The Right to Privacy under Pressure

Rikke Frank Jørgensen

Today we are facing something of a paradox with regard to our right to privacy. On the one hand, the international human rights system has never been clearer in its message that the right to privacy applies online as well as offline. This message has been confirmed in UN resolutions, by the UN High Commissioner for Human Rights, the Council of Europe, the European Court of Human Rights, the European Court of Justice etc. On the other hand, however, there are very few possibilities to enforce the right to privacy on the internet. Data is collected from a large number of public and private players across national borders; there is a very limited idea of the scope and little control with regard to this data collection; users routinely give their consent to allow their data to be collected; and privacy policies are hard to access and are only read by a minority of users.

The leak by Edward Snowden of documents from the US intelligence service, which started in the summer of 2013, has illustrated the amount and scope of the personal information that can be tapped from the internet infrastructure and online services. Snowden's revelations led to the adoption of the first UN resolution on the right to privacy in the digital age (UN General Assembly Resolution No. A/RES/68/167) on 18 December 2013. The Snowden case is about the access of intelligence services to personal information, but the current challenges for the right to privacy are much broader. Basically, the challenges relate to the fact that personal information is increasingly being considered as a commercial raw material, and that today there are unprecedented possibilities to harvest and exchange this raw material (Mayer-Schönberger & Cukier 2013; Lane et al. 2014; Matzner 2014). In this context there is a close link between the nature of the media (digital), the use of personal information and the challenges these pose to privacy. The following is a brief account of the current challenges facing the right to privacy, a summary of the regulatory framework and a couple of ideas for possible solutions.

Right to privacy under pressure

Privacy is a human right according to the 1948 UN Universal Declaration of Human Rights. Article 12 of the Declaration stipulates that: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon

Jørgensen, Rikke Frank (2016). The Right to Privacy under Pressure. *Nordicom Review*, 37(special issue): 165-170. doi:10.1515/nor-2016-0030

his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks." A number of international conventions contain similar provisions to protect privacy, including the UN Covenant on Civil and Political Rights and the European Convention on Human Rights. Moreover, the right to privacy is protected under the EU Charter on Fundamental Rights. The right to privacy is not absolute, but interventions must follow human rights standards, including statutory authority, and they must be necessary and proportional. The duty of states to protect privacy applies both offline and online, as stipulated in the first UN resolution on human rights on the internet in 2012 (UNHRC 2012).

The privacy standard has been subject to extensive research and elucidation, since the definitive article by Warren and Brandeis (1890), in which the right to privacy is defined as the right to be let alone. The dominant perspective has focussed on the right to privacy as the possibility of control; control of what others know about us (control of information), control of decisions related to us personally, and control of a physical area. "Something is private when I am in a position to and have a right to control access to it – whether to data, to a home, to decisions or to ways of acting" (Rössler 2007: 27). The principle of control of one's own data permeates EU data protection legislation, which contains specific requirements for consent. The idea of control through consent is based on the assumption of informed citizens who consciously choose to submit, or not to submit, their information to a given authority or private service. In other words, if the user is provided with sufficiently clear and accessible information, then the user will have real options and there is a basis to grant informed consent. However, recent research indicates that this rational approach to data protection fails to capture the special characteristics of online services. "Notice and consent remains a procedural mechanism divorced from the particularities of relevant online activity" (Nissenbaum 2011: 35). This is partly because the internet changes the perceptions of public and private life, and thereby the foundation for protecting privacy.

On the internet, users' activity and the information they disclose is generally recorded, shareable, searchable and commercially very valuable. In contrast, keeping information private is a challenge that demands extra effort and use of technical protection tools. Where it has previously required an effort to step out of the private domain and into the public, today the situation is the reverse. On the internet we are *public by default*, and only to a limited extent, and through individual effort, can we maintain our private space. Even data from types of communication we traditionally consider as private, such as telephone and email, is increasingly being stored and used to combat serious crime. This is due in part to the digital form of the internet (all activity leaves a searchable footprint), but it also reflects that data has become increasingly valuable, both commercially and in terms of national security. One example is the controversial EU Data Retention Directive (2006/24/EC), which in 2006 established the legal foundation to register and store information about all EU citizens' use of telephone and email, even though the information basically belongs to the private domain and the citizens in question are not under suspicion. In 2014, the Data Retention Directive was overruled by the European Court of Justice, as the Court found that general registration of all communication by EU citizens was a violation of the right to privacy, as protected by the EU Charter on Fundamental Rights (Digital Rights Ireland and Seitlinger and others, Joined Cases C-293/12 and C-594/12)

