Available online at www.sciencedirect.com

SciVerse ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

Comment

Data protection in Europe – Academics are taking a position

Keywords:
European Data Protection
Regulation
Digital identity
Informed consent
World Wide Web Consortium 'W3C'

ABSTRACT

CLSR welcomes occasional comment pieces on issues of current importance in the law and technology field. The current debate on the Commission's proposal for a new data protection framework includes a plethora of very specific issues. As important as these may be, it should not be overlooked that the very principles of data protection are at stake at the moment. Given the lobby efforts to exclude large parts of today's data processing from the ambit of the proposed Regulation, to weaken the principle of informed consent, and to broaden the exceptions for "legitimate interests", we want to stress that data protection in Europe needs to be strengthened, and that this can be achieved without threatening innovation and legitimate business models.

1. Background

The automatic processing of personal data is growing at an incredible pace and is starting to become an integral part of economic, administrative and social processes in Europe and throughout the world. On the Web in particular, users have learned to pay for a nominally free service by providing personal data for marketing purposes. Against this background, the overhaul of data protection regulation is now being discussed across Europe. A year ago, the European Commission presented a new draft of a European Data Protection Regulation. The European Parliament and the European Council are now preparing their views on this new regulation. At the same time, huge lobby groups are trying to massively influence the regulatory bodies.

To contribute a more objective perspective to this heated debate, we – as scientists and academics – would like to bring forward some professional arguments. We want to reply to some arguments that aim to weaken data protection in Europe.

2. Innovation and competition are not threatened

The core argument against the proposed data protection regulation is that the regulation will negatively impact innovation and competition. Critics argue that the suggested data protection rules are too strong and that they curb innovation to a degree that disadvantages European players in today's global marketplace. We do not agree with this opinion. On the contrary, we have seen that a regulatory context can promote innovation. For example, regulation has promoted innovation in the areas of road safety, environmental protection, and energy. For data protection, we already see start-ups throughout Europe that offer European citizens solutions to protect their personal data "out-of-the-box". Security and privacy experts are selling consulting services to companies to help them manage their IT infrastructures more securely. For many important business processes, it is not data protection regulation that prevents companies from adopting cloud computing services; rather it is uncertainty over data protection itself.

The Boston Consulting Group's recent report on "The Value of Digital Identity" provides further support for the notion that new data protection regulation from the European Commission will not impede the personal data economy. Five of the six usage areas BCG outlines for personal data are compatible with the proposed regulation. The consulting firm sees personal data, for example, as a lever for process automation, personalization, and the improvement of products and services. From our perspective, companies can use personal data for such purposes if they maintain personal relationships with their customers. For a long time, it has been shown that people are happy to exchange their personal data in return for valued services. Personalized offerings and continuous

0267-3649/$ – see front matter
http://dx.doi.org/10.1016/j.clsr.2013.03.002

service improvement are feasible in the context of fair exchange relationships between companies and customers. Moreover, more trust in data handling practices will strengthen such relationships.

Current business practices will only be constrained if companies create value based solely on the aggregation and trade of personal data and do not invest in direct relationships with end customers. For example, large ad-targeting networks or data brokers will be restricted in their use of personal data if the regulation is passed in its current form. In these areas, however, we indeed see a need to adjust regulation and introduce sanctions.

Also, innovation is not threatened by the new data protection regulation because many services do not need data that relates directly to individuals. In many cases, the use of personal data can be avoided by using anonymization technologies. Where a service really requires personal data, this data can be collected on a contractual basis. Services can also gain access to data by asking citizens – in a fair way – for their informed consent.

3. On informed consent

Since 1995, usage of personal data in the European Union has relied on the principle of informed consent. This principle is the lynchpin of informational self-determination. However, few would dispute that it has not been put into practice well enough so far. On one side, users criticize that privacy statements and general terms and conditions are difficult to read and leave users without choices: If one wants to use a service, one must more or less blindly confirm. On the other side, companies see the legal design of their data protection terms as a tightrope walk. Formulating data protection terms is viewed as a costly exercise. At the same time, customers are overstrained or put off by the small print.

