Available online at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

The digital future – A challenge for privacy?

Rolf H. Weber *

University of Zurich, Switzerland

Keywords:
Privacy concepts
Privacy issues
Regulatory measures
Technological solutions

ABSTRACT

Increasingly, data protection laws and the concept of privacy are subjected to manifold challenges created through advancing new technologies such as Big Data, digital identity, biometrics and social media sites. Such technological shifts, although being immensely beneficial to society at large, create problems for the protection of an individual's privacy. This article addresses the arising issues and suggests innovative technological solutions for minimizing privacy infringements and negative impacts on the private sphere of individuals.

1. Introduction to privacy concepts

Privacy protection in Europe follows a long tradition. As part of the European Convention on Human Rights,[1] national constitutions of EU Member States[2] and the Charter of Fundamental Rights of the European Union[3] (CFREU) the right to privacy forms a foundation for the European Member States' data protection legislations. Increasingly, however, these laws and the concept of privacy are subjected to manifold challenges created through advancing new technologies such as Big Data,[4] digital identity, biometrics and social media. These technological shifts, although being immensely beneficial to society at large, create problems for the protection of individual privacy. This article addresses the present issues and suggests innovative technological solutions for minimizing privacy infringements and negative impacts on the private sphere of individuals.

The first part of this paper highlights the current privacy issues created by various forms of new technologies. In the second part technological solutions are proposed to counteract the identified privacy risks and the boundaries of such measures are analyzed. In particular the ability of an individual to consent to privacy infringements as a way of allowing the service provisioning poses a question of accountability and power abuse. Currently, users are "paying" for services by making available their personal data. Therefore, as a potential solution clear rules must be established on the steps required to inform a user of the data's utilization by the provider as well as third parties.

* Chair Professor for International Business Law at the University of Zurich, Visiting Professor at Hong Kong University, Attorney-at-Law in Zurich, Switzerland.
E-mail address: rolf.weber@rwi.uzh.ch.

[1] European Convention on Human Rights and Fundamental Freedoms, 01.06.2010, <http://www.echr.coe.int/Documents/Convention_ENG.pdf>.

[2] Charter of the Fundamental Rights of the European Union, (2000/C 364/01), 18.12.2000, <http://www.europarl.europa.eu/charter/pdf/text_en.pdf>.

[3] Charter of Fundamental Rights of the European Union (2000/C 364/01), 18.12.2000, <http://www.europarl.europa.eu/charter/pdf/text_en.pdf>.

[4] Big Data usually includes data sets with sizes beyond the ability of commonly used software tools to capture, curate, manage, and process the data within a tolerable elapsed time. See Chris Snijders/Uwe Matzat/Ulf-Dietrich Reips, (2012) 'Big Data': Big gaps of knowledge in the field of Internet. International Journal of Internet Science, 7, 1–5. <http://www.ijis.net/ijis7_1/ijis7_1_editorial.html>.

http://dx.doi.org/10.1016/j.clsr.2015.01.003

2. Current privacy protection frameworks

2.1. *Fundamental rights*

Fundamental rights are key to the international legal framework and touch upon an individual's right to privacy. However, in practice these rights are not yet sufficient to cater for the privacy challenges faced in today's online world. Additional national laws are necessary to extend the essential privacy protection to new technologies and scenarios currently emerging.

In Article 1 of the UN Universal Declaration of Human Rights[5] (UDHR) as well as in the CFREU the protection of human dignity is a central concept. Furthermore the European Convention on Human Rights contains an express protection for privacy of individuals applying not only to government but also to private actors. Thus, appropriate privacy laws must be implemented in all countries to ensure the protection of these fundamental rights.

Privacy infringements can occur in various forms either by an individual directly disclosing information to a third party on a social networking website or by a commercial entity collecting the data for business purposes. This paper is concerned with the second of these scenarios as private disclosure is more likely to be acceptable within certain boundaries.

