques,¹⁶ which are directed not just against dangerous criminals, but in many cases innocent administrators of computers networks and international mobile operators.¹⁷ In a particularly scandalous case, GCHQ used these tools to hack into the systems of Belgian telecoms firm Belgacom.¹⁸

Weakening the internet

In order to make it possible for the NSA and GCHQ to break into thousands of computers, the agencies have been actively undermining fundamental security technologies, such as encryption systems. The UK has its own programme to weaken internet security called Edgheill.¹⁹

The revelations that UK and US security services have actively sought to lower the security of the internet as a whole for their own purposes have caused massive consternation²⁰ among the internet technical community. There are concerns that cyber

6 https://en.wikipedia.org/wiki/SYN_flood

7 https://en.wikipedia.org/wiki/Denial-of-service_attack

8 NBC News Investigations. (2014). *The Snowden files: British intelligence agency describes attack on Anonymous*. msnbcmedia.msn.com/i/msnbc/sections/news/snowden_anonymous_nbc_document.pdf

9 The Intercept. (2014, April 4). Full-spectrum cyber effects. *The Intercept*. <https://firstlook.org/theintercept/document/2014/04/04/full-spectrum-cyber-effects/>

10 NBC News Investigations. (2014). *The Snowden Files: British Spies Used Sex and ‘Dirty Tricks’*. msnbcmedia.msn.com/i/msnbc/sections/news/snowden_cyber_offensive2_nbc_document.pdf

11 NBC News Investigations. (2014). *The Snowden files: British Spies Used Sex and ‘Dirty Tricks’*. msnbcmedia.msn.com/i/msnbc/sections/news/snowden_cyber_offensive1_nbc_document.pdf

12 Greenwald, G. (2014, July 14). Hacking Online Polls and Other Ways British Spies Seek to Control the Internet. *The Intercept*. <https://firstlook.org/theintercept/2014/07/14/manipulating-online-polls-ways-british-spies-look-control-internet>

13 NBC News Investigations. (2014). *The Snowden files: British intelligence agency describes attack on Anonymous*. msnbcmedia.msn.com/i/msnbc/sections/news/snowden_anonymous_nbc_document.pdf

14 Greenwald, G., & Gallagher, R. (2014, February 18). Snowden Documents Reveal Covert Surveillance and Pressure Tactics Aimed at WikiLeaks and Its Supporters. *The Intercept*. <https://firstlook.org/theintercept/article/2014/02/18/snowden-docs-reveal-covert-surveillance-and-pressure-tactics-aimed-at-wikileaks-and-its-supporters>

15 cryptome.org/2013/12/nsa-quantum-tasking.pdf

16 Gallagher, R. J. (2013, December 12). GCHQ’s Dubious Role in The ‘Quantum’ Hacking Spy Tactic. *Ryan Gallagher*. notes.rjgallagher.co.uk/2013/12/gchq-quantum-hacking-surveillance-legality-nsa-sweden.html

17 Paterson, T. (2013, November 10). GCHQ used ‘Quantum Insert’ technique to set up fake LinkedIn pages and spy on mobile phone giants. *The Independent*. www.independent.co.uk/news/uk/home-news/gchq-used-quantum-insert-technique-to-set-up-fake-linkedin-pages-and-spy-on-mobile-phone-giants-8931528.html

18 Der Spiegel. (2013, September 20). Belgacom attack: Britain’s GCHQ hacked Belgian telecoms firm. *Der Spiegel*. www.spiegel.de/international/europe/british-spy-agency-gchq-hacked-belgian-telecoms-firm-a-923406.html

19 Larson, J., Perlroth, N., & Shane, S. (2013, September 5). Revealed: The NSA’s Secret Campaign to Crack, Undermine Internet Security. *ProPublica*. www.propublica.org/article/the-nsas-secret-campaign-to-crack-undermine-internet-encryption

20 Schneier, B. (2013, September 5). The US government has betrayed the internet. We need to take it back. *The Guardian*. www.theguardian.com/commentisfree/2013/sep/05/government-betrayed-internet-nsa-spying

1 MacAskill, E., Borger, J., Hopkins, N., Davies, N., & Ball, J. (2013, June 21). Mastering the internet: how GCHQ set out to spy on the world wide web. *The Guardian*. www.theguardian.com/uk/2013/jun/21/gchq-mastering-the-internet

2 MacAskill, E., Borger, J., Hopkins, N., Davies, N., & Ball, J. (2013, June 21). GCHQ taps fibre-optic cables for secret access to world’s communications. *The Guardian*. www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa

3 Clark, J. (2014, February 27). UK spies on MILLIONS of Yahoo! webcams, ogles sex vids - report. *The Register*. www.theregister.co.uk/2014/02/27/gchq_optic_nerve

4 Ackerman, S., & Ball, J. (2014, February 28). Optic Nerve: millions of Yahoo webcam images intercepted by GCHQ. *The Guardian*. www.theguardian.com/world/2014/feb/27/gchq-nsa-webcam-images-internet-yahoo

5 Ackerman, S. (2014, February 28). Senators to investigate NSA role in GCHQ ‘Optic Nerve’ webcam spying. *The Guardian*. www.theguardian.com/world/2014/feb/28/nsa-gchq-webcam-spy-program-senate-investigation

criminals and other spying agencies will eventually use the same weaknesses.

Intercepting the internal communications of internet companies

Unfortunately we live in a world where all too often laws are for the little people. Nobody at GCHQ or the NSA will ever stand before a judge and answer for this industrial-scale subversion of the judicial process. (Mike Hearn, Google security engineer)²¹

The NSA – in partnership with the FBI – has direct access to data held by several major US internet companies through the PRISM programme. But in addition, the NSA and GCHQ have been intercepting the private cables that connect the data centres of some of these companies, including Google and Yahoo. The joint programme – called Muscular²² – is based in Britain and mainly run by GCHQ.

This type of bulk collection had been ruled illegal in the US²³ because operations in the homeland have to filter out the data of US persons (citizens and permanent residents). The NSA appears to bypass these restrictions by getting GCHQ to collect the data, which they are then free to search and process.

Failures in the regulation of GCHQ

All of GCHQ's work is carried out in accordance with a strict legal and policy framework which ensures that our activities are authorised, necessary and proportionate, and that there is rigorous oversight. (GCHQ boilerplate response to inquiries)

We have a light oversight regime compared with the US. (Leaked GCHQ internal memo)

The legislation governing GCHQ is very complex. The organisation operated in the shadows from its creation²⁴ until 1994, when its existence was officially recognised in the Intelligence Services Act,²⁵ which also created a parliamentary committee to provide some oversight. The Regulation of Investi-

gatory Powers Act (RIPA 2000)²⁶ created a system of warrants and further oversight by independent commissioners.

The UK surveillance system has some peculiarities, for example:

- Ministers or staff, not judicial courts, sign surveillance warrants.
- A secret court, the Investigative Powers Tribunal, which is deemed by rights groups to be insufficient, hears complaints about surveillance or intelligence services.
- Intercept evidence is not admissible in court in order to protect the methods of the security services. This means that when police or GCHQ wiretap a phone call they will use this to obtain further evidence, but a jury will not hear the content of the call. Metadata in the form of call logs and mobile location is widely used.

It is important to note that there is a legal and practical distinction between surveillance for national security by spy agencies and the use of similar techniques by police forces.

Weak oversight of the surveillance regime

A recent report²⁷ by the Home Affairs Committee of the British Parliament was overtly critical of the current oversight mechanisms. They found the Intelligence and Security Committee (ISC) to be too cosy with the executive, despite recent changes to its statute. For example, the ISC had cleared GCHQ of any wrongdoing about PRISM in July 2013,²⁸ soon after the first publication of leaked documents. As the evidence of potential abuse piles up month after month, the ISC remains broadly supportive of GCHQ.

According to the report, the independent commissioners tasked with monitoring the security services simply do not have the capacity to deal with the hundreds of thousands of surveillance requests in place every year.

Jurisdiction hopping

There are concerns that the NSA and GCHQ use gaps in their regulatory frameworks to help each other bypass limitations on indiscriminate surveil-

lance carried out within national soil or affecting their own nationals.

The US and UK are not meant to spy on each other's population, but a leaked memo²⁹ from 2007 shows that the US is now "incidentally collecting" data on UK citizens who were not the target of any investigation. Proposals to increase privacy protections in any of these countries, such as those recently proposed by the Obama administration in the US,³⁰ are hollow if other countries in the alliance can help bypass them.

Mass surveillance is a breach of human rights

Bulk collection of data is lawful in the UK.³¹ The Secretary of State³² can sign special "certificates" that allow for mass surveillance of any targets outside the British Isles under very broad themes, including "intelligence on the political intentions of foreign governments; military postures of foreign countries; terrorism, international drug trafficking and fraud."

These certificates have been labelled "a blank cheque to spy on the world" by campaigners³³ who doubt they comply with international human rights laws.

Unaccountable hacking is unlawful

In contrast to the justifications provided for some of the other programmes, no government official has replied to the widespread evidence of mass hacking in leaked documents. Privacy International has challenged³⁴ the compliance of these activities with human rights legislation.

Weak public and political reaction

The public reaction to the Snowden revelations has been quite muted in the UK. There are several

inquiries and reviews in motion but no substantial changes. The Royal United Services Institute has been commissioned by the deputy prime minister to report after the next general election in May 2015.³⁵ The parliamentary committee in charge of overseeing GCHQ has predictably concluded that the agency did not break any laws.³⁶ The Labour Party, currently in opposition, has asked for a fundamental review of surveillance to deal with the lack of trust in the spy agencies but it has stopped short of criticising the activities of GCHQ.

These timid reactions are in stark contrast to the US, where there are competing legislative reforms.³⁷ Undoubtedly the lack of political reactions reflects the low level of public awareness and debate about mass surveillance among the UK population. There are several hypotheses for this apparent lack of public concern.

Media self-censorship

The coverage of the Snowden leaks in the UK has fallen disproportionately on *The Guardian* newspaper, with little coverage in other papers and TV. The paper had a natural lead as the original recipient of the leaked documents. But while media outlets in other countries have since obtained source documents and produced their own stories, this has not been the case in Britain.

The UK operates a system of voluntary censorship for national security issues, called the D-Notice,³⁸ issued by the Defence, Press and Broadcasting Advisory Committee (DPBAC). The DPBAC sent out a reminder to the media the day after *The Guardian* started publishing the leaked documents, and it seemed to work.

Trust in the spy agencies?

Popular wisdom is that the enduring mythology about British spies, from Lawrence of Arabia to James Bond,³⁹ makes it hard to challenge the UK "secret state". In addition, GCHQ is widely credited with a major contribution to the allied victory in World War Two by cracking the German encryption

21 <https://plus.google.com/+MikeHearn/posts/LW1DXJ2BK8k>

22 apps.washingtonpost.com/g/page/world/how-the-nas-muscular-program-collects-too-much-data-from-yahoo-and-google/543

23 Gellman, B., & Soltani, A. (2013, October 30). NSA infiltrates links to Yahoo, Google data centers worldwide, Snowden documents say. *The Washington Post*. www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html

24 www2.warwick.ac.uk/fac/soc/pais/people/aldrich/vigilant/lectures/gchq/

25 www.gchq.gov.uk/how_we_work/running_the_business/oversight/Pages/the-law.aspx

26 www.legislation.gov.uk/ukpga/2000/23/contents

27 UK Parliament Home Affairs Committee. (2014). *Oversight of the security and intelligence agencies*. www.publications.parliament.uk/pa/cm201314/cmselect/cmhaff/231/23108.htm

28 UK Parliament Intelligence and Security Committee. (2013, July 17). Statement on GCHQ's Alleged Interception of Communications under the US PRISM Programme. *Statewatch*. www.statewatch.org/news/2013/jul/uk-isc-gchq-surveillance-statement.pdf

29 Ball, J. (2013, November 20). US and UK struck secret deal to allow NSA to 'unmask' Britons' personal data. *The Guardian*. www.theguardian.com/world/2013/nov/20/us-uk-secret-deal-surveillance-personal-data

30 Cohn, C., & Higgins, P. (2014, January 17). Rating Obama's NSA Reform Plan: EFF Scorecard Explained. *Electronic Frontier Foundation*. <https://www.eff.org/deeplinks/2014/01/rating-obamas-nsa-reform-plan-eff-scorecard-explained>

31 MacAskill, E., Borger, J., Hopkins, N., Davies, N., & Ball, J. (2013, June 21). The legal loopholes that allow GCHQ to spy on the world. *The Guardian*. www.theguardian.com/uk/2013/jun/21/legal-loopholes-gchq-spy-world

32 In the United Kingdom, a secretary of state is a cabinet minister in charge of a government department.

33 Bunyan, T. (2014). GCHQ is authorised to "spy on the world" but the UK Interception of Communications Commissioner says this is OK as it is "lawful". *Statewatch*. www.statewatch.org/analyses/no-244-gchq-intercept-commissioner.pdf

34 Wilson, C. (2014, May 13). Explaining the law behind Privacy International's challenge to GCHQ's hacking. *Privacy International*. <https://www.privacyinternational.org/blog/explaining-the-law-behind-privacy-internationals-challenge-to-gchqs-hacking>

35 <https://www.rusi.org/news/ref:N5315B2C9B1941/>

36 BBC. (2013, July 17). GCHQ use of Prism surveillance data was legal, says report. www.bbc.co.uk/news/uk-23341597

37 Glaser, A. (2014, April 23). Comparing NSA Reforms to International Law: A New Graphic by AccessNow. *Electronic Frontier Foundation*. <https://www.eff.org/deeplinks/2014/04/comparing-nsa-reforms-international-law-new-graphic-accessnow>

38 www.dnotice.org.uk

39 Frith, H. (2014, February 20). Ian Fleming romance points up ambiguous attitude to spying. *The Week*. www.theweek.co.uk/tv-radio/57398/ian-fleming-romance-points-ambiguous-attitude-spying

codes at Bletchley Park.⁴⁰ In contrast, the 1960s and 1970s saw several scandals that shook the polished image of the UK spy agencies,⁴¹ but their effect on current popular perceptions is unclear.