As a result, many industry representatives suggest an inversion of the informed consent principle and an embrace of an opt-out principle, as is experienced today in the USA. In the USA, most personal data handling practices are initially allowed to take place as long as the user does not opt out.

The draft regulation, in contrast, strengthens informational self-determination. Explicit informed consent is preserved. Moreover, where there is a significant imbalance between the position of the data subject and the controller, consent shall not provide a legal basis for the processing. The coupling of service usage with personal data usage is even prohibited if that usage extends beyond the immediate context of customer service interaction.

We support the draft of the data protection regulation because we believe that explicit informed consent is indispensable. First, an inversion of the informed consent principle into an opt-out principle considerably weakens the position of citizens. Such an inversion gives less control to individuals and therefore reduces their trust in the Internet. Second, we see several solutions that can solve today's user problems. European companies are producing technical tools that will help users manage their privacy decisions automatically or with very little effort. In the USA, we see the W3C's "do-not-track" initiative, which foresees the implementation of user preferences in browsers. Furthermore, technologies are being developed that interpret privacy terms for users and summarize the terms to facilitate decision-making.

As soon as the coupling of personal data use to unrelated service use is outlawed, users can make real choices.

4. On 'legitimate interest'

Currently, companies can process personal data without client consent if they can argue that they have a legitimate interest in the use of that data. So far, unfortunately, the term "legitimate interest" leaves plenty of room for interpretation: When is an interest legitimate and when is it not?

To prevent abuse of this rule, which is reasonable in principle, the new data protection regulation defines and balances the legitimate interests of companies and customers. The regulation requires that companies not only claim a legitimate interest, but also justify it. Moreover, the draft report of the European Parliament's rapporteur now outlines legitimate interests of citizens. It determines where the interests of citizens outweigh company interests and vice-versa. In the proposed regulatory amendments provided by the rapporteur, citizens have a legitimate interest that profiles are not created about them without their knowledge and that their data is not shared with a myriad of third parties that they do not know about. We find this balancing of interests a very fair offer that aligns current industry practices with the interests of citizens.

5. When to apply the regulation? When is data "personal"?

An important point of contention is what data processing activities should actually be covered by the regulation. Online users are often identified implicitly; that is, users are identified by the network addresses of their devices (IP addresses) or by cookies that are set in web browsers. Implicit identifiers can be used to create profiles. Some of these implicit identifiers change constantly, which is why at first sight they seem unproblematic from a data protection perspective. To some, it may appear as if individuals could not be re-identified on the basis of such dynamic identifiers. However, many experiments have shown that such re-identification can be done.

Despite the undisputable ability to build profiles and re-identify data, some industry representatives maintain that data linked to implicit identifiers should not be covered by the regulation. They argue that Internet companies that collect a lot of user data are only interested in aggregated and statistical data and would therefore not engage in any re-identification practices.

For technical, economical and legal reasons we cannot follow this opinion. Technically, it is easy to relate data collected over a long period of time to a unique individual. Economically, it may be true that the identification of individuals is not currently an industry priority. However, the potential for this re-identification is appealing and can therefore not be excluded from happening. Legally, we must protect data that may be re-identifiable at some point, as such precautionary measures could prove to be the only effective remedy.

Some EU parliamentarians suggest that anonymized, pseudonomized and encrypted data should generally not be covered by the data protection regulation. They argue that such data is not "personal" any more. This misconception is dangerous. Indisputably, anonymization, pseudonomization, and encryption are useful instruments for technical data protection: Encryption helps to keep data confidential. Pseudonyms restrict knowledge about individuals and their sensitive data (e.g., the relation between the medical data of a patient) to those that really need to know it. However, in many cases even this kind of protected data can be used to re-identify individuals. We therefore believe that this type of data also needs to be covered by the data protection regulation, even if it may be treated in a different manner than personal data that is directly identified. Moreover, coverage of this kind of data is also necessary to ensure that protection is properly and professionally applied. We need binding rules that are regularly adjusted to technical standards (i.e. best available techniques) and that define when data is sufficiently pseudonymized and when it can be considered anonymous.

