EUROPEAN SOCIAL NETWORKS RESPONSE TO THE COMMISSION´S PUBLIC CONSULTATION ON THE COMPREHENSIVE APPROACH ON PERSONAL DATA PROTECTION IN THE EUROPEAN UNION

Introduction

It becomes increasingly relevant that further Data protection and privacy regulation is necessary, especially when considering emerging technologies that change the nature of data collection and protection. As an interest group comprised of the largest European social networks, we present this response to the European Commission's proposal for a revision of the *Directive 95/46/CE of the European Parliament and the Council dated 24th October 1995, on the protection of individuals regarding the processing of personal data and the free movement of this data*[1] in order to provide Commissioners with an industry perspective when evaluating the future of data protection regulation and enforcement.

As data controllers, we uphold the 1995 Directive in the capacity that it applies to data protection within our industry. However, the Commission rightly points out that this directive is missing key points necessary to ensure that individuals are guaranteed the protection they deserve, regardless of which member state they live in or which online service they choose to use.

In this revision, one major point that needs to be addressed is the need for harmonization within and across member states with regards to the level of implementation and enforcement of the Directive. Harmonization can go a long way in increasing legal certainty amongst stakeholders, and coupled with a explicit clause concerning the applicability of European data protection law to both European and non-European providers who target European customers, will help assure the protection of all European citizens.

In terms of enforcement, we are in favor of working towards a strengthened self-regulatory system, which is an effective mechanism for keeping legislation industry-neutral and allows protection to evolve at the same rate as technology. Notwithstanding, in our comments we elaborate on further measures that can be taken to increase accountability.

[1] Directive 1995/46/EC, dated 24th October, by the Parliament and Council, on the Protection of individuals with regard to the processing of personal data and the free movement of such data.

By considering our points and consolidating them into a document that reflects the realities of the current age, we believe that the Social Networking industry in Europe will be better able to provide cutting edge technologies to European citizens and compete in the international marketplace without compromising an individuals' right to data protection. Our proposal continues with a comments section that acts as a direct response to points raised from the Commission's consultation.

Comments on the Commission´s Communication

1. Strengthening individuals rights

A. Increasing transparency for data subjects

Transparency is an important general principle to incorporate into a revised data protection directive, along with a principle requiring increasingly coherent application of data protection regulation across all industries. In the case that the commission was to adopt a **standard form** as a mechanism to increase transparency and coherence across and between different industries, this could benefit users, if and when such a form remained technologically neutral, unobtrusive, and was easy for users understand.

Users of online services should trust that they remain protected and maintain visibility and access to their personal data. Data controllers should inform users if a **personal data breach** occurs, but we believe it is unnecessary to make this process any more cumbersome for the data controller. If the end user is informed in the case of a breach, users can quickly make the necessary security adjustments regarding their personal data. Moreover, a data breach notification should not lead to an obligation to self-report to the supervising authorities, as this process can be quite cumbersome and does little to ensure the future safety of a data subject's security.

B. Enhancing control over one´s data

Regarding **data minimalisation**, we propose to incorporate the household principle, which establishes a new paradigm that takes into account the way users introduce personal data into online social networks (this is further explained in the "Recitals" section). Users should feel informed about the finality of their data when they enter it into a social network. For this reason, many networks across Europe have already collaborated on **data awareness** campaigns, and will continue to do so. Requiring these types of activities may put a great deal of pressure on smaller enterprises, which is why we are in favor of more widespread campaigns and increased availability of funds for these types of activities. Another instrument to support data

minimalisation is the principle of **privacy by design**, which is and will continue to be the best basis for new product development.

We are in favor of the addition to current legislation of the **right to be forgotten,** in that individuals should maintain the freedom to remove their information from a network once it is deemed unnecessary for the contract to which they have agreed. This requires a clarification in the current legislation, since it could be inferred that an individuals right to access, correction, cancellation and opposition of their data already establishes the instances the proposed introduction intends. We are against imposing a mandatory date of expiration because of the technical of storing and copying data.

D. Data portability

The introduction of a mandatory data portability clause applicable to the social networking industry does not strike us as a necessary measure. The majority of personal data provided by individuals to social networks contains information that is easily transferred to other networks (name, photos uploaded from ones own computer, potentially phone number, or localization information). When a user cares to remove their information from a network, most social platforms generally make it easy for users to remove their information permanently, with shorter ¨holding¨ times than other industries.

Additionally, the implementation of a data portability clause could be problematic, because social networks create shared data networks which fundamentally link one user´s data with the data of other users. Contemplating the possibility of allowing users to port entire networks from one platform to another contemplates the possibility of allowing users to share their friends' data without their consent.

E. Processing Data for a User

Our group believes that imposing a mandatory data portability clause as illustrated above may actually create an unstable standard and potentially leave citizens without adequate protection. However, there are certain situations that require further clarity and perhaps general provisions to accommodate them.

A very common use case for social network providers is the upload of personal data by users. This can be best described by an example:

A user is registered on a social network and is the customer of a provider, who offers an online social phonebook. Using this product the user can transfer friend data to the social phonebook and store them in this phonebook.

The data controller is processing a non-users data, but it is the end user that initiates and benefits from this procession of data. Social Networks need to provide features for users to import/upload their data, in the case that the imported data is not

fundamentally linked to entire data networks and the network does not use this data for their own purposes.

We need legal certainty in this regard and would suggest to clarify that the lawfulness of uploading personal data to a social network is a responsibility of the user.

Naturally, the friend's rights must be respected by the natural person who initiates the data transfer.