Trust in public institutions has declined in much of Europe,⁴² and the UK seems to follow a similar pattern to other countries. In most European countries, citizens trust the police more than politicians and other public bodies.⁴³ It is possible that this trust somehow extends to spy agencies.

Terrorist threat

The UK is a clear target of terrorist groups due to its close alignment with the US and military involvement in Iraq and Afghanistan. Citizens are acutely aware of the threat, with constant reminders in public spaces. This has a likely influence on perceptions of the balance of risk.

Action steps

Don't Spy on Us

UK civil society groups have been running a joint advocacy campaign – DontSpyonUS.org.uk – demanding fundamental reforms of surveillance legislation and practices:

Don't Spy On Us is calling for a new Parliamentary Bill to make the spooks accountable to our elected representatives, to put an end to mass surveillance and let judges, not the Home Secretary, decide when spying is justified.⁴⁴

The campaign is asking for international supporters to sign up and endorse its proposals.

Legal challenges

There are several legal challenges being brought forward by UK civil society groups. Open Rights Group, Big Brother Watch and English PEN, together with German activist Constanze Kurtz, have taken the UK government to the European Court of Human Rights. They managed to crowd-fund over £20,000 for legal fees⁴⁵ in just 48 hours.

Other organisations – including Liberty (the National Council for Civil Liberties) and Privacy International – have placed a complaint at the Investigatory Powers Tribunal. The first hearings have led to unprecedented disclosures, as the security services have been forced to defend the legality of their practices⁴⁶ – but in all likelihood the case will end up in a European court.

Most major reforms of the British security services over the past 30 years have been driven by European legislation and court rulings. For example, the RIPA law mentioned above was created in order to comply with the European Convention on Human Rights, as it became UK law. So it would be important for more civil society organisations and concerned individuals to challenge the activities of the UK at European courts.

Advocacy for reform

The Don't Spy on Us Campaign has a set of principles for reform, based on the 13 International Principles on the Application of Human Rights to Communications Surveillance.⁴⁷ They are trying to get all major political parties to support a wholesale review of surveillance. But while all the three main parties are proposing some form of review or enquiry, these fall short of the demands of civil society.

International agreements

Even if UK campaigners won each of their demands, reforms at the national level would not be enough. The UK and the US have built a very complex surveillance machine that involves many other countries, and reforms will need to take place elsewhere to be effective. Third party allies such as Sweden, France and Germany will need to put their own house in order as well.

There is a need for some form of international agreement, as no state will unilaterally reduce its surveillance capability. Mass digital surveillance and the corresponding militarisation of cyberspace are complex problems, much like nuclear weapons or climate change. These involve systemic changes beyond tinkering with oversight mechanisms.

Technical and business measures

Stopping mass surveillance requires more than legal and political changes. As long as the business models of internet companies are based on surveillance, governments will find a way to tap into these data pools. There is a need for new models that

minimise corporate surveillance for commercial purposes.

Mass surveillance systems are a very good example of Larry Lessig's maxim, "Code is law."⁴⁸ Any proposals for change must also involve technology. For example, there are several campaigns to promote widespread encryption,⁴⁹ and the technical community that keeps the internet running have started to consider a fundamental architectural redesign to make the job of the spooks harder.⁵⁰

The securocrats strike back

The Snowden leaks were not a complete surprise to British human rights campaigners, who had long complained about legal loopholes creating the potential for excessive surveillance. The leaks arrived just as these groups were winning a temporary reprieve against legislative proposals to strengthen the UK's surveillance capability. The draft Communications Data Bill (CDB)⁵¹ – dubbed the Snoopers' Charter – had proposed to give the security services automated direct access to the inner systems of communications providers and internet companies through a form of search engine.

The draft bill was blocked by the minority partners of the coalition government – the Liberal Democrats – due to concerns over the human rights implications of such an intrusive system. With hindsight, the CDB appears eerily similar to some of the systems described in the leaks, such as PRISM and XKEYSCORE. Although the law was put in the freezer, several hundred million pounds have already been spent on these systems. It is not known what level of implementation and oversight is in place.

Any hopes that the current UK government would voluntarily commit to fundamental reforms on mass

surveillance were dashed with the introduction of the Data Retention and Investigatory Powers (DRIP) Bill⁵² in July 2014. This emergency legislation was ostensibly introduced to deal with the fallout of the ruling of the Court of Justice of the European Union in April 2014 that declared the EU Data Retention Directive invalid.⁵³ The directive forced communications providers to keep logs of all calls, websites, emails, etc. from all customers, in case the security services needed them. This was found to be too broad and disproportionate to be compatible with human rights law.

The new bill is meant to be just a replacement of the Data Retention Directive, but it adds a unique extraterritorial expansion⁵⁴ of British surveillance powers to cover any form of internet provider anywhere in the world.

Instead of carefully considering the content of the ruling and its implications for all forms of indiscriminate blanket data collection, the UK government has rammed through parliament groundbreaking surveillance legislation without any proper debate. This has been achieved in a deal among the three main parties, which have all supported the core aspects of the bill. In exchange the government has now committed to review surveillance laws by the next election, in May 2015, and to introduce a US-inspired privacy board.

The DRIP Bill has already been threatened with legal challenges by human rights groups. Two parliamentarians have asked for a judicial review on the grounds that it breaches human rights, with the support of Liberty.⁵⁵ Open Rights Group also has plans to take the Home Office to court over the DRIP Bill.⁵⁶

40 www.bletchleypark.org.uk

41 www2.warwick.ac.uk/fac/soc/pais/people/aldrich/vigilant/lectures/gchq/

42 Park, A., Bryson, C., Clery, E., Curtice, J., & Phillips, M. (Eds.) (2013). *British Social Attitudes: The 30th Report*. London: National Centre for Social Research bsa-30.natcen.ac.uk/read-the-report/key-findings/trust-politics-and-institutions.aspx

43 Committee on Standards in Public Life. (2014). *Public Perceptions of Standards in Public Life in the UK and Europe*. www.public-standards.gov.uk/wp-content/uploads/2014/03/2901994_CSPL_PublicPerceptions_acc-WEB.pdf

44 <https://www.dontspyonus.org.uk/pi>

45 <https://www.privacynotprism.org.uk>

46 <https://www.privacyinternational.org/what-to-know-gchq-on-trial>

47 <https://en.necessaryandproportionate.org/text>

48 Lessig, L. (2000). Code Is Law. *Harvard Magazine*, January-February. harvardmagazine.com/2000/01/code-is-law.html

49 <https://en.necessaryandproportionate.org/text>

50 <https://www.w3.org/2014/strint>

51 <https://www.openrightsgroup.org/issues/Snoopers%20Charter>

52 services.parliament.uk/bills/2014-15/dataretentionandinvestatorypowers.html

53 European Data Protection Supervisor. (2014, April 8). Press statement: The CJEU rules that Data Retention Directive is invalid. https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Press/2014/14-04-08_Press_statement_DRD_EN.pdf

54 Open letter from UK Internet Law Academic Experts to All Members of Parliament, 15 July 2014. www.slideshare.net/EXCCLEssex/open-letter-uk-legal-academics-drip

55 <https://www.liberty-human-rights.org.uk/news/press-releases/liberty-represents-mps-david-davis-and-tom-watson-legal-challenge-government%E2%80%99s-g99s->

56 Killock, Jim. (2014, July 18). Dear Theresa, see you in court. *Open Rights Group*. <https://www.openrightsgroup.org/blog/2014/dear-theresa-see-you-in-court>

UNITED STATES

The Necessary and Proportionate Principles and the US government



Access

Amie Stepanovich, Drew Mitnick and Kayla Robinson
www.accessnow.org

Introduction

In June 2013, the scale and scope of US foreign intelligence surveillance began to be revealed to the world. Over a year later, the surveillance programmes described in the revelations facilitated by Edward Snowden continue to draw the ire of human rights advocates who argue the surveillance is, among other issues, unnecessary, disproportionate, and fundamentally lacking in transparency and oversight. The attention has galvanised policy makers in Washington, D.C., where the US Congress is moving closer to passing some version of communications surveillance reform. The Obama administration has released a number of reports and statements detailing its version of the operation of US surveillance work, and defending the constitutionality of these programmes. Simultaneously, the administration has quietly promoted principles which, if implemented, would bring US surveillance closer in alignment with international human rights law.

The Obama administration's principles provide a framework for US compliance with its own stated objectives (the US Framework).¹ The US Framework largely mirrors several of the International Principles on the Application of Human Rights to Communications Surveillance (Principles), an evaluative framework for assessing how human rights obligations and norms apply when conducting surveillance.² Below, we compare US surveillance practices to its own stated Framework and the Principles.

Policy and political background

Many US surveillance operations are authorised under either Section 215 of the Patriot Act (the “business records” provision), which has been

interpreted to authorise bulk collection, or Section 702 of the FISA [Foreign Intelligence Surveillance Act] Amendments Act, which permits targeting of non-US persons “reasonably believed to be located outside the [US]” for foreign intelligence purposes.³ Notably, the National Security Agency (NSA) presumes that a target is a non-US person when their location cannot be determined.⁴

The government also uses Executive Order (EO) 12333 to authorise surveillance programmes where the collection point is located outside of the US. It is widely believed that the government has interpreted EO 12333 to authorise any surveillance activities that are not otherwise unlawful or unconstitutional. Traditionally, there has been very little public information about EO 12333, including any oversight thereof. According to recent reports, EO 12333 authorises, inter alia, collecting all calls made in the Bahamas and another, undisclosed country.⁵

In March 2014, the US government adopted six privacy principles to govern surveillance. Scott Busby, Deputy Assistant Secretary of State for Democracy, Human Rights and Labor, articulated the US Framework at the 2014 RightsCon Silicon Valley conference, hosted by Access.⁶ Secretary of State John Kerry reiterated the US Framework at a recent Freedom Online Coalition conference.⁷

A closer look at the US Framework for surveillance

Prior to the release of the US Framework, a number of government reports made recommendations encompassing several human rights principles. The President's Review Group on Intelligence and Communications Technologies (President's Review

Group) released a report that included a number of recommendations in line with the Principles: transparency in the operation of the US surveillance programmes; due process reforms for the Foreign Intelligence Surveillance Court (FISC); and more effective government oversight.⁸ The Privacy and Civil Liberties Oversight Board (PCLOB) separately released a report arguing that bulk metadata collection is illegal under the terms of Section 215 and called for the creation of a special advocate to argue against the government before the FISC.⁹ These recommendations could help guide the implementation of the US Framework and ensure compliance with its commitments.

The US Framework expands upon President Obama's Presidential Policy Directive 28 (PPD-28) which establishes principles to guide surveillance.¹⁰ The six principles endorsed by the US are (1) rule of law, (2) legitimate purpose, (3) non-arbitrariness, (4) competent external authority, (5) meaningful oversight, and (6) increased transparency and democratic accountability. While the US Framework borrows heavily from the Principles, it omits several of them, and even in the case of those it adopts it often fails to meet the same standards. Principles not adopted by the US include due process, user notification, integrity of communications and systems, safeguards for international cooperation, and safeguards against illegitimate access.

Below, we examine the overlap between the US Framework and the Principles and examine where US policy fails to comply with the US Framework:

1. **Rule of law** – In his speech setting out the US Framework, Assistant Secretary Busby discussed how surveillance operates “pursuant to statutes and executive orders that were adopted as part of our democratic process.” This principle further requires that laws, and their subsequent policies, provide clarity for individuals within the jurisdiction. US surveillance policy has proven to be anything but clear and accessible to the public. Instead, surveillance practices often depend on loose legal interpretations written in secret, approved by secret

courts, and overseen by secret Congressional committees. By contrast, the Principles require that the law contains a “standard of clarity and precision” to provide users notice of the application of surveillance.

US surveillance policy does not conform with the rule of law principle. For example, Section 215 permits collection of records only when they are “relevant to an authorized investigation.” However, authorities have interpreted the language to permit the acquisition of *all* phone records transiting the US. Similarly, Section 702 contains language that is overly vague, granting the Attorney General and Director of National Intelligence (DNI) the authority to “target persons reasonably believed to be located outside the United States to acquire foreign intelligence information.” Programmes under this authority, namely PRISM and “Upstream” collection,¹¹ involve virtually limitless surveillance on any non-US person outside the US, and, by extension, “incidental” collection of vast amounts of data from US persons.