2.2. *Specific laws*

The US approach to privacy is primarily derived from constitutional protections which have been expanded over the last decades to include certain aspects of private conduct. Furthermore, in addition to state data protection legislation federal laws are in place in certain areas such as for the protection of medical data.[6] Recently the topics of surveillance and privacy have gained traction based on the Snowden revelations.

Already in 2011 a push for better privacy protection had been undertaken by introducing the Do Not Track Me Online Act of 2011[7] which aimed at enhancing customer rights in order to limit the use of their personal information by commercial entities. Due to a lack of a majority in Congress the introduced law has not been passed yet. However, fresh legislation action is being taken by Congresswoman Speier to introduce a new Mobile App Privacy Protection Act[8] which aims at the privacy issues created by the tracking functions in mobile phone applications. The Act would ensure that users of mobile services are made aware of the type and extent of the data being collected from them as well as their options in limiting disclosure by adjusting their mobile phone settings. Importantly the Act would also allow for civil actions and potentially even class actions against the app-providers which do not follow the disclosure provisions.

Currently, there are various class actions before US courts based on the controversial topic of preventing companies from tracking their users.[9] California has passed such a "Do not Track Law" requiring the companies to inform their customers whether they conform to rules supplied by browsers signaling that the user does not want to be tracked or referring the consumer to choice options of the provider. This also includes the requirement to disclose third party tracking on a website.[10] The US Federal Trade Commission (FTC) has issued guidelines on the subject.[11]

The FTC has long realized that most commercial providers of online services, falling outside the scope of specific privacy legislations, such as for the protection of children under the age of 13, do not adequately inform their customers of their collection practices.[12] In its 2012 report the FTC has therefore recommended to Congress "*that* Congress enact legislation to implement a Consumer Privacy Bill of Rights based on the Fair Information Practice Principles[13] ("FIPPs")".[14]

In Europe these issues have not yet been specifically addressed by way of sector-related legislations. However, the Article 29 Working Party (an advisory group to the European legislator) has raised the privacy issues created by apps in a working paper.[15] In particular it highlighted that only 61% of the top 150 apps provide a privacy policy to the customer.[16] Furthermore, no real choice is given to the app-user for raising objections against the terms and conditions once the software is downloaded. In most cases, only a simple box is left for the

[5] UN Universal Declaration of Human Rights <http://www.un.org/en/documents/udhr/>.

[6] U.S. Department of Health & Human Services, Privacy Protection, <http://www.hhs.gov/ocr/privacy/index.html>.

[7] Bill Text 112th Congress (2011–2012) H.R.654.IH <http://thomas.loc.gov/cgi-bin/query/z?c112:H.R.654.IH:>.

[8] Congresswoman Speier commits to introduce such a legislation in the 113th Congress <http://speier.house.gov/index.php?option=com_content&view=article&id=203:protecting-your-consumer-rights&catid=10:issues&Itemid=46>.

[9] For example the $14 million settlement in Harris v. comScore, No. 11 C 5807, <http://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=1338&context=historical>.

[10] Dominique Shelton, Inside Calif.'s Proposed Guidance for Do-Not-Track Law, <http://www.law360.com/articles/496938/inside-calif-s-proposed-guidance-for-do-not-track-law>.

[11] FTC, The Do Not Track Option: Giving Consumers A Choice, <http://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/do-not-track>.

[12] FTC, Privacy Online: Fair Information Practices In The Electronic Marketplace, May 2000, <http://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf>.

[13] White House, Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy (Feb. 2012), <http://www.whitehouse.gov/sites/default/files/privacy-final.pdf>. The FIPPs as articulated in the Administration paper are: Transparency, Individual Control, Respect for Context, Security, Access, Accuracy, Focused Collection, and Accountability.

[14] Protecting Consumer Privacy in an Era of Rapid Change, FTC Report 2012, 3, <http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf>.

[15] Article 29 Working Party, Opinion 02/2013 on apps on smart devices, 6, <http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf>.

[16] FPF Mobile Apps Study, June 2012, <http://www.futureofprivacy.org/wp-content/uploads/Mobile-Apps-Study-June-2012.pdf>.