Preliminary Views on the Proposed Data Protection and Privacy Regulation in the European Union

February 2012

We welcome the review of the Data Protection Directive. Its fundamental aims remain as important as they were in 1995, but it should come as no surprise that the law, adopted before widespread public access to the internet, requires careful updating.

The importance of the Internet to European society is large and growing. For citizens, it has democratized access to information, fostered new avenues for free expression, and contributed to the preservation and promotion of cultural diversity. At the societal level, the Internet makes a large and growing contribution to the economy. While the size of that contribution varies from country to country, the general trend is clear: a 2011 survey of 13 national economies by McKinsey & Co. found that the internet accounted for 3.4% of GDP and 21% of GDP growth in the previous five years, while creating 2.6 new jobs for every job lost in traditional media industries. And the Internet isn't simply driving growth in the technology sector: 75% of the Internet's impact arises from traditional industries.

The task facing the Council and the European Parliament is to update this important law in a way that both protects the fundamental rights of Europeans and enables the Internet to continue driving economic growth in Europe. We believe those two important goals are compatible with one another, and we look forward to working with European policymakers and industry towards that goal.

What the proposed Regulation gets right

Among other things, the Regulation makes significant improvements to harmonization and decreasing bureaucratic barriers to international data transfers:

- Right to Data Portability (Article 18). We believe this will empower citizens and increase competition among firms, including competition to protect privacy.
- Harmonization, applicable law and lead regulator concept (Articles 3.1, 51) and simplified rules for international transfers that are based on accountability, substantive criteria and forego additional national requirements (Articles 41,1, 42, and 44: 1.h, 3, 6). The reduction of bureaucratic burdens will be good for business while maintaining strong protection of personal data.
- Recognition of interplay between the Regulation and the eCommerce Directive (Article 2.3). The eCommerce directive's recognition of the important role played by intermediaries online--and the importance of protecting intermediary services from burdensome forms of liability--is and should be maintained.
- The rules concerning transparent communication of data practices (Article 11). We're working hard to make sure that our privacy policies are easy for our users to read and understand, and we welcome the principled approach taken in the draft Regulation.
- The fundamental concept of the Right to Be Forgotten, though its particulars require work (Articles 3, 4, and 17.1).

What the proposed Regulation gets wrong

There are areas of the proposed Regulation that require significant modification to avoid adverse impact on both citizens and organizations. The challenges, in general, flow from the Regulation's failure to update the definitions to reflect the role of different actors online (e.g. hosting platforms and other intermediaries). The definitions of personal data and the relationship between controllers and processors raise particular challenges. The 139 recitals appended to the Regulation go some way to addressing the ambiguities and logical inconsistencies in the draft, but these failings would be better addressed in the text of the Regulation itself, and especially by addressing the definitions, which do little to improve the current situation under the 1995 directive.

A. The Definition of Personal Data, Rules on Consent and Profiling

Personal data: (Article 4: (1) and (2), 10, recitals 23, 24, 45)
Consent (Articles 6, 7, 10, recitals 25, 45)
Legitimate Interest (Article 6(1)(f), recitals 38, 39)
Profiling (Article 20, recitals 21, 58)

Summary

The proposed Regulation follows the 1995 directive in attempting to force every piece of information into one of two buckets ('personally identifiable' or 'non-personally identifiable'). This binary distinction fails to match the nature and use of data in the real world. This weakness is acknowledged implicitly by the tempering of the definition found in the text of the Regulation by the language of recitals 23 and 24.

IP addresses are a good example of the weakness of the binary approach to defining personal data: a website operator generally can't use an IP address to identify a visitor, but an ISP generally can. Should a user be able to go to a website operator to exercise his rights of access and rectification? If the website operator were to comply with such a request, it would likely share page view information related to other people, since IP addresses do not map well to individuals--or even to individual devices. On the other hand the website operator shouldn't treat IP addresses as if they were anonymous; it should not, for example, publish a list of IP addresses that have visited its page. In many uses, IP addresses are indirectly identifiable: they deserve to be protected, but a data controller may not be able to allow full exercise the data subject rights outlined in the Regulation.

The binary definition of personal data has perverse consequences in several other areas of the draft Regulation, which could be remedied more simply by defining a category of 'indirectly identifiable' data, giving both data subjects and organizations that process data more certainty about their rights and obligations. This shortcoming is recognized by the language in Article 10 & recital 45 ("If the data processed by a controller do not permit the controller to identify a natural person, the controller shall not be obliged to acquire additional information in order to identify the data subject for the sole purpose of complying with any provision of this Regulation."), but addressing the shortcomings of the definition itself would provide a clearer framework of trust for companies and users.

Consent

The ill-defined concept personal data makes the Regulation's rules on consent and profiling more complicated than they need to be. Creating a default expectation of explicit consent--including for use of data that do not directly identify an individual--creates uncertainty and significant burdens for organizations.

The draft proposal specifies the conditions to assure valid consent for the purposes of data protection and privacy. It also lacks proportionality, equating more sensitive uses of personal data with other uses of data, whether the data in question identify an individual or not. It treats different sensitivities in the same way, even when the impact on the individual is very different.

As drafted, the Regulation bars any form of consent that does not consist of an action or a statement by the user. This myopic approach ignores the importance of user expectations and therefore creates a very real risk that by complying with the new Regulations data controllers will undermine consumer confidence and disempower the citizens that the Regulation seeks to protect.

