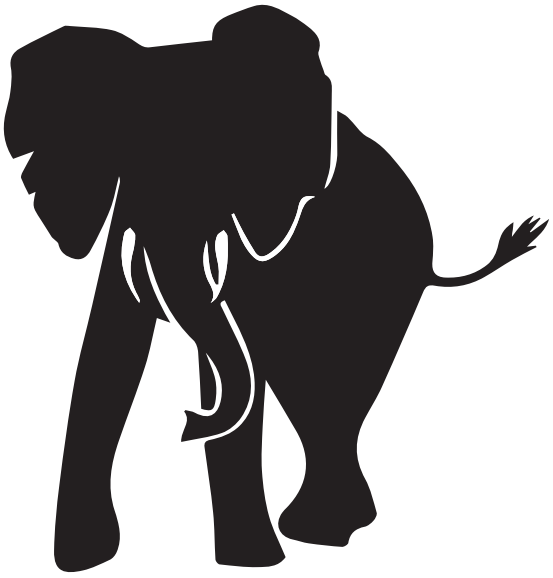
Statement from Free Press Unlimited, Bits of Freedom, Greenhost, Panoptykon Foundation, ARTICLE 19 and La Quadrature du Net

Press Conference April 16th 2015 at 9AM, The Hague

The elephant in the room at GCCS2015

The biggest threat to cybersecurity and the Internet is mass surveillance



ARTICLE 19 · BITS OF FREEDOM VERDEDIGT DIGITALE BURGERRECHTEN · greenhost. sustainable hosting & digital security · FREE PRESS UNLIMITED · PANOPTYKON FOUNDATION · π

The elephant in the room at GCCS2015

The biggest threat to cybersecurity and the Internet is mass surveillance

Today the Global Conference on Cyberspace opens. Representatives of governments, law enforcement, corporations and civil society will discuss how the Internet can be policed and secured. Free Press Unlimited, ARTICLE 19, Bits of Freedom, Panoptykon La Quadrature du Net and Greenhost are calling for a spotlight on the real issue of this conference - mass surveillance.

Since the revelations of whistleblower Edward Snowden we know the Internet has been turned into the largest mass surveillance system ever seen. Indeed, many of the countries participating in this conference are endangering both online privacy and security through the deployment of surveillance tools that indiscriminately sweep up the data of innocent citizens.

We know that they are conducting, facilitating or allowing mass-surveillance, using and producing malware, and demanding backdoors in hardware and software. In doing so, they are in violation of international human rights treaties and endanger the very core on which the Internet is built: trust.

The Internet has become indispensable for freedom of expression, access to information and economic development. It is the first medium in the history of the world where everyone that is connected can receive but also send and discuss information and opinions freely. As such, it must be protected.

Citizens are now more concerned about their online privacy than ever before, with more and more people self-censoring their online behaviour by choosing not to visit certain websites.

There can never be a free and secure Internet as long as governments keep violating citizens' rights to privacy and freedom of expression.

We urge the states participating in GCCS2015 to adopt, comply with, and implement the International Principles on the Application of Human Rights to Communications Surveillance.

These principles address the following:

- Legality: Any limitation on the right to privacy must be prescribed by law.

- 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.
- Necessity: Laws permitting communications surveillance by the State must limit surveillance to that which is strictly and demonstrably necessary to achieve a legitimate aim.
- Adequacy: Any instance of communications surveillance authorised by law must be appropriate to fulfill the specific legitimate aim identified.
- Proportionality: Communications 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.
- Competent judicial authority: Communications surveillance must be authorised by a competent judicial authority that is impartial and independent.
- Transparency: States should be transparent about the use and scope of communications surveillance laws, regulations, activities and powers.
- Public oversight: States should establish independent oversight mechanisms to ensure transparency and accountability of communications surveillance.
- Integrity of communications and systems: States should not compel service providers, or hardware or software vendors to build surveillance or monitoring capabilities into their systems, or to collect or retain information purely for State communications surveillance purposes.
- Safeguards for international cooperation: Mutual Legal Assistance Treaties (MLATs) entered into by States should ensure that, where the laws of more than one State could apply to communications surveillance, the available standard with the higher level of protection for users is applied.
- Safeguards against illegitimate access: States should enact legislation criminalising illegal communications surveillance by public and private actors.

Widespread, untargeted surveillence and data collection is not consistent with these principles.

You can find the full text of the Principles here: https://necessaryandproportionate.org/

These principles, the concept of privacy by design, and the international human rights framework should also be applied to the technical architecture of communications and surveillance systems, ensuring that technological and policy protections are developed hand in hand.

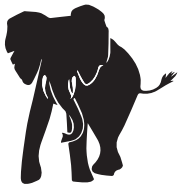
As long as there is

MASS SURVEILLANCE

There can be no

FREE AND SECURE INTERNET

for anyone anywhere



#theElephantInTheRoom

ARTICLE 19 · BITS OF FREEDOM VERDEDIGT DIGITALE BURGERRECHTEN · greenhost. sustainable hosting & digital security · FREEEE PRESS UNLIMITED · PANOPTYKON FOUNDATION