2. **Legitimate purpose** – The US Framework would permit surveillance only on the “basis of articulable and legitimate foreign intelligence and counter-intelligence purposes.” This does not match the standard of the legitimate aim principle, which requires surveillance to be conducted only in the furtherance of a “predominantly important legal interest that is necessary in a democratic society.” Further, PPD-28 permits bulk collection only for “detecting and countering” certain enumerated threats, and expressly prohibits the use of bulk collection for suppression of dissent, discrimination, or promoting US commercial interests. However, no similar restriction is placed on other non-bulk, yet highly intrusive forms of surveillance authorised under Section 702. The government should specify – and identify meaningful limits to – the purposes for which it acquires and collects foreign intelligence.

3. **Non-arbitrariness** – Non-arbitrariness, as articulated by the US Framework, requires surveillance to be tailored and intrusiveness minimised. This element matches up to the proportionality, necessity and adequacy principles.

1 Speech by Scott Busby at RightsCon, 4 March 2014. www.humanrights.gov/2014/03/04/state-department-on-internet-freedom-at-rightscon; Remarks to the Freedom Online Coalition Conference by US Secretary of State John Kerry, 28 April 2014. www.state.gov/secretary/remarks/2014/04/225290.htm
2 https://en.necessaryandproportionate.org/text

3 50 U.S.C. § 1881a (2008).

4 The Guardian. (2013, June 20). Procedures used by NSA to target non-US persons: Exhibit A – full document. *The Guardian*. www.theguardian.com/world/interactive/2013/jun/20/exhibit-a-procedures-nsa-document

5 Devereaux, D., Greenwald, G., & Poitras, L. (2014, May 19). The NSA is recording every cell phone call in the Bahamas. *The Intercept*. https://firstlook.org/theintercept/article/2014/05/19/data-pirates-caribbean-nsa-recording-every-cell-phone-call-bahamas

6 Speech by Scott Busby at RightsCon, 4 March 2014. www.humanrights.gov/2014/03/04/state-department-on-internet-freedom-at-rightscon

7 Remarks to the Freedom Online Coalition Conference by US Secretary of State John Kerry, 28 April 2014. www.state.gov/secretary/remarks/2014/04/225290.htm

8 Report and Recommendations of the President's Review Group on Intelligence and Communications Technologies: Liberty and Security in a Changing World, 21 December 2013. www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf

9 Privacy and Civil Liberties Oversight Board. (2014). Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court. www.pclob.gov/SiteAssets/Pages/default/PCLOB-Report-on-the-Telephone-Records-Program.pdf

10 Office of the Press Secretary. (2014). Presidential Policy Directive/PPD-28. www.whitehouse.gov/sites/default/files/docs/2014signit_mem_ppd_rel.pdf

11 Some slides used by the NSA revealed by Edward Snowden make a distinction between the “PRISM” and “Upstream” collection programmes. While we will use that shorthand in this submission, our understanding is that “Upstream” encompasses a wide range of surveillance programmes that have been revealed to date, including BLARNEY, FAIRVIEW, OAKSTAR, LITHIUM, and STORMBREW.

Proportionality requires considering government interests in light of the severity of intrusion and sensitivity of information. However, US indiscriminate bulk surveillance practices are not conducted in accordance with either the Principles or the US Framework.¹² The president has proposed a limit on the use of bulk collection of telephone metadata.¹³ Obama's proposal, however, does not prohibit bulk collection generally, but only addresses telephone metadata bulk collection under the 215 authority.¹⁴ The US should rather immediately end all mass surveillance practices.

In an example of the mismatch between the Framework and past practices, in 2012, the NSA queried its database of hundreds of millions telephone metadata records 288 times.¹⁵ Of those 288 queries, only 16 produced a potential connection to suspected terrorist activity that warranted a referral to the FBI for investigation. It is difficult to see how this programme comports with the adequacy principle, or with the necessity principle's requirement that "[c]ommunications surveillance must only be conducted when it is the only means of achieving a legitimate aim, or, when there are multiple means, it is the means least likely to infringe upon human rights."

4. **Competent authority** – While the US Framework seeks guidance from a "competent external authority", the Principles specify that the authority be judicial. In contrast to the Principles, the Framework expressly retains an exception

for some operational decisions to be made within intelligence agencies. FISC, the judicial authority that reviews surveillance programmes and applications, has been repeatedly misled by US intelligence agencies in their applications, which makes its rulings inherently unreliable.¹⁶

The Principles further require that the competent judicial authority be "conversant in issues related to and competent to make judicial decisions about the legality of communications surveillance, the technologies used and human rights." However, the secret nature of FISC makes it difficult for judges to consult with the independent technical and legal experts necessary to fairly decide complicated issues. One former FISC judge has gone on the record proposing the use of specially appointed advocates to help alleviate this problem, though this has not been adopted.¹⁷

5. **Oversight** – The US Framework calls for meaningful oversight. To underscore US adherence to this element, Assistant Secretary Busby highlighted extant internal oversight mechanisms. However, despite claims that the NSA's activities have been approved by all three branches of government, the NSA has reportedly lied to or misled all three branches.¹⁸

In accordance with the Principles, true oversight mechanisms should operate independently of the state entity conducting surveillance. Public oversight calls for independent oversight mechanisms that have the authority to access all potentially relevant information, an element lacking from current US policy.

6. **Increased transparency and democratic accountability** – The final element of the US Framework is transparency. Assistant Secretary Busby pointed to recent efforts to declassify FISC opinions and the government's intention to

release the statistics on the issuance of national security orders and requests.

In fact, the DNI has released a transparency report including the total number of orders issued under certain authorities in 2013, and the number of targets affected.¹⁹ This report supplements the information already required as part of the intelligence community's annual FISA reporting.²⁰ While this is a step forward for transparency around government surveillance activities, the report falls short of what was called for by the We Need to Know Coalition,²¹ which urged Congressional leaders and the Obama administration to require the government to publish information about the specific numbers of requests, the specific authorities making those requests, and the specific statutes under which those requests are made.²²

Unlike Google's and Microsoft's transparency reports, which break down both the number of requests they receive and the number of accounts affected, the DNI's report only includes the number of requests and "targets", which makes the scope of the nation's surveillance machine appear far more limited than it actually is. To put this in context, in 2012, there were 212 requests for business records justified under Section 215, but that number also includes requests for the "ongoing, daily" disclosure of communications metadata of the millions of customers of AT&T, Verizon and Sprint. We know this because public disclosure of aggregate numbers of requests pursuant to most of the statutes to be included in the DNI's report is already required.

It is also worth noting that the government has only released the number of targets, not the exponentially larger number of people whose privacy is violated when their data are caught in the NSA's dragnet. Moreover, by grouping statutes together in the

categories, the DNI is further obfuscating the nature and scope of the government's surveillance activities, and limiting an informed, public debate about the extent of the intelligence community's intrusions into the private lives of users all over the world.

Public disclosure by both the government and the communications providers who hold user data is crucial in keeping both accountable. At this time, the US government has not demonstrated an intention to publicly disclose details of the scope and scale of its surveillance activity at the level of clarity and granularity envisioned by the Principles, nor has it allowed corporations it requests data from to do so either.

Conclusions

The revelations provide evidence of widespread violations of the fundamental right to privacy, with implications for the rights to freedom of expression and association, among other rights. Bulk surveillance is inherently arbitrary, and therefore in violation of international law. Legitimate surveillance activities should always be based on probable cause and targeted toward a specific individual or organisation.

Unfortunately, currently proposed legislative reforms would fail to move the US towards the Framework or the Principles. The House of Representatives recently passed the USA Freedom Act, a bill that many advocates viewed as the best hope for human rights reforms. The bill passed the House after being weakened during secret deliberations between the Obama administration and members of the House. The changes were so significant that most rights groups withdrew support.²³

As originally written, the USA Freedom Act would have achieved a number of significant human rights reforms, including preventing bulk collection by requiring a nexus to an investigation, bringing clarity to Section 215, increasing FISC oversight and introducing a special advocate, increasing the ability of companies to disclose government national security data requests, and increasing the power of internal oversight bodies, as well as adding external checks. The House watered down many of the reforms.

Congress' failure to enact reforms is a great disappointment. The US must change its laws if it is to bring its surveillance programmes closer in

12 Although some of these practices "only" collect communications metadata, a recent study has demonstrated exactly how revealing this information can be, even over a short period of time. See Mayer, J., & Miltcher, P. (2014, March 12). MetaPhone: The Sensitivity of Telephone Metadata. *Web Policy*. webpolicy.org/2014/03/12/metaphone-the-sensitivity-of-telephone-metadata/; Lohr, S. (2014, May 31). Quantifying Privacy: A Week of Location Data May Be an 'Unreasonable Search'. *New York Times*. bits.blogs.nytimes.com/2014/05/31/quantifying-privacy-a-week-of-location-data-may-be-unreasonable-search

13 Savage, C. (2014, March 24). Obama to Call for End to NSA's Bulk Data Collection. *New York Times*. www.nytimes.com/2014/03/25/us/obama-to-look-into-nsa-bulk-data-collection.html

14 This is problematic because the intelligence community engages in bulk collection of other information, including records of international money transfers. Savage, C., & Mazzetti, M. (2013, November 14). CIA Collects Global Data on Transfer of Money. *New York Times*. www.nytimes.com/2013/11/15/us/cia-collecting-data-on-international-money-transfers-officials-say.html. The U.S. government previously operated a programme to bulk collect internet metadata. Gellman, B. (2013, June 15). US Surveillance architecture includes collections of revealing internet, phone metadata. *Washington Post*. www.washingtonpost.com/investigations/us-surveillance-architecture-includes-collection-of-revealing-internet-phone-metadata/2013/06/15/ebf004a-d511-11e2-b05f-3ea3f0e7bb5a_story.html

15 This is according to Professor Geoffrey Stone, a member of the President's Review Group. Speech by Geoffrey Stone at Public Citizen, 6 January 2014. www.citizen.org/pressroom/pressroomdirect.cfm?ID=4057

16 Cushing, T. (2013, August 21). Declassified FISA Court opinion shows NSA lied repeatedly to the Court as well. *techdirt*. <https://www.techdirt.com/articles/20130821/16331524274/declassified-fisa-court-opinion-shows-nsa-lied-repeatedly-to-court-as-well.shtml>

17 Carr, J. (2013, July 22). A Better Secret Court. *New York Times*. www.nytimes.com/2013/07/23/opinion/a-better-secret-court.html

18 McCormick, R. (2013, October 28). Obama wasn't aware of the NSA's wiretap of world leaders, says White House Review. *The Verge*. www.theverge.com/2013/10/28/5037300/obama-unaware-of-wiretaps-on-world-leaders; Blake, A. (2013, June 11). Sen. Wyden: Clapper didn't give 'straight answer' on NSA programs. *Washington Post*. www.washingtonpost.com/blogs/post-politics/wp/2013/06/11/sen-wyden-clapper-didnt-give-straight-answer-on-nsa-programs; Ackerman, S. (2013, August 21). NSA illegally collected thousands of emails before FISA Court halted program. *The Guardian*. www.theguardian.com/world/2013/aug/21/nsa-illegally-collected-thousands-emails-court

19 The report contained figures for Section 702 and Section 215 orders, as well as other authorities including the FISA "Trap and Trace" provision and National Security Letters. Office of the Director of National Intelligence. (2014, June 26). Statistical Transparency Report Regarding Use of National Security Authorities Annual Statistics for Calendar Year 2013. www.dni.gov/files/tp/National_Security_Authorities_Transparency_Report_CY2013.pdf

20 U.S. Department of Justice. (2014, April 30). 2013 Report pursuant to the Foreign Intelligence Surveillance Act of 1978. www.justice.gov/nsd/foia/foia_library/2013fisa-ltr.pdf

21 We Need to Know is a multi-stakeholder group including companies like Google and Microsoft, NGOs including Access, CDT and the ACLU, and various trade associations. We Need to Know. (2013, July 18). Letter to Congressional leaders and Obama administration on transparency. <https://www.accessnow.org/page/-/weneedtoknow-transparency-letter.pdf>

22 Furthermore, the Coalition called for the ability to differentiate requests based on content versus non-content data, and enumerate the number of persons, accounts or devices affected. The DNI report only includes the numbers of orders issued, and the number of "targets" affected.

23 Masnick, M. (2014, May 21). As feared: House guts USA Freedom Act, every civil liberties organization pulls their support. *techdirt*. www.techdirt.com/articles/20140520/17404727297/as-feared-house-guts-usa-freedom-act-every-civil-liberties-organization-pulls-their-support.shtml; Stepanovich, A. (2014, May 20). Access withdraws conditional support for USA FREEDOM Act. *Access Now*. <https://www.accessnow.org/blog/2014/05/20/access-withdraws-conditional-support-for-usa-freedom-act>

alignment with the Principles and other international human rights standards. While the president's policy statement is an admirable show of commitment to surveillance reform, only greater legal restrictions and increased external oversight of these programmes can assure the protection of fundamental freedoms, and reassure the public that the US conducts its surveillance activities in a rights-respecting manner.