The current struggles faced by companies trying in good faith to comply with the ePrivacy rules on cookies points to the dangers inherent to legislating methods of establishing consent that are highly prescriptive, ambiguous in practical application, and divorced from they ways in which consumers experience such interactions. Obvious questions raised by the current draft include:

- What would it mean to ask for specific consent that is also explicit?
- How many times would a user be prompted with questions and requests for actions?
- At what threshold of consent requests do consumers cease? (Research from the Microsoft security team suggests that consumer attention drops steeply if they receive more than 2 requests per day)

We think that consent understood as a form of user control can be valid in different ways, but addressing the exact ways in which a controller should seek consent is neither justified, nor future proof. We believe that the legislation should be flexible enough to allow for the creation of innovative ways in which users can maintain control about the data related to them. In particular, we think that when the use of data is in accordance with both industry standards and the expectations of the average consumer, the bar for gaining consent should be less onerous for both industry and the citizen.

We do note that consent is only one of several ways that the Regulation allows for the legitimate processing of personal data. Compared with the current legislative framework, however, consent has been prioritized against the 'legitimate interests' rule, which has heretofore controllers to process information if it does so for legitimate business interests and insofar as the processing does not affect the data subjects' fundamental rights to privacy. Maintaining the viability of the 'legitimate interests' rule is important because it leaves room for organizations to process information outside explicit consent through enhanced transparency and user control.

Profiling

The proposed rules on profiling go well beyond the limitations imposed in 1995 and, as drafted, risk degrading the quality of services available to European citizens. Previously, the rules on profiling applied specifically to processing by automated means that causes adverse effects on

individuals. These rules have now been extended to cover all forms of personalization, penalizing service customization, regardless of its potential impact on users.

The intention of the original rules was to restrict discrimination between individuals with a negative effect (e.g. using profiling through automated means to deny a service such as a mortgage or insurance). There is no justification for extending those restrictions to practices that pursue the opposite objective--making information more relevant and useful for the individual--in a way that has no adverse effects, especially if individuals are given the ability to control the way in which their preferences are considered.

B. The Right to be Forgotten

Article 17
Recitals 53, 54, 121.

Summary

In general, we support the Right to be Forgotten as envisioned by the Commission. At the core of the right to be forgotten is the idea that a consumer using a hosting platform should have full control over, including the ability to delete, data he or she published intentionally. That means a consumer should be able to delete an individual post, photo or video that they stored with the hosting platform. The consumer should also be able to delete their entire account with a given hosting platform, thereby deleting all the materials they had published and which was stored in that account.

As drafted, though, the Regulation's approach to the Right to be Forgotten has two main weaknesses:

1. It confuses the role of the user and that of a hosting platform in assigning responsibility in cases where personal data has been made public (Article 17.2).
2. It lacks internal consistency, confusing what is possible when information is made public to an unspecified number of people (for example open access on the Internet) and what is possible when a data controller chooses to make information available to specific third parties.

These rules would require individuals or organizations covered by the Regulation to use technical means to inform any third party that might have had access to the information, even if that information had been consciously made public by the individual user to whom the information pertains. While the obligation is an information requirement, as drafted it would prove extremely difficult (if not impossible) to achieve, as platforms that allow users to publish information online typically do not and should not keep track of who has retrieved the information or where it might be used subsequently. Where clear information and control mechanisms are offered to the user of a platform, these responsibilities appropriately lay with the user him or herself.

Matters are further complicated when the information posted does not pertain to the user who chooses to publish it. In these cases, the draft regulation seems squarely focused on users of online social networks, but it ignores the fact that many (if not most) online platforms have no way to understand who the information published by one of its users concerns, let alone whether it breaches another individual's privacy? The text of the Regulation does not make clear how the definitions of data controller, data processor, data subject, and third party would

apply to the actors in such a situation, making it very difficult to envision how a hosting platform could comply with this provision.

We do welcome the clarifications in Recital 121 that establishes that freedom of expression exceptions should be interpreted broadly, instructing Member states to recognize the expression of opinions of ideas under the scope of this fundamental right irrespective of the medium used. However, it would have been more advisable to include these thoughts and the reference to jurisprudence in the text of the Regulation itself.

C. Responsibilities and Liabilities of Controllers and Processors

Articles 22, 24, 26, 27, 28, 30, 33, 34, 75, 77.
Recitals 65, 70, 116.

Summary

Controller and processors have different roles and responsibilities. Blurring these will only bring more uncertainty, and is not the way to deal with the complexities of Cloud.

Processors by their very nature act on behalf of a Controller, who is the one determining the purposes and means of the processing. Processors do not have access to data or other processing strategies, which remain the remit of the controller. Therefore, processors are not in a position to assist the controller in complying with information requirements, nor will they be able to conduct an impact assessment or make any determination as to the handling of the personal data. Any obligation on the processor should be clearly linked to activities inherent to the processor, not activities taking place under the instruction of a controller.

Where processors are not involved in the business decisions taken by the controller to process a given set of data they will not be in a position to provide the required documentation. Only controllers are in a position to decide what type of information is to be processed, for what purposes, and how it needs to be protected, taking into account their obligations, individual expectations and using their own read of the risks involved.

The processor is responsible to the controller if it fails to execute its processing in accordance with the instructions given. It will therefore be subject to redress based on prior negotiated contractual obligations. Hence there is no justification for joint liability of processors and controllers.

Likewise, obliging the processor to get an agreement by the controller on every single processor/subprocessor that in any shape or form deal with data, considering the broad definition of processing, is a burdensome and very impractical obligation for the processor, with no benefit for data protection in itself.

Based on the above, we suggest the deletion of the word "processor" on articles 28.1, 33.1, 34, 75 and 77 and the word ‘’controller’’ in article 30.1. Alternatively, we request a derogation of these provisions for B2B relationships, on the bases of the contractual arrangements that govern these relationships.

***