F. Consent

We agree that it is necessary to clarify and strengthen the conditions for consent as a key concept for self-determination. This clarification could be achieved by providing a unified definition to be adopted by all member states. Currently, different definitions increase uncertainty throughout member states when consent is in question.

G. Clarification for processing of user data for ad-targeting and other services

Many Internet services are characterized by the fact that they are free of charge to users or charge just for specific services. Most services rely – at least partially - on revenue generated by integrating advertising, analyzing user behavior for advertisers, and/or using demographic analysis for more meaningful advertising (so called `targeting´). This "targeting" is NOT a ceding of the users data but rather a treatment done on the data controller's side that integrates advertisement to a specific slice of the user base and reports statistics back to the advertiser.

Whether analyzing user data for ad targeting or suggesting individual services is lawful is a controversial topic. *We would highly appreciate if the future legal framework for processing of user data would clarify that these ways of analyzing and using user data do not necessarily require consent but rather are part of the processing that is necessary for the performance of a contract to which the data subject is party.*

Expenses for providing free or partially free services to users have to be covered. The most common way to generate revenue on a website is with advertising, and more relevant advertizing makes for a more positive experience for both the user and the advertiser. Users of free services are accustomed to the fact that these services rely heavily on advertisement revenues. A requirement to obtain explicit consent to display ads would be inappropriate.

We don't consider it necessary to amend the Directive, although at least a clarification could be helpful. Nevertheless, it must be possible to provide an advertisement based Internet service without asking for the users consent to process his data for advertisement purposes as long as the data subject is properly informed in his acceptance of the initial contract and the data are not transferred to a third party.

Furthermore, it is absolutely necessary to provide a legal basis for denying services to users that refuse to be the subjects of targeted advertising. Allowing the inclusion of this in the contract the user accepts at the initiation of the service creates a legal certainty for both the provider and for the data subject (as the finality of their data should be explicitly explained within that contract).

G. Enforcement

In terms of enforcement, we are in favor of working towards a strengthened self-regulatory system, which is an effective mechanism for keeping legislation industry-neutral and allows protection to evolve at the same rate as technology.

Notwithstanding, we agree with the Commission that appropriate responses need to be put in place in order to increase accountability among data controllers.

2. Enhancing the Internal market Dimension

A. Increase legal certainty

Harmonisation within and between member states is extremely important to protecting individuals' rights and those of companies operating within and between different countries. The need for this harmonization influences almost every aspect of this response, because no new measure will have the effect it should if only certain member states are required to comply, or certain companies are held accountable.

The introduction of an overarching Harmonization principle, along with a much needed **rules clarification** would be one of the most impactful changes new legislation could introduce. It is evident when observing the differing implementations of social networks that not all are required to follow the same rules regarding protection of user data. If a web application is collecting European data and operating in Europe, that company should comply with European law. To make this feasible, law needs to be harmonized across Europe and accountability principles need to be enforced either in a consistent way throughout member states or at the EU level.

B. Clarification of legal directives

To allow for the broad adoption of the revised directive, we would like to encourage the consolidation of data protection law into one piece of legislation instead of maintaining conflicting standards set by different legal norms. There is legal uncertainty surrounding applicable legislation and the jurisdiction of different governing legislations, especially when applied to companies operating across international borders. As a group, we seek clarification between discrepancies and varying levels of implementation between member states and internationally.

C. Self-regulation and Accountability

Instead of extending the powers of data protection authorities to bring actions against European data controllers, we favor the following principles:

- Endowing the data protection authorities with the powers to investigate and engage in legal proceedings against both European and non-European data controllers whose services are targeted to European consumers. Legal proceedings should be possible at an EU-wide level.
- Strengthening the principle of self-regulation by providing companies with mechanisms to demonstrate their compliance: Privacy seals, Data Protection Compliant certifications, and access to guidelines to perform internal data protection audits are potential examples that could be investigated by companies responsible for data protection accountability. The implementation of these ideas, coupled with increased awareness amongst consumers could further empower users to make their online decisions based on the security of their data.

The strengthening of the above principles does not take away from the necessity of enforcement if an entity is found out of compliance with data protection law.

D. Stronger institutional arrangement for better enforcement of data protection rules

Instead of imposing greater regulations on all member states, harmonisation should be reached so that across all member states companies can expect the same treatment from national data protection agencies. This is important for fairness between states, and also provides a stronger platform for defending European data protection law in the face of globalisation.

Furthermore, in order to strengthen the sustainability of the Directive, we believe it is necessary to ensure that it applies to both European and non-European providers who's online services explicitly target European consumers.

Additionally, it would greatly benefit the industry if universal principles were reached that extended beyond Europe. The online world is knows no borders, and

the ideal legislation to adapt to this changing ecosystem is legislation and best practices that can be adopted for businesses operating at an international level.

E. Commonly Accepted Practices

The term "Commonly Accepted Practices" has recently been mentioned by the Federal trade Commission, which has proposed a framework for business and policymakers called "Protecting Consumer Privacy in an Era of Rapid Change"[2]. In some cases (i.e. Fraud detection) it is necessary to process users data without obtaining their specific consent. We believe industry-specific "commonly accepted practices" need to be defined in order to provide a legal basis to carry out this type of data processing.

To define these practices, we suggest that a European institution define these practices for all member states. This would perhaps be a perfect task for the Article 29 Working Party, the Working Group has a great deal of knowledge surrounding these issues and we are confident that they would be able to identify practical solutions that respect the rights of data subjects, help to sustain the level of data protection in Europe and provide a foundation for the competitiveness of the European online market.

[2] Federal trade Commission, protecting Consumer Privacy in an Era of rapid Change, A Proposed Framework for business and Policymakers, December 2010