Action steps

The following advocacy steps are recommended in the US:

- Call or write to Congress urging them to support rights-respecting surveillance reform.
- Provide comments to the PCLOB showing support for efforts to ensure that rights are

protected during the development of laws to protect the nation against terrorism.


- Endorse the International Principles on the Application of Human Rights to Communications Surveillance:

<https://en.necessaryandproportionate.org/take-action/access>

- Encourage companies to protect your personal information by supporting the Data Security Action Plan: <https://www.encryptallthethings.net>
- Take steps to protect your own information by using secure communications platforms, like those suggested by Reset the Net: <https://pack.resetthenet.org>

URUGUAY

Penumbra: Surveillance, security and public information in Uruguay



DATA
Fabrizio Scrollini
www.datauy.org

Introduction

In July 2013 a local newspaper revealed that the Uruguayan government had purchased secret surveillance software called “El Guardián”.¹ El Guardián (or The Guardian) is a radical shift towards online and phone surveillance, and the challenges it represents remain largely out of public debate. This report aims to analyse the most recent developments in terms of the use of technology for surveillance in Uruguay. It will provide a description of key events and regulations that have recently emerged in Uruguay, analysing challenges to privacy. Finally it will provide a set of issues to develop an agenda for privacy according to the International Principles on the Application of Human Rights to Communications Surveillance.²

Government surveillance in the Uruguayan context

Uruguay is considered a stable and relatively transparent democracy by several indicators available, including that offered by Transparency International.³ Uruguayan democracy was regained from military rule in 1985, but the country's democratic tradition goes as far back as the beginning of the 20th century, when Uruguay was one of the few democratic nations in Latin America. During the past military dictatorship (1973-1985) the Uruguayan government ran extensive surveillance programmes in order to monitor its citizens. According to the weekly publication *Brecha*, a former intelligence officer revealed that the dictatorship managed to develop profiles of at least 300,000 Uruguayans.⁴ Access to these files is still contested in Uruguay,

but increasingly they are becoming available to people who were under state surveillance.

Uruguay has recently being portrayed as a liberal and progressive country. In the last five years it has passed laws legalising same-sex marriage, abortion and the cultivation and sale of cannabis. Furthermore, Uruguay passed a law on free and open source software which requires that the government use free and open source software in all its activities. Regulations in line with this law are still to be developed so that it can be implemented. Montevideo City Hall was one of the leading city governments in advancing open source and open data policies in the country.

Uruguay set up a monopoly in terms of internet provision run by the state-owned telecommunications company ANTEL.⁵ ANTEL is implementing a wide-ranging programme to provide internet access through optic fibre to the whole country. Previously ANTEL had secured connectivity across the country and established a scheme to provide basic access to the internet for every citizen. Today, 58% of the population has direct access to the internet, and 18% of Uruguayans are frequent internet users.⁶ Furthermore, the establishment and development of the Ceibal programme has allowed every child in Uruguay access to devices (i.e. netbooks) to connect to the internet in their schools, homes and also public squares. Ceibal is fostering a new kind of education which relies heavily on the internet. In the next 10 years a new generation of digital natives with full access to computers and the internet will emerge in Uruguay.

The country has a strong judiciary system with a long tradition of upholding the rule of law. Uruguay also has a relatively strong privacy law, although there is no systematic evaluation of its implementation. Nevertheless, technological change has outpaced the capacity of government watchdog institutions to keep an eye on several developments emerging, mostly in the areas of security and defence. Most of these developments are justified

1 Terra, G. (2013). Gobierno compró “El Guardián” para espiar llamadas y correos. *El País*. www.elpais.com.uy/informacion/gobierno-compro-guardian-espiar-llamadas-correos.html
2 <https://en.necessaryandproportionate.org/text>
3 www.transparency.org/country#URY
4 Sempol, D. (2008). Article in *Brecha*, 16 May, cited in Zabala, M., & Alsina, A. (2008). *Secretos Públicos*. Montevideo: Fin de Siglo, p. 46.

5 Administración Nacional de Telecomunicaciones: www.otelcom.uy
6 El Observador. (2013, April 3). Uruguay a la cabeza de Latinoamérica en penetración de internet *El Observador*. www.elobservador.com.uy/noticia/247366/uruguay-a-la-cabeza-de-latinoamerica-en-penetracion-de-internet

in public discourse as new tools to fight organised crime and possible external threats, as well as to improve policing services through technology. The Uruguayan government, similar to governments in many other Latin American countries, is under heavy pressure to deal with security issues, most notably street crime. In this context there are three developments that offer a set of challenges to privacy and democracy:

- The purchase and use of digital technology (software) to potentially spy on the civilian population.⁷
- The development of surveillance systems using CCTV cameras and drones to foster public safety and better policing.⁸
- The development of a cyber-crime law which effectively outlaws a set of behaviours considered “dangerous” and limits liberties in the digital age.⁹

The aforementioned developments are taking place in a context of a lack of regulation and understanding of a number of human rights issues on the part of the authorities, the judiciary and institutions defending human rights.

The Guardian: Software for surveillance

In July 2013, the local newspaper *El País* broke the news about the secret purchase of The Guardian software by the Uruguayan government.¹⁰ The Ministry of Home Affairs (*Ministerio del Interior*), which is responsible for security issues, classified this purchase as secret under the access to information law, hiding it from official records. There was no tender as it was a direct and exceptional purchase. The cost of the software licence was USD 2 million and there is a yearly service fee of USD 200,000. The Guardian is a system designed to monitor several networks, allowing up to 30 people to work simultaneously on mobile phones, landlines and emails. The software was designed by a Brazilian company called Digitro Tecnologia. Uruguay has recently passed a “free software” law, which essentially suggests that the government should use free or open source software unless a good justification exists.

The Guardian does not comply with this regulation as it is proprietary software.

According to *El País*, Digitro also provides services to the Brazilian Federal Police. In Brazil there has been intense debate about the use of The Guardian. The army and the police in Brazil openly admit that they use the tool.¹¹ Several accountability agencies are worried about the extent to which the software is being used on its civilian population and how exactly several state units at the national and state level are using it.¹² For instance, there were concerns that it was used in the context of the last Confederations Cup football tournament in Brazil, and the social unrest that erupted in a number of cities. Privacy Latam, a specialised blog dealing with surveillance in Latin America, reports that according to General José Carlos dos Santos from the Brazilian Army’s Centre for Cyber Defence, “the monitoring is legal and justified on the grounds of national security policies and actions.” He also claims that the software is adapted and customised by the user and is not used to monitor citizens in general, and that it was “used only during the 2013 Confederations Cup.”¹³

In Uruguay, the authorities have reassured the media that the surveillance software will be used within the traditional legal framework, which implies that the judiciary would need to authorise surveillance activities. In the words of the Secretary of the Presidency of the Republic: “This system will centralise surveillance through telecommunications and will provide more guarantees to subjects during this process. The technology is much more advanced than we currently have in Uruguay. But we are going to keep using [as required] an order from a competent judge or a request from the public solicitor, with the consent of the telecommunications operator. Guarantees remain in place.”¹⁴

Since then the media and the government have been relatively silent about the use of The Guardian. While the assurances that there will continue to be a legal framework that respects basic liberties and due process are comforting, there are serious challenges ahead. There are still no regulations con-

cerning the specific use of this tool for intelligence gathering by authorities. Currently Uruguay is in the middle of a discussion about how to structure security and intelligence services and as a result the use of these kinds of technologies is poorly regulated. At the same time, the triangulation of data collected through different security services such as the new CCTV system in place and drones is a matter of worry. A set of key questions emerge:

- How will this complex set of surveillance technologies be deployed? What is the protocol for deploying them and will it reflect the proportionality and necessity principles?
- What are the basic accountability arrangements for security officers operating these technologies?
- How will Uruguayan agencies cooperate with other intelligence agencies around the world and the region, and to what extent?

Another set of questions emerge about how the current privacy laws apply in this setting. There is a need to rethink privacy in the context of surveillance of communications, particularly where private information is held, and for how long Uruguayan authorities will be able to hold this information.

The fact that this software was purchased using a secret procedure with no parliamentary control or the involvement of other oversight bodies shows that it is necessary to rethink the accountability arrangement in this sector. Furthermore, while the Ministry of Home Affairs argues that the software is auditable, there is no specification of how it is auditable, who would perform such an audit, and whether the results of these audits are going to be available to the public.

Conclusion

The debate about surveillance, intelligence gathering and privacy is ill-informed in Uruguay. Authorities are reacting to a regional and global trend to use software to monitor telephone calls and networks for security purposes with no clear guidance or strategy (at least known to the public) that reflect human rights concerns. While public reassurances about upholding the rule of law are a good sign, the complexity of the matter calls for better regulation and engagement with civil society organisations and human rights institutions, in order to work on a human rights approach to surveillance in an age of technological change. The Uruguayan government and civil society organisations are not prepared to have a proper debate on the matter yet. On the other hand, due to its tradition of upholding the rule of

law, Uruguay presents an opportunity to foster appropriate and proportionate regulation in this field.

Action steps: A call for a human rights-centred vision of security in the digital age

Denying the challenges that the state faces in an age of transnational crime is foolish and irresponsible from a citizen’s perspective. But granting “carte blanche” to government authorities for surveillance with no restrictions is equally irresponsible. Uruguay has a history of less technologically developed but equally damaging surveillance during the 1973-1985 dictatorship. Until now, the release of these files and access to the records for people who were under surveillance remain problematic. In the context of a progressive democratic society, as Uruguay portrays itself, it is time to have a serious debate about privacy and security in the digital age.

The following steps are recommended to advance a human rights-centred agenda on this topic:

- Foster dialogue about principles for the use of The Guardian and other surveillance technologies between human rights institutions (such as the Ombudsman), the intelligence community and civil society, to identify common ground on this issue.
- Define clear protocols to use these tools and clear lines of accountability for public officials involved in the surveillance process.
- Define clear lines of democratic accountability and transparency on surveillance processes involving the parliament, the Ombudsman and civil society. In particular, establish a minimum of transparency around surveillance activities and a yearly report open to public scrutiny.
- Review the current privacy law and identify gaps and best practices in the context of surveillance and security activities. Consider progressive frameworks in terms of data retention and access to data for people potentially subject to surveillance.
- Promote the use of auditable (ideally open source or free software) technologies to manage data retention and secure critical data for intelligence and surveillance activities.

For a democratic society, the way forward implies allowing access to knowledge around surveillance activities, as well as keeping agencies in check when these technologies are developed. The aforementioned recommendations are the starting point for much-needed dialogue and debate on these issues in Uruguay.

7 Terra, G. (2013). Op. cit.

8 El País. (2014, April 21). Así vuelan los colibríes de la Policía uruguaya. *El País*. www.elpais.com.uy/informacion/asi-vuelan-colibri-drones-ministerio.html

9 Presidencia de la República. (2014, June 30). Ejecutivo remitió al Parlamento proyecto de ley que pena los delitos cibernéticos. *Presidencia de la República*. www.presidencia.gub.uy/comunicacion/comunicacionnoticias/seguridad-informatica-proyecto-ley

10 Terra, G. (2013). Op. cit.

11 Lobo, A. P. (2013, July 17). Exército usou software Guardiã para monitorar redes sociais. *Convergência Digital*. wap.convergenciadigital.com.br/cgi/cgilua.exe/sys/start.htm?infoid=34302&sid=11#.U5ZMmSghtbo

12 Veja. (2013, May 6). Conselho do MP investiga uso de grampos por promotores. *Veja*. veja.abril.com.br/noticia/brasil/conselho-do-mp-investiga-uso-de-grampos-por-promotorias

13 Monteiro. (2014, February 13). Brazil monitors protests against the 2014 World Cup. *Privacy Latam*. www.privacylatam.com/?p=200

14 Portal 180. (2013, July 30). Gobierno: Guardián centraliza vigilancia electrónica pero mantiene garantías. *Portal 180*. www.180.com.uy/articulo/34766_Gobierno-guardian-centraliza-vigilancia-electronica-pero-mantiene-garantias

VENEZUELA

Spying in Venezuela through social networks and emails



Escuela Latinoamericana de Redes (EsLaRed)

Sandra Benítez
sandrab@ula.ve

Introduction

In the following report, government measures and legal instruments that have been implemented in Venezuela in connection with the surveillance of communications are analysed. These measures were implemented as a way to ensure national security – but they can affect fundamental rights, such as freedom of expression and the right to privacy of individuals. Some cases involving the violation of human rights during the surveillance of communications are also presented. These have occurred in recent years in Venezuela, and are the result of a series of national economic, political and social events that have had a significant impact on the population, and, according to the government, have jeopardised national security. In addition, some statements by civil society on the measures implemented by the government in the period February to April 2014 are discussed. Actions that citizens can take to prevent access to protected information and to guarantee the privacy of communications are suggested, alongside actions that the state can implement to institutionally coordinate surveillance of communications and to establish clear principles.