6. Who should determine data protection requirements?

Besides the many positive aspects of the draft regulation, we see one structural weakness, albeit one that can be easily rectified: In many articles, the current draft from the European Commission sets only vague goals. For further details, it establishes the European Commission itself as the institution that would later define details through 'delegated' and 'implementing' acts. This plan would put the European Commission into a position of power that does not correspond to the European constitutional requirements. Data protection rules can have major impacts on economic, administrative and social activities. It is therefore the duty of the European legislative bodies to make such decisions by themselves. All relevant rules therefore need to be embedded within the regulation itself. Only details that are less critical from the perspective of politics and fundamental rights may be left to the Commission's discretion.

Signatories

Austria
- Sarah Spiekermann, Vienna University of Economics and Business, Institute for Management Information Systems, Vienna

Belgium
- Jacques Berleur, University of Namur, Computer Science Faculty, Namur
- Paul de Hert, Vrije Universiteit Brussel, Brussels, Law Science Technology & Society (LSTS)
- Cécile de Terwangne, University of Namur, Faculty of Law, Namur
- Séverine Dusollier, University of Namur, Faculty of Law, Namur
- Yves Poullet, University of Namur, Rector and Faculty of Law, Namur
- Jean-Marc Van Gyseghem, University of Namur, Faculty of Law, Namur

Cyprus
- Marios D. Dikaiakos, University of Cyprus, Department of Computer Science, Nicosia
- Tatiana Synodinou, University of Cyprus, Department of Law, Nicosia

Czech Republic
- Vaclav Matyas, Masaryk University, Faculty of Informatics, Brno

Denmark
- Ivan Damgård, Aarhus University, Department of Computer Science, Aarhus
- Niels Christian Juul, Roskilde University, Department of Communication, Business and Information Technologies, Roskilde
- Jakob I. Pagter, Head of Research and Innovation, Security Lab, The Alexandra Institute
- Jan Pries-Heje, Roskilde University, Department of Communication, Business and Information Technologies, Roskilde
- Christian W. Probst, Technical University of Denmark, Department of Applied Mathematics and Computer Science, Kongens Lyngby

Finland
- Jukka Heikkilä, University of Turku, Department of Management, Turku

France
- Catherine Barreau-Saliou, Institut de l'Ouest - Droit et Europe, Faculté de Droit et de Science Politique, Rennes
- Claude Casteluccia, Institut National de Recherche en Informatique et Automatique, Grenoble
- Yves Deswarte, Centre National de la Recherche Scientifique, Laboratoire d'Analyse et d'Architecture des Systèmes, Toulouse
- Marc-Olivier Killijian, Centre National de la Recherche Scientifique, Laboratoire d'Analyse et d'Architecture des Systèmes, Toulouse
- Daniel Le Métayer, Institut National de Recherche en Informatique et Automatique, Lyon
- Refik Molva, Eurecom Graduate School and Research Center In Communication Systems, Sophia Antipolis
- Philippe Pucheral, University of Versailles Saint-Quentin en Yvelines

Germany
- Andreas Albers, Goethe-Universität Frankfurt am Main, Faculty of Economics and Business Administration, Frankfurt am Main
- Michael Backes, Saarland University, Center for IT-Security, Privacy and Accountability (CISPA) and Max Planck Institute for Software Systems, Saarbruecken
- Harald Baier, Hochschule Darmstadt, Department of Computer Science, Darmstadt
- Eric Bodden, Technische Universität Darmstadt, Department of Computer Science and Fraunhofer Institute for Secure Information Technology, Darmstadt
- Tim Güneysu, Ruhr-Universität Bochum, Horst Görtz Institute for IT-Security, Bochum
- Oliver Günther, Universität Potsdam, Präsident, Potsdam
- Markus Hennies, Hochschule der Medien Stuttgart, Faculty Information and Communication, Stuttgart