Legal framework

Venezuela has a regulatory framework which guarantees fundamental freedom of expression and information rights of people, freedom of association, the right to privacy, honour, reputation and private life, and the right to privacy of communications. These are stipulated in articles 2, 29, 48, 57, 58, 59, 60 and 61 of the constitution.¹ Moreover, there are legal instruments that guarantee the implementation of human rights when it comes to surveillance of communications and the security of citizens, such as: the Law Against Computer Crimes² (Articles 6, 7 and 11); the Law on the Protection of

Privacy of Communication³ (Articles 1 to 9); the Law on Data Messages and Electronic Signatures;⁴ the Law on the Social Responsibility of Radio, Television and Electronic Media, and Telecommunications;⁵ a law called Infogobierno⁶ (Article 25); the Code of Criminal Procedure;⁷ the Law on Science, Technology and Innovation⁸ (Articles 5 and 6); the Law Against Organised Crime and Financing of Terrorism⁹ (Article 30); the Law on National Security;¹⁰ and the Law of the Bolivarian Armed Forces.¹¹ There are also regulatory bodies that are responsible for monitoring communications, such as the National Telecommunications Commission¹² (CONATEL); the Centre for Strategic Security and Protection of the Fatherland¹³ (CESPPA); the Vice Ministry of Social Networks;¹⁴ the Bolivarian National Intelligence Service¹⁵ (SEBIN); the National Telecommunications Company of Venezuela¹⁶ (CANTV); and the National Centre for Forensic Computing¹⁷ (CENIF).

Venezuela, as a member of the Organization of American States (OAS), is committed to supporting agreements and statements such as those made by the OAS Special Rapporteur for Freedom of Expression,¹⁸ mandates from the sixth Summit of the Americas on the use of information and communica-

tions technologies (ICTs),¹⁹ and the Joint Declaration on Security Programs and their Impact on Freedom of Expression.²⁰ However, it is important to note that in September 2013, Venezuela withdrew²¹ from the Inter-American Commission on Human Rights (IACHR), which does not guarantee the protection of rights in Venezuela under the OAS. However, citizens may use other protective mechanisms, such as the International Court of Justice at the United Nations,²² even though there is a risk that the government ignores its deliberations, such as in the case of judgments on the violations of human rights issued by Frank La Rue, Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression.²³

Analysis

Venezuela in recent years has faced a series of national events that have had a significant impact on Venezuelan society, from the inevitable call for a new presidential election process in 2013 because of the death of President Hugo Chávez, to the different mobilisations of civil society in 2014. These have resulted in a deterioration in the quality of life of Venezuelans, a greater division in society, the violation of human rights, and greater control by the government.

In this area the government is implementing a range of policies included in the Plan of the Nation 2013-2019,²⁴ which seek to deepen the socialist model that President Chávez began. Among the most notable strategic objectives related to the surveillance of communications and national security are the following:

- Strengthening and expanding the Military Intelligence and Counterintelligence for Integrated Homeland Defence system.
- Adapting the legal framework to develop the intelligence and counterintelligence capabilities of the Armed Forces, under the principles of the comprehensive defence of the nation.
- Using citizen information for the security and defence of the country.

- Establishing communications hegemony, including strengthening the regulation and social control of the media and developing a media sector that contributes to the overall defence of the country.
- Strengthening the responsible and critical use of the media as a training tool to promote Bolivarian values.
- Updating and developing the technology platforms for communication and information sharing, ensuring access to timely communication.

Importantly, the Plan of the Nation was approved²⁵ in the National Assembly despite opposition, and has resulted in criticism. This can be seen in a statement²⁶ issued by the Academy of Political and Social Sciences of Venezuela, which said that “the government plan deepens the trend to politicise the activity of the National Armed Forces and merge the civil administration and the military, which is underpinned by an overemphasis of the idea of the safety of the nation.” This has been “aggravated by introducing a permanent state of emergency and increased the militaristic character of government and public administration.”

Moreover, the government in recent years has strengthened the intelligence agencies of the state, consolidated registration systems and other citizen data, and developed legal instruments to regulate social networking and protect its citizens. Here are some examples:

- Creating the Deputy Minister of Social Networks,²⁷ CESPPA, the Counterintelligence Directorate SEBIN,²⁸ and forensic laboratories (CENIF) to support criminal investigations using ICTs.²⁹
- Drawing on the Administrative Identification System for Migration and Aliens³⁰ (SAIME), the data capturing system used by the National Electoral Council,³¹ the Military Register

1 www.tsj.gov.ve/legislacion/constitucion1999.htm

2 www.tsj.gov.ve/legislacion/ledi.htm

3 www.suscerte.gob.ve/media/filer_public/16/c7/16c7e2e2-5acf-4e18-84ea-f9bc5893abc4/1ley-sobre-proteccion-a-la-privacidad-de-las-comunicaciones.pdf

4 www.tsj.gov.ve/legislacion/dmdfe.htm

5 www.conatel.gob.ve/files/leyrs.pdf

6 www.cnti.gob.ve/images/stories/documentos_pdf/leydeinfogobierno.pdf

7 www.mp.gob.ve/LEYES/CODIGO_OPP/index.html

8 www.uc.edu.ve/uc_empresas/LOTIC.pdf

9 www.casai.com.ve/chartisint/internet/VE/es/files/Ley-Organica-Contra-la-Delincuencia-Organizada-y-Financiamiento-al-Terrorismo_tcm1286-533853.pdf

10 www.menpet.gob.ve/repositorio/imagenes/file/normativas/leyes/Ley_Organica_de_Seguridad_de_la_Nacion.pdf

11 www.mindefensa.gob.ve/fundacionmuroto/imagenes/ZonaDescargas/LOFANB.pdf

12 www.conatel.gob.ve

13 espaciopublico.org/index.php/biblioteca/doc_download/491-reglamento-del-cesppa

14 www.minci.gob.ve/el-ministerio

15 es.wikipedia.org/wiki/Servicio_Bolivariano_de_Inteligencia_Nacional

16 www.cantv.com.ve

17 www.suscerte.gob.ve/cenif

18 www.oas.org/es/cidh/expresion/index.asp

19 www.summit-americas.org/SIRG/2012/041412/mandates_sc_es.pdf

20 www.oas.org/es/cidh/expresion/showarticle.asp?artID=927&IID=2

21 www.ultimasnoticias.com.ve/noticias/actualidad/politica/venezuela-se-retira-de-la-cidh.aspx

22 www.un.org/es/icj

23 www.elnuevoherald.com/2014/06/28/1786572/venezuela-deplora-declaraciones.html

24 www.nicolasmaduro.org.ve/programa-patria-venezuela-2013-019/#.U59xO3YvCSp

25 albaciudad.org/LeyPlanPatria

26 goo.gl/UvoUai

27 www.ultimasnoticias.com.ve/noticias/actualidad/politica/gobierno-crea-vice-ministerio-para-redes-sociales.aspx, tn.com.ar/internacional/maduro-creo-un-ministerio-de-redes-sociales_438424

28 The Directorate of Counterintelligence (SEBIN) refers to the Interior Intelligence and Counterintelligence service in Venezuela. This directorate is responsible for the coordination of computer services and coordination of strategic analysis.

29 www.suscerte.gob.ve/cenif, www.taringa.net/posts/noticias/15335864/El-hacker-argentino-que-trabajo-para-Chavez.html

30 www.saime.gob.ve

31 www.cne.gob.ve/web/sistema_electoral/tecnologia_electoral_descripcion.php

for Comprehensive National Defence³² and the National Incident Management System³³ (VenCERT).

- Creating networks of cooperating patriots,³⁴ citizen policing committees³⁵ and Special Brigades to tackle those who promote violence,³⁶ and which manage citizen information to secure the defence of the nation.
- The implementation of the Law on the Use of Social Networks³⁷ and the Law on the Protection of the Privacy of Citizens.³⁸

Venezuela currently finds itself in a difficult political and socioeconomic situation. This has led to significant levels of scarcity and shortages,³⁹ insecurity,⁴⁰ high levels of inflation,⁴¹ censorship of traditional media communications, which has limited access to information,⁴² and social protests. According to the Penal Forum,⁴³ in the period February-April 2014, 41 people were killed, 80 cases of torture occurred and 2,500 arrests were made⁴⁴ during social protests, as reported to the Attorney General's Office. However, in the official report⁴⁵ of the public prosecutor, only one case of torture was recorded.

Given this reality, citizens have used social networks⁴⁶ and email to learn, communicate, organise and report on violations of human rights and undemocratic behaviour when it comes to the Armed Forces re-establishing public order during the protests. At the same time, the internet has been used by civil society and student movements to promote peaceful protests.

Meanwhile, various agencies of the government that ensure national security found a way to identify dissidents on social networks, and used the internet to stay informed about the actions of the opposition. They also implemented a series of actions that affected the privacy of communications of citizens, and conducted computer espionage with the support of the government and the explicit support of CANTV, whose president was also a minister of the government. Moreover, the government increased control of the media, affecting freedom of expression and other media freedoms. Among the most emblematic cases are:

Control of communications

- Taking TV channels off the air without legal formalities, and through making fast and deliberate decisions without any procedure,⁴⁷ as in the case of international channel NTN24.⁴⁸
- Blocking Twitter⁴⁹ and restricting access to content posted using Twitter.⁵⁰
- Blocking and restricting access to websites⁵¹ (twimg.com, pastebin.com, bit.ly, zello.com) and news portals nationwide.⁵²
- Blocking social networks such as Zello's voice application.⁵³
- Censoring social networks.⁵⁴

- Blocking the internet⁵⁵ in the city of San Cristóbal from 19 to 21 February 2014.
- Cancelling television and radio programmes critical of the government.⁵⁶
- Censoring traditional media.⁵⁷
- Blackouts (i.e. cutting electricity).⁵⁸
- Monitoring and analysis of behaviour on social networks⁵⁹ through CESPPA.⁶⁰
- Monitoring of social media by the Deputy Minister of Social Networks, as seen in the case of Minister Delcy Rodríguez.⁶¹
- The purchase of the only television channel critical of the government (GLOBOVISION) by a company linked to the government.⁶²
- The purchase of the newspaper *El Universal*, which was critical of the government.

Interception of communications

- The interception of emails of individual citizens⁶³ to determine their connection with alleged plans to destabilise the government,⁶⁴ authorised by the Attorney General in 2014.
- The interception of telephone calls from various members of the opposition in the National Assembly, such as Juan José Caldera⁶⁵ and Maria Corina Machado,⁶⁶ during the 2013 presidential election.

- The interception of emails from the president of the Venezuela Awareness Foundation⁶⁷ by the Ministry of Interior and Justice.⁶⁸

Access to the information of users on social networks and web portals

- Accessing and publishing the private details of citizens through the Twitter account @Drodri-guezMinci by the MPPIC⁶⁹ in January 2014.⁷⁰ In this instance, a list that contains data about the holiday destinations abroad of 27 Venezuelans was exchanged between opposition leaders.
- Unauthorised access to the personal Twitter accounts @RBADUEL and @AndreinaBadue.⁷¹
- Attacks on Twitter accounts and websites⁷² that reported on the cancer of President Chávez, such as the account of the journalist Casto Ocando.⁷³
- Real-time monitoring of the computer activities of citizens,⁷⁴ with the authorisation of SEBIN.
- SEBIN targeting hackers who tried illegally to access government computer portals.⁷⁵

Using software to monitor web applications and internet traffic

- According to a report by Miguel Useche,⁷⁶ a study by The Citizen Lab⁷⁷ at the University of Toronto found that the Venezuelan government is a client⁷⁸ of the security company Blue Coat Systems,⁷⁹ and uses the service PacketShaper,⁸⁰

32 notihoy.com/en-gaceta-oficial-oficializan-aprobacion-de-la-ley-de-registro-y-alistamiento

33 www.suscerte.gob.ve/noticias/2014/06/10/puesto-en-marcha-el-sistema-nacional-de-gestion-de-incidentes-telematicos-vencert

34 www.franciscoalarcon.net/2014/05/redes-de-patriotas-cooperantes-se.html, www.eluniversal.com/opinion/140509/patriotas-cooperantes-sapearan-a-sapos

35 www.mp.gob.ve/c/document_library/get_file?p_l_id=29950&folderId=420779&name=DLFE-2509.pdf

36 www.eluniversal.com/nacional-y-politica/protestas-en-venezuela/140626/se-creo-la-brigada-especial-contra-generadores-de-violencia

37 www.noticierodigital.com/2014/05/dip-oficialista-farinas-pide-a-la-an-lesgilar-sobre-uso-de-las-redes-sociales

38 www.noticierodigital.com/2012/12/propondran-ley-de-proteccion-a-la-intimidad-y-la-vida-privada-de-los-ciudadanos

39 informe21.com/escasez, www.eluniversal.com/economia/140429/en-12-meses-se-acelero-la-escasez-de-alimentos-basicos, eltiempo.com.ve/venezuela/salud/gremio-estima-que-escasez-de-medicamentos-ronda-40/122632

40 prodavinci.com/blogs/las-muertes-por-violencia-en-venezuela-comparadas-con-el-mundo-por-anabella-abadi-m-numeralia, www.el-nacional.com/alejandro_moreno/Tasa-homicidios-Venezuela_o_407959364.html

41 cecede.org.ve/boletin-oe-venezuela-con-la-inflacion-mas-alta-de-america-latina/, cecede.org.ve/wp-content/uploads/2014/06/Venezuela_CREES_03JUN2014.pdf, www.el-nacional.com/economia/Pi-Venezuela-inflacion-paises-Latinoamerica_o_427157376.html

42 www.prensa.com/impreso/panorama/venezuela-sip-%C2%B4maduro-censura-medios-tradicionales-e-internet%C2%B4/305897, www.sipiapa.org/sip-repudia-estrategia-de-censura-del-gobierno-de-venezuela

43 foropenal.com

44 www.lapatilla.com/site/2014/04/30/foro-penal-venezolano-denuncia-ante-fiscalia-80-casos-de-tortura-durante-protestas

45 www.mp.gob.ve/c/document_library/get_file?uid=52da67d8-ae04-4ebd-g1de-dbf770de03c&groupId=10136

46 www.elsiglo.com.ve/article/72030/Redes-sociales-en-Venezuela--Del-faranduleo-a-trinchera-informativa-ciudadana

47 www.derechos.org/ve/pw/wp-content/uploads/Informe-final-protestas1.pdf, páginas 82-92

48 noticias.univision.com/article/1851146/2014-02-14/america-latina/venezuela/maduro-confirma-la-salida-del-aire-del-canal-colombiano-ntn24

49 ipys.org.ve/alerta/caracas-red-twitter-sufrio-bloqueo-parcial-cuando-usuarios-difundian-informacion-sobre-hechos-violentos-registrados-en-el-pais

50 www.eluniversal.com/vida/140214/bloomberg-confirma-que-gobierno-venezolano-bloqueo-imagenes-de-twitter

51 skatox.com/blog/2014/02

52 www.entornointeligente.com/articulo/2209577/VENEZUELA-Portal-de-noticias-Al-Momento-360-sufre-bloqueo-parcial-16032014

53 www.lapatilla.com/site/2014/02/21/bloquean-aplicacion-zello-en-venezuela-tuits, www.infobae.com/2014/03/06/1548288-zello-la-aplicacion-terrorista-los-estudiantes-venezolanos

54 es.panampost.com/marcela-estrada/2014/02/14/censura-en-venezuela-alcanza-redes-sociales

55 www.maduradas.com/se-arrecia-la-dictadura-maduro-busca-bloquear-la-internet-en-venezuela, skatox.com/blog/2014/02

56 www.noticierodigital.com/2014/05/conatel-ordeno-la-suspension-del-programa-radial-plomo-parejo, informe21.com/artey-espectaculos/cancelan-el-programa-de-luis-chataing-en-televen

57 apevex.wordpress.com/category/censura-a-medios-de-comunicación

58 voces.huffingtonpost.com/fernando-nuneznoda/blackout-informativo-en-v_b_4812480.html

59 eltiempo.com.ve/venezuela/redes-sociales/las-redes-en-la-miradel-cesppa/131622

60 Dirección de Estudios Tecnológicos y de Información y la Dirección de Procesamiento y Análisis de la información.

61youtu.be/gHqEYaKgyU4, www.maduradas.com/delcy-rodriguez-llama-a-la-oposicion-enemiga-y-le-anuncia-derrota-en-las-redes-sociales

62 www.abc.es/internacional/20131118/abci-globovision-201311181903.html

63 Maria Corina Machado (former deputy), Diego Arria (former IDB director), Pedro Burelli (former PDVSA director), among others.

64 www.noticias24.com/venezuela/noticia/241035/luisa-ortegadiaz-aseguro-que-todas-las-personas-denunciadas-por-jorge-rodriguez-seran-investigadas/cç, www.noticias24.com/venezuela/noticia/240859/alto-mando-politico-muestra-evidencias-que-vinculan-a-politicos-y-empresarios-en-un-plan-macabro, www.noticias24.com/venezuela/noticia/240876/en-fotos-presentan-correos-electronicos-que-muestran-golpe-militar-contra-nicolas-maduro, www.lapatilla.com/site/2014/05/30/la-fiscalia-admite-que-el-sebin-espia-a-maria-corina-machado

65 zdenkoseligo.blogspot.com/2012/09/sobre-la-grabacion-del-diputado-caldera.html

66 www.notitarde.com/Seccion/Espionaje-telefonico-denuncia-Maria-Corina-Machado/2011/11/28/79239

67 www.lapatilla.com/site/2011/06/16/cubanos-realizan-espionaje-digital-en-venezuela

68 El Ministro Jesse Chacón en el 2006 admitió públicamente que la organización era blanco de espionaje electrónico

69 Ministry of Information and Communications.

70 www.ifex.org/venezuela/2014/01/10/intimidacion_ministra_comunicacion/es

71 resistenciav58.wordpress.com/2014/06/21/comunicado-de-la-familia-baduel-ante-ataques-de-hacker

72 www.lapatilla.com/site/2011/10/01/la-patilla-informa-a-sus-lectores-sobre-ataque-a-su-plataforma

73 runrun.es/runrunes/26882/%C2%B4hackeo-majunche-pero-con-billete-y-tecnologia-china.html

74 https://adribosch.wordpress.com/2013/01/31/venezuela-sebin-usa-hackers-para-violar-la-privacidad-de-los-ciudadanos

75 www.noticias24.com/venezuela/noticia/150427/sebin-combate-los-hackers-que-intentan-vulnerar-el-orden-institucional-en-venezuela

76 skatox.com/blog/2014/02/23/disminucion-de-la-libertad-de-la-informacion-en-la-red-en-venezuela

77 https://citizenlab.org

78 skatox.com/blog/images/2014/02/planetbluecoat.jpg

79 https://www.bluecoat.com

80 Cloud-based monitoring for web applications and network devices, with the capability to control unwanted traffic service in real time, allowing for the filtering of applications by category. www.bluecoat.com/sites/default/files/documents/files/PacketShaper_Application_List.c.pdf

which allows more control in the monitoring of internet traffic and web applications.

Given these government actions, citizens and various national and international organisations have warned of violations of human rights, the privacy of communications of citizens, the freedom of speech and internet neutrality. These include:

- A communiqué⁸¹ issued by the free software communities of Venezuela in favour of freedom of speech and network neutrality in Venezuela.
- A statement⁸² issued by organisations in the Forum for Life⁸³ pointing out serious human rights violations in Venezuela, from the criminalisation of social protest, to the systematic harassment of journalists and media, among others.
- Complaints by MCM⁸⁴ to the National Office in which it claims to be a victim of identity theft, computer espionage, telephonic espionage,⁸⁵ eavesdropping and forgery.
- Complaints by Pedro Burelli⁸⁶ before a court in the state of California, in the United States, in which he requested an independent investigation of the content of intercepted emails implicating him in an alleged assassination attempt in 2014.
- Reporters Without Borders (RSF) warning of internet censorship and access to social networks in Venezuela by CONATEL, which represents a decline in freedom of expression in Latin America.⁸⁷

- A report⁸⁸ issued by civil society organisations where human rights⁸⁹ violations in the period February-April 2014 in Venezuela are detailed. Cases of arbitrary arrests and violations of due process, violations of freedom of expression and attacks on journalists and others are presented in this report.

Conclusions

- In December 2013, a new government plan that seeks to strengthen the defence of the nation – among other things by increasing intelligence and counterintelligence systems where the collating of information on citizens is a fundamental component – was started. This included monitoring the media.
- The events between February and April 2014 were a challenge for the government. During civil society protests undemocratic acts were committed under the pretext of defending national security. These included violations of human rights, the violation of the privacy of the communications of citizens, the violation of freedom of expression and opinion, and blocking the internet, among others. In this context, social networks and email became essential to share any information that the state media chose not to report on, and the private media was skewed by self-censorship.
- During this period the intelligence agencies in the government increased measures that were aimed at preventing the diffusion, dissemination and publication of content dealing with the protests on social media sites and through the traditional media. However, citizens found ways to denounce abuses by the armed forces through initiatives such as the “SOS Venezuela”⁹⁰ campaign that gave international visibility to the abuses. Regulators blocked internet communications, Twitter, Zello, web pages and news portals, as well as monitored and analysed the behaviour of social networks as a way to neutralise the organisation of so-

cial movements and the flow of information content against the government. According to journalist Fernando Nunez Noda,⁹¹ intelligence agencies promoted “espionage, lifted records and monitored topics that are inconvenient to those in power,” particularly CESPPA. These actions reveal how the government has established mechanisms and defined strategies for surveillance of communications and to prevent the flow of information through social networks that allow citizens to be informed about events of national impact, and which can undermine national security.

- Importantly, the cases presented, such as intercepting emails, phone calls, and Twitter communications of opposition leaders, among others, reflect a kind of political espionage that might be going on in Venezuela, and could lead to the criminal liability of the actors involved. This includes cases of illegal access to and publication of the data and private information of users of social networks, websites and computer systems. Many of the reported cases were managed by government agencies without due process or the respective court orders to record and disseminate citizen information. This violates the rights to privacy, honour and reputation in the communications of Venezuelans.

Given the above, one could conclude that the government has mechanisms for intelligence espionage, found both in political and technical bodies that aim to neutralise and defeat plans that seek to destabilise the nation, as conceptualised in the Homeland Plan 2013-2019. The warnings by civil society and national and international organisations about potential violations that occur in Venezuela are an indicator that citizens are not involved sufficiently in the work of state agencies and public authorities.⁹² The guarantees necessary for the protection and defence of human rights and for the surveillance of communications, such as due process, proportionality, a competent and impartial judiciary, transparency and integrity of communications and systems have not been secured.

Action steps

Government:

- Ensure the independence of public powers and respect for the legal framework when it comes to restrictions on the right to privacy of citizens, and ensure that the collection and use of personal information is clearly authorised by law.
- Encourage dialogue to increase awareness of the implementation of the Plan of the Nation 2013-2019 and its implications for the surveillance of communications.
- Ensure that actions related to the security of the state and the agencies responsible for communications do not violate human rights during the surveillance of citizens.
- Establish mechanisms for independent oversight bodies to ensure transparency in the surveillance of communications.
- Ensure state sovereignty and national security without violating the fundamental rights of citizens.⁹³
- Avoid practices that promote attacks on, threats to and the defamation of internet users.
- Review the nature of intelligence agencies like CESPPA that may be violating the constitutional order and promoting censorship based on the criteria of ensuring the safety and defence of the nation.

Citizens and organisations:

- Establish mechanisms to document and organise cases where surveillance violates the rights of citizens, and present these cases to public protectors, both domestic and international.
- Use applications and methods to ensure that the internet is not blocked.
- Be vigilant about the veracity of the content disseminated through social networks in order to ensure timely and accurate information.

81 skatox.com/blog/2014/02

82 www.derechos.org.ve/2014/02/24/organizaciones-sociales-y-deddh-de-venezuela-difunden-accion-urgente-ante-situacion-del-pais

83 foroporlavida.blogspot.com

84 www.lapatilla.com/site/2014/05/29/maria-corina-machado-denunciara-ante-la-fiscalia-infamia-en-su-contr

85 www.notitarde.com/Seccion/Espionaje-telefonico-denuncia-Maria-Corina-Machado/2011/11/28/79239

86 cnnespanol.cnn.com/2014/07/01/pedro-burelli-presenta-pruebas-forenses-de-la-presunta-falsificacion-de-correos

87 cifrasonlinecomve.wordpress.com/2014/05/04/denuncia-internacional-contra-maduro-por-espionaje-telefonico-y-bloqueo-del-trafico-de-internet, www.eluniversal.com/nacional-y-politica/140312/reporteros-sin-fronteras-alerta-sobre-censura-en-internet-en-venezuela

88 www.derechos.org.ve/wp-content/uploads/Informe-final-protestas1.pdf

89 Programa Venezolano de Educación-Acción en Derechos Humanos (PROVEA) y de la Comisión Inter-Institucional de Derechos Humanos de la Facultad de Ciencias Jurídicas y Políticas de la Universidad del Zulia, Espacio Público, Foro Penal Venezolano, Asociación Civil Justicia, Solidaridad y Paz (FUNPAZ) del estado Lara, Escuela de Derecho de la Universidad Rafael Urdaneta, la Comisión de Derechos Humanos del Colegio de Abogados del estado Zulia, Centro de Derechos Humanos de la Universidad Católica Andrés Bello (CDH-UCAB), el Observatorio Venezolano de Conflictividad Social (OVCS).

90 https://www.youtube.com/watch?v=RYOiafOSZKk

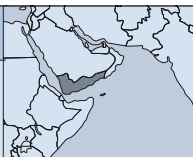
91 www.laverdad.com/politica/44878-un-ente-oficial-para-espionar-twitter.html

92 chile.embaajada.gob.ve/index.php?option=com_content&view=article&id=84%3Apoderes-publicos&catid=1%3Acontenido-embaajada&Itemid=98&lang=es

93 The freedom of expression and information, freedom of association, right to privacy, honour, reputation and private life, and right to privacy of communications.

YEMEN

A country in transition with its share of cyber challenges



Walid Al-Saqaf
www.yemenportal.net

Introduction

Being one of the least-developed countries in the world, it was natural to see Yemen trail all neighbouring Arab countries in utilising information and communications technologies (ICTs). With an internet penetration not exceeding 14%, it was also not surprising to see Yemen rank lowest on the Global Web Index¹ released in 2013 by the Web Foundation. Yet despite suffering from a weak telecommunication infrastructure and lack of human resources in the domain of internet services, the country recently witnessed significant growth in internet usage. Part of this may be attributed to wider use of Facebook in discussing political and social issues and in mobilising mass protests following the emergence of the Arab Spring in December 2010.

After hundreds of protestors were killed, jailed, maimed or injured during the 2011 popular revolts, a peaceful transfer of power deal was secured, ending the 33-year reign of Ali Abdullah Saleh and handing the presidency to his deputy Abd Rabbuh Mansur Hadi. Within the last several years, much has happened in the Yemeni cybersphere, particularly in the area of online freedom of expression. While Yemen's internet is relatively modest and limited in scope and impact, cases of online restrictions, privacy violations, and cyber attacks occurred, as will be described in this report.

A brief background

Under Ali Abdullah Saleh's rule, practices of repression were committed using the 1990 Press and Publications Law and the Penal Code, which restricted free speech on multiple levels under the pretext of protecting national security, religion, foreign relations, etc. Despite the low level of internet activity compared to other countries, cases of website blocking were documented and several individuals complained about surveillance of their phone calls and hacking of their email and Facebook accounts. While there were no documented

cases of digital surveillance in Yemen, some cyber activists have expressed concern that if it is not already the case, surveillance technology will soon be used by the authorities, particularly the national security agency, to spy on digital communication.

While broadcast media remain the most popular method to reach the public, internet has taken a modest share because it grants users the ability to publish, share and consume content much more easily than other forms of media. Internet usage has increased steadily since it was first introduced in 1996 by the Ministry of Telecommunication's Public Telecommunications Corporation (PTC) and Teleyemen, which was formed in 1990 as a joint company owned by PTC and the United Kingdom's Cable and Wireless plc. Today, those two companies monopolise the internet service provider (ISP) business as no private companies are allowed to operate. This has created an environment that lacks accountability and transparency and in which not many choices are provided to the public.

An environment of fear

One of the country's most feared arms is the national security apparatus – sometimes called state intelligence – which, as is the case in many Arab countries, often keeps track of dissidents and monitors their activity. Prominent blogger and founding member of the Internet Society Yemen Chapter Fahmi Al-Baheth was one of the victims of this apparatus when he was told he would be detained or caused to “disappear” because of his online activities in support of the 2011 anti-Saleh popular revolution. Al-Baheth described how he discovered that the phone line of a fellow activist was tapped when a national security officer listed to him the people he called a day earlier. While it is known that the intelligence apparatus monitored and tracked regular dissidents and political activists, it has become clear that they have started to track and monitor cyber activists as well.

Among the more aggressive forms of attacks that targeted online journalists and activists during Saleh's rule was the blocking of websites by the government-run ISP Yemen Net, based on instructions from the national security. This practice has been verified by many websites that contained dissident

content or even news and opinion articles that contained criticism of the Saleh regime. In some cases, extensive long-term blocking of websites effectively killed their prospects and led to their permanent shutdown due to the lack of access for readers. While the government announced that blocking of news websites ceased in 2012, websites that allegedly contained socially inappropriate content (e.g. pornography and nudity) remained blocked.

A doctoral study² I carried out during 2010-2012 has demonstrated that forms of restrictions that targeted Yemeni websites and their operators ranged from prosecution to intimidation, and from hacking to filtering. Such violations have resulted in an environment of fear where online journalists and even regular users succumbed to self-censorship to avoid harm.

Breaches of privacy

As Yemen has no laws or regulations protecting the privacy of citizens, cases where private information was published online have emerged. The monopoly over the ISP sector maintained by the government resulted in a lack of transparency and accountability when it comes to the data transferred through or stored on the local servers. According to a source who requested to stay anonymous, the national security has backdoor direct access to the servers of Yemen Net, which exposes sensitive and personal data of millions of Yemeni users to potential abuse. The United States Department of State's 2012 human rights report³ has also given credibility to reports that the Yemeni authorities monitored email and internet chat rooms.

An app entitled Yemen Phone was produced, allowing anyone to access millions of Yemeni citizens' names and phone numbers and even physical addresses. Such an app, according to several privacy advocates, is a violation of privacy and should have been investigated by the authorities.

The Yemeni government was accused of breaching the privacy of citizens as early as 2009, when subscribers to the Yemen Mobile GSM service, which is run by the PTC, were assigned a special ring tone⁴ in the form of a national song without their consent, causing outrage among some subscribers.

The lack of sensitivity to citizens' privacy was demonstrated again in 2013 when the Supreme Commission for Elections and Referendum made

public the databases of citizens who applied to work in voter registration positions. Initially, all the applicants' information was made public, including their name, data and place of birth, academic qualifications, place of work, addresses, telephone numbers, email addresses, and even their national identity card numbers. To many privacy advocates such as Fahmi Al-Baheth, this was a major privacy breach that was only partially remedied by removing telephone numbers and email addresses while keeping all the other information public and accessible on the Commission's official website.⁵

Victims of hacking

The fact that Yemen is a relatively inexperienced nation when it comes to technical internet-related operations has contributed to creating a fertile environment for hacking websites, emails and social media accounts. The lack of awareness of how the technology works and how to take proper precautions to prevent attacks was exploited during the peak of the popular revolution during 2011-2012. According to an anonymous source working for Yemen Net, the national security apparatus hired a large team of hackers in 2011 to target many websites, personal social media accounts and email accounts.

Hamza Alshargabi, who was active on Facebook in supporting the 2011 anti-Saleh uprising, indicated that his Facebook account and those of many of his friends were hacked during that period, probably due to their activities in support of the revolution. He discovered that his account was hacked when he realised that notifications were marked as “read” during the time he was logged off. He further indicated that an anonymous source working for Yemen Net verified the existence of advanced spying tools utilised by the national security.

Among the highest profile individuals attacked during that time was Nobel Laureate Tawakkol Karman, whose Facebook account was hacked multiple times. Due to her vocal opposition to the Saleh regime, she was subject to both physical and cyber attacks over the course of the revolution. In a recent correspondence, she described how Facebook decided to close her account due to the apparent changing of the telephone number used for verification. She remained unable to get her account back despite applying the instructions provided to her by Facebook. She also indicated that her email account was attacked several times, but not hacked due to the added security measures she has taken.

1 <https://thewebindex.org/data/index>

2 The full text of the study can be found at: oru.diva-portal.org/smash/record.jsf?pid=diva2:710477

3 www.state.gov/j/drl/rls/hrrpt/2013/nea/220385.htm

4 A news story in Arabic can be accessed at: marebpress.net/news_details.php?sid=16695&lng=arabic

5 web.scer.gov.ye/ar-page.aspx?show=47

But it is not only oppositional websites that got hacked. In 2011, a major governmental website was hacked for political reasons by elements in exile calling for the secession of south Yemen from the north. The attack on the website was possible after hacking the email account of its manager, who requested to stay anonymous. Thereafter, the hacker took over the whole domain by changing the name server settings on the GoDaddy domain registrar. While it was possible to fix the domain configuration after reclaiming the email address, the incident highlights the level of sophistication and extent of the cyber warfare that went on during that turbulent period of Yemen's recent history.

While it would be expected that such incidents would subside after the transfer of power in 2012, in reality, such cases not only continued, but also increased in depth and breadth. One of the most severe attacks⁶ targeting several websites happened in April 2014 when at least six news websites were hacked all at once in what appeared to be a planned systematic attack. While it was not evident who was behind it, website owners accused the Yemeni authorities.

Much of the talk about who is behind the hacking and malicious attacks remains speculation due to the lack of technical documentation and research. Given that hacking tools and know-how are accessible globally by anyone willing to invest time and energy to find them, it is likely that different political rivals were involved in attacks and counter-attacks for various motives. Prior to the Arab Spring, however, it was evident that the government was more pervasive in attacking activists and online journalists. When the power transfer deal went into force in 2012, it was hoped that those attacks would subside. However, it was later found that attacks resumed, but this time, they seem to have come from different players.

In June 2014, a Yemeni media report⁷ identified signs that surveillance and wiretapping will resume but now under the guidance of the new president, and will target dozens of journalists, activists and military leaders. According to the report, the feared national security apparatus will be used by Jalal Hadi, who is the son of the new president, to track and monitor phone calls and activities of those who could be a "threat to the transitional period."

Conclusion

While Yemen remains one of the countries with the lowest internet penetration levels, it has had its share of troubles when it comes to surveillance, privacy, security and human rights on the internet. The few incidents described above present examples of violations that ranged from threats to bloggers and cyber activists to website filtering and hacking attacks. They constitute a major concern to human rights advocates who argue that free speech on the internet needs to be defended vehemently, particularly during this critical period for Yemen: a country undergoing massive political and social transformations.

One of the major challenges noted was the lack of sufficient skills on the part of users of the technology to keep their transactions safer and their websites and accounts protected. The need to address this challenge is pressing given the growth in internet usage the country is expected to witness. It is also important given that the political transition will require the free flow of information and ideas to contribute to the various new developments, from elections to new forms of cyber dissent.

The lack of legal frameworks to protect freedom of expression and privacy is another major concern because the status quo gives authorities a free hand to practice online restrictions on free speech. The revolution that emerged in 2011 and led to the downfall of Saleh's presidency had the promotion of free speech and access to information among its main goals. As a result, any deterioration in that respect would carry with it a great deal of disappointment, particularly after so many lives were sacrificed to achieve the desired political change.

Unfortunately, however, Yemen faces numerous challenges ranging from poverty to security and from water shortages to power outages. Those challenges have used up most of the energy of the government, private sector and even civil society, who have given human rights on the internet a back seat in favour of other more pressing issues. Nonetheless, there remains hope in bringing the violations against online journalists and activists to the forefront, particularly with the rise in social media use and after the launch of the Internet Society Yemen Chapter, whose goals include protecting security, privacy and freedom of expression on the internet. The chapter's role could be significantly important given that improving human rights and freedom of expression helps stability, and stability in this part of the world is crucial for the fight

against terrorism and for protecting the Bab Al-Mandab Strait, through which most of the world's oil passes.

These challenges facing Yemen were also mentioned in the Arab Internet Governance Forums (IGF) in 2012 and 2013 in Kuwait and Algiers respectively, and these were useful to compare experiences with other countries in the region and learn as the country moves forward.

The threats that Yemeni internet users are facing are but a reflection of the risks that are associated with using the internet at large. Discussions at the IGF and efforts undertaken by international bodies such as ICANN and global software platforms to provide more secure services, better regulatory models and more human rights-conscious policies, will all have a positive impact on Yemen as well.

Action steps

For Yemen to confront the challenges described earlier, it is important to address the issues based on the particular subjects in question.

Firstly, the low internet penetration level in Yemen is a hindrance because it deprives the population of taking advantage of the enormous benefits that the internet has to offer. It also limits the number of people with enough skills and know-how to

provide training and develop solutions that could tackle issues that are of a technical nature, such as securing accounts, tracking attacks, etc. To address this, the government's monopoly over the ISP business should end, and the private sector needs to be able to provide adequate, secure and competitive services to reduce the cost and increase accessibility, particularly in remote areas.

When it comes to acts of surveillance, civil society needs to do more systematic research to identify how surveillance is being carried out. As of mid-2014, reports of digital surveillance remain speculative and lack empirical evidence to back any claims. Researchers in Yemen, perhaps in collaboration with international donors and institutes, could work together in tracking and identifying cases of digital surveillance and suggest solutions.

Finally, there will be a need for advocacy groups to coordinate their actions, hold discussions with different stakeholders, and suggest policies to limit abuse of power, whether by the government or any other party. For this to be done, it will be necessary to engage more with international and regional actors in this area and pull resources to launch systematic and long-term campaigns and projects that could put the issue of human rights on the internet at the forefront.

⁶ Read an Arabic story about those attacks at: www.sanaapress.net/news9376.html

⁷ Read the Arabic story at: marebpress.net/mobile/news_details.php?sid=100613

ZIMBABWE

Surveillance under the garb of rule of law



MISA-Zimbabwe
Nhlanhla Ngwenya
www.misazim.com

Introduction

Zimbabwe is a multi-party democracy with a population of 13 million, located in southern Africa. As the country's political crisis worsened between 2000 and 2008, with swelling opposition against the ruling ZANU-PF party which has governed Zimbabwe since its independence in 1980, the government reacted by enacting a raft of laws meant to control and restrict free and active citizenry. These included the Interception of Communications Act. The law provides for the "lawful interceptions and monitoring of certain communications during their transmission through a telecommunication, postal or any other related system or service in Zimbabwe."¹ While it was always suspected that the government conducted communications surveillance of its opponents and human rights activists, the enactment of the law simply provided a legal basis for the practice. In October 2013 the government sought to entrench the surveillance law through Statutory Instrument (SI) 142 on Postal and Telecommunications (Subscriber Registration) Regulations. The SI provides for the establishment of a central database of information about all mobile phone users in order to assist emergency services and law enforcement agencies and to protect national security. This was despite the fact that five months prior, in May 2013, Zimbabwe had adopted a new constitution with better safeguards for the enjoyment of freedom of expression. And as things stand there is discord in the legislative framework caused by disharmony between the statutes and the constitution, providing fertile ground for violation of citizens' basic liberties including their right to privacy.

Policy and political background

After 33 years of debate and failed attempts at constitutional reform, Zimbabwe finally adopted a new constitution in May 2013 to replace the Lancaster House Constitution, which ushered in the

country's independence. Key among the content of the new charter is an expansive Bill of Rights, which among other liberties, grants for the first time in Zimbabwe's history explicit guarantees for freedom of expression, media freedom and access to information.

Despite this, the country is still to align its laws to the new constitution, thereby ensuring that a gamut of laws remain in place to curtail freedom of expression. These include the Access to Information and Protection of Privacy Act, the Criminal Law (Codification and Reform) Act, the Interception of Communications Act, and the Official Secrets Act, among other laws. These acts separately and/or collectively severely erode Zimbabweans' right to freedom of expression. Although the Interception of Communications Act is the one that is more relevant to online communication, the authorities can still use the other laws to press charges against those deemed to have crossed the line when expressing themselves through online platforms. The recent arrest of a teenager, Gumisai Manduwa,² over a Facebook post on President Robert Mugabe, and threats of the arrest of those who may have provided information to an online Facebook character called *Baba Jukwa*,³ demonstrate the extent to which the state can go in trying to sniff out those expressing themselves online.

² Gumisai Manduwa appeared in court in January 2014 facing charges of contravening Section 33 of the Criminal Law (Codification and Reform) Act for allegedly insulting President Robert Mugabe. Manduwa had posted on Facebook claims that Mugabe had died and his body was being preserved in a freezer. Manduwa's arrest was the second such case following the arrest in 2011 of Vikas Mavhudzi, who had also posted a Facebook comment that suggested the opposition should emulate pro-democracy protests in Egypt. He was charged with subversion and spent close to a month in prison. He was subsequently acquitted in 2013 for lack of evidence.

³ Baba Jukwa is a faceless online blogger with a Facebook account that has gained popularity in Zimbabwe for exposing alleged unpleasant secrets of the government and the ruling party, ZANU-PF. On 11 May 2014, a state-run newspaper, *The Sunday Mail*, alleged that individuals behind the Facebook account had been unmasked by unnamed hackers in New Zealand, who had hacked into Baba Jukwa's private Google account. The hackers reportedly then passed the information to Zimbabwean state authorities. Since then the state-controlled newspapers have been feasting on the story, serialising private correspondence between Baba Jukwa and his associates as well as informants calling on the authorities to arrest them and charge them under the country's security laws.

¹ The Interception of Communications Act (Chapter 11:20), enacted in Zimbabwe in August 2007.

Legislative paralysis provides room for surveillance

Although the new Zimbabwean constitution has received its fair share of criticism, especially as it relates to executive authority,⁴ there is general consensus that it is far more democratic than its predecessor, as it seeks to promote and protect wholesale civil liberties. Further, it obligates the "[s]tate and every person, including juristic persons, and every institution and agency of the government at every level" to "respect, protect, promote and fulfil the rights and freedom set out" in the Declaration of Rights provided for in Chapter 4 of the constitution. One of the key elements of the constitution is its protection of citizens' right to privacy.

Article 57 states:

Every person has the right to privacy, which includes the right not to have—

- (a) their home, premises or property entered without their permission;
- (b) their person, home, premises or property searched;
- (c) their possessions seized;
- (d) the privacy of their communications infringed; or
- (e) their health condition disclosed.

This provision is anchored on international human rights law and instruments such as the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights, which Zimbabwe ratified in 1991.

Besides constitutionally outlawing infringement of citizens' right to privacy, the constitution also guarantees citizens' freedom to express themselves and their right of access to information. It does this under Articles 60 and 61.

For example, Article 60 stipulates as follows:

- (1) Every person has the right to freedom of conscience, which includes—
 - (a) freedom of thought, opinion, religion or belief; and
 - (b) freedom to practise and propagate and give expression to their thought, opinion, religion or belief, whether in public or in private and whether alone or together with others.

⁴ New Zimbabwe. (2013, February 5). NCA slams Constitution, urges 'No' vote. New Zimbabwe.com. www.newzimbabwe.com/news-10197-NCA+urges+rejection+of+new+constitution/news.aspx

Article 61 states:

- (1) Every person has the right to freedom of expression, which includes—
 - (a) freedom to seek, receive and communicate ideas and other information;
 - (b) freedom of artistic expression and scientific research and creativity; and
 - (c) academic freedom.

Cognisant of the fact that freedom of expression is not absolute, the constitution then provides precise and narrow scope within which the right could be limited under Article 61 (5). These limitations are in line with international instruments on freedom of expression and in particular satisfy the three-part test for measuring restrictions on freedom of expression; this test has been elaborated on in judgments delivered by international courts on matters related to human rights treaties.⁵

However, despite this development, Zimbabwe has continued to retain interception of communication laws – disguised as upholding the rule of law – specifically the ICA and SI 142, which contain provisions that are in conflict with the new constitutional dispensation. For example, while the new constitution provides for the right to privacy and free expression, the ICA legalises the interception of one's communication and actually establishes an interception of communications unit named the Monitoring of Interception of Communications Centre. The Centre is staffed, controlled and operated by designated experts of the state.⁶ The process of establishing the Centre, its composition and work is opaque, and as a result there is no accountability around its activities.

Although the ICA provides for procedure for interception, the requirements to obtain a warrant of interception remain vague and subject to abuse. According to the law, an application for interception may be made to the ministry responsible for transport and communications by the Chief of the Defence Intelligence, the Director General of the President's Department of National Security, the Commissioner General of the Police and the Commissioner General of the Zimbabwe Revenue Authority. A warrant for interception can be issued where there is "reasonable suspicion" that a serious offence has been, is being, or will probably be committed, or to prevent

⁵ Center for Law and Democracy. (2010). Restricting Freedom of Expression: Standards and Principles. Background paper for meetings hosted by the UN Special Rapporteur on freedom of opinion and expression. www.law-democracy.org/wp-content/uploads/2010/07/10.03.Paper-on-Restrictions-on-FOE.pdf

⁶ MISA-Zimbabwe. (2010). *An Analysis of Amendments to Media Laws in Zimbabwe Since the Year 2005*. Harare: MISA-Zimbabwe.

a threat to national security, the economic interests of the state or public safety.⁷ There is no clarity on what constitutes reasonable suspicion and how it is determined. Neither is there an explanation on what constitutes sufficient grounds to prove that an offence is likely to be committed. Further, the Act defines “serious offence” as conduct constituting an offence punishable by a maximum jail sentence of up to four years. There are a number of offences that fall under this category, which include abortion, assault perjury, reckless driving and violating a corpse. Lack of clearly listed offences considered serious under the interception law leaves the Act vague and open to abuse by those in authority.

To make matters worse, the minister’s decisions are not subject to court review. Instead, it is only the Attorney General, who is a political appointee, who has authority to review the conduct of the minister and the exercise of their power. And this is only done within three months of the end of each year, thereby allowing potential abuse of the law to go unchecked and giving state agents latitude to intercept citizens’ communications without restraint.

Besides giving wide discretionary powers in the administration of the Act to the relevant minister while circumventing effective judicial oversight, the Act also places harsh duties on service providers to undertake interception and monitoring, and gives authorities any assistance they may require to snoop into private communication. Refusal to provide assistance is punishable by up to three years imprisonment.

There are no provisions in the Act guaranteeing the safe keeping or storage of information or data collected through interception. Neither is an individual whose information has been intercepted informed after the completion of investigations, nor does the law provide specific timeframes within which the information should be destroyed when no longer needed. Instead, the Act simply enjoins the responsible state officer to destroy it “as soon as possible after it is used for the purposes of (the) Act.”⁸

Instead of addressing the law’s patently intrusive nature and aligning it with the new constitution, the state seemingly entrenched the harmful effects of the Act through SI 142. The Instrument calls for the establishment of a database of information about all mobile phone users in the country; compulsory SIM card registration; and the release of private information to the police in the absence of a search warrant, supposedly with the objec-

tive of assisting emergency services, assisting law enforcement agencies and safeguarding national security.⁹ While it is acknowledged that concerns around e-crimes and state security would require legislative intervention, SI 142 generally fails the democratic test as it simply legalises intrusion of citizens’ privacy guaranteed in the constitution.

As Gwagwa¹⁰ argues, for example, mandatory registration provides the government with the means to track citizens’ whereabouts – and by extension the people with whom they associate – and creates a situation in which personal data could theoretically be shared between government departments, allowing for the creation of individual profiles based on data stored elsewhere.

Gwagwa further argues that while the regulations stipulate that no information shall be released if doing so would violate the constitution, by empowering the police to request information without informing the individual concerned and without judicial oversight, citizens are not provided time to object to the release of their data based on the constitutional rights granted to them.

It is against these constitutional deficiencies that in March 2014 the Parliamentary Legal Committee, whose mandate is to assess the constitutionality or legality of laws made by parliament, found the regulations to be unconstitutional. This was due to their potential infringement of Article 57 providing for the right to privacy and Article 61 guaranteeing freedom of expression.¹¹ The Committee recommended that the regulations should be amended to bring them into line with the constitution and guarantee judicial oversight over access to subscriber databases.

While government subsequently repealed SI 142 in June 2014 and replaced it with Statutory Instrument 95 in response to the Parliamentary Legal Committee’s report, the import of the new regulations largely remain similar to the old instrument.

It is the failure and/or reluctance to amend the law that continue to provide the legal basis to erode citizens’ freedoms in complete disregard for the constitution and international protocols on the right to privacy.

Conclusion

While it is not uncommon for countries to promulgate laws that seek to safeguard their national

security and prevent e-crimes through interception of communications, this should not be to the detriment of citizens’ fundamental freedoms. Aside from threatening the very freedoms guaranteed in the constitution, the interception of communications laws that the state can use to conduct surveillance of its citizens fails the democratic test in a number of ways when juxtaposed against international human rights law and standards on communications surveillance. For instance, there is no transparency in the establishment and operations of the monitoring and interception body, which fosters arbitrary actions that infringe on citizens’ right to privacy. In other jurisdictions such as Australia, New Zealand and the UK, independent commissions that report to parliament conduct interception and undertake public reporting processes. Such a commission is imperative, especially in Zimbabwe, where there is mistrust of those in power.¹² Also, one of the key principles in ensuring democratic legislations on surveillance is judicial oversight in the implementation of the law. This is not the case with the Zimbabwean laws. As a result, the instruments do not contain the requisite checks and balances that will guarantee the balance between the need for interception and protection of citizens’ rights, which is key in preventing the arbitrary abuse of the law. In essence, the interception laws in Zimbabwe do not meet the minimum standards as prescribed in the 13 International Principles on the Application of Human Rights to Communications Surveillance.¹³ The Principles call for:

- Clear laws governing how state authorities may access communications data
- Communications data to be given the same protection as the content of communications
- Access to communications data to be authorised by a competent judicial authority
- Prior or post user notification that a request for communications data has been authorised
- Transparency about the use and scope of communications surveillance powers
- Effective public oversight of the implementation of surveillance laws
- Better protection for the integrity of communications and systems

- Strong privacy safeguards in mutual legal assistance treaties
- The introduction of criminal offences against illegitimate access to communications data
- The protection of whistleblowers.¹⁴

Action steps

While Zimbabwe is still to publicly record incidents where the interception law has been used against citizens, there is general fear that the state is snooping. This fear is grounded on the publication of information and correspondence as well as unflattering details of government opponents and civil society activists. This has resulted in either self-censorship when it comes to electronic correspondence or the exercise of extreme caution in how people express themselves through online platforms. In this regard it is therefore critical that the Zimbabwean government:

- Repeals its interception of communications and surveillance laws in line with the new constitution to protect citizens’ right to privacy and freedom of expression.
- In its review of the laws, the government should ensure that the new acts are in line with regional and international instruments on the right to privacy and expression, as well as in sync with international principles in formulating democratic legislation on surveillance.

Civil society and media freedom groups should:

- Provide policy alternatives that will inform their lobbying of state actors on policy and legislative reforms.
- Build public support for legislative reforms by raising awareness on the right to privacy and its relevance to Zimbabweans’ livelihoods and their democratic well-being.
- Seek judicial intervention through test litigation around provisions of the law so as to create legal precedents that will prompt the review of the law as well as inform its content.
- Forge alliances with like-minded regional organisations to lobby states to comply with their own international agreements.

7 Ibid.

8 Section 17 of the Interception of Communications Act.

9 Gwagwa, A. (2014). State Security and Personal Liberty in the Digital Age. Paper presented at a discussion on surveillance in Harare, 8 May 2014.

10 Ibid.

11 Veritas. (2014) Bill Watch Report 15/2014. Zimbabwe Situation. www.zimbabwesituation.com/news/bill-watch-152014-19th-march

12 MISA-Zimbabwe. (2010). Op. cit.

13 The Principles were developed by a coalition of civil society organisations and have been endorsed by more than 250 organisations across the world. See: en.necessaryandproportionate.org/text

14 Article 19. (2013, September 20). Principles on Surveillance and Human Rights: UNHRC must take action on surveillance. *Article 19*. www.article19.org/resources.php/resource/37251/en/principles-on-surveillance-and-human-rights-unhrc-must-take-action-on-surveillance