In addition, the internet is characterised by a radical heterogeneity comprising a myriad of social and commercial practices that in many contexts have blurred borders with regard to the public and/or the private. For many, social media represent a social infrastructure, but they are also commercial services which survive by selling advertisements based on users' preferences, identified through their shopping patterns and information which users disclose about themselves. In other words, information which users disclose in one context (social interaction with friends) is used in another context (targeted advertising based on users' behaviour and preferences). The widespread use of social media means that contexts that have traditionally been separate (home/work, school/leisure, private communication/public disclosure, social sphere/commercial sphere) are increasingly melting together (Marwick 2012: 379). These characteristics are challenging protection of privacy on the internet, and the associated legislation on processing personal data, on several fronts.

Since 1995, EU Member States have been bound by the EU Data Protection Directive (95/46/EC), which imposes requirements on both public and private enterprises with regard to the processing of personal data. The Data Protection Directive is based on the premise that specific types of data should be protected, i.e., information that directly or indirectly can be traced to a person. This personal information may only be processed in relation to a predefined target; there must be proportionality between the objective and the data collected; as little data as possible should be collected; the user should generally give his or her consent; and specific security regulations should be observed. However, the reality on the internet is that the complexity and amount of data collected is huge (and often a mixture of several types of data); data is collected across countries and very different contexts; the use of data is far wider than the original purpose; there are very different levels of security; there is poor transparency with regard to the practice of enterprises and authorities; and consent is granted as a requirement for using a given service rather than as a conscious choice. These factors challenge the effectiveness of the existing data protection rules, including the concept of control through consent. In addition, there are no common binding standards for data protection at the international level. The OECD's guidelines for protection of privacy and transnational data flow (OECD, 1980/2013) are often referred to, but they are merely guidelines and not binding. The Council of Europe Convention no. 108 (CoE, 1981) represents one of the first standards for the area, and like the EU regulations, it has undergone extensive revision, among other things to account for online services. Convention no. 108 is, however, only binding for member states of the Council of Europe. At the global level, UN resolutions have confirmed that the right to privacy is under serious pressure in the online domain, and that states have an obligation to ensure that national legislation and practices that intrude on the right to privacy meet the international human rights standards for the area (UN General Assembly Resolutions No. A/RES/68/167, 18 December 2013 and No. A/RES/69/166, 18 December 2014). However, these resolutions are not binding and they focus primarily on government (not commercial) monitoring.

A further challenge is linked to the fact that most of the infrastructure and basic services on the internet (technical infrastructure, information search, social network, etc.) are administrated by private companies, many of which are American. This poses a number of specific challenges with regard to enforcing EU legislation on personal data, as illustrated in the recent Schrems case concerning Facebook´s transfer of personal

data of EU citizens' to the United States. As a result of the case, the European Court of Justice on October 6, 2015, invalidated the Safe Harbor arrangement, which governed data transfers between the EU and the United States (Maximillian Schrems v Data Protection Commissioner, Case C-362/14).

The way forward?

As mentioned in the introduction, there are different ideas as to how the right to privacy can be strengthened in the online domain. One principal player at the European level is the European Commission, which since 2011 has been working on an extensive reform of the Data Protection Directive. In April 2016, the new Data Protection Regulation was finally adopted and will enter into force in all EU member states in 2018 (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016). The Data Protection Regulation aims at a uniform level of data protection across member states, and includes a number of provisions to increase protection for individuals, especially when using online services. For example, the requirements for consent have been strengthened, the possibility for extensive fines has been introduced for companies that violate the rules, and there are requirements that data protection be incorporated both at technical and organisational levels (privacy by design and privacy by default). The new regulation has been described as an extremely ambitious response to the challenges described above, and it has met massive resistance from US industrial lobbyists in Brussels (European Digital Rights 2011). Furthermore, the Data Protection Regulation does not solve the fundamental problem that users' activities and preferences are essential elements in the business model of many internet services, and the cost to the users for not taking part may be that they have no access to the social community represented by the service (Bechmann 2014; Jørgensen 2014). Effectively, user consent to processing of personal data is the price paid for access to the majority of internet services. In reality, this limits users' options; especially in situations where the service is experienced as an important requirement for being part of a community. For example, a 2013 study of Danish high school students on their use of social media such as Facebook highlighted that consent is perceived as a necessary prerequisite for participating in social networks, rather than a real option (Jørgensen 2014). Therefore there is an increasing mismatch between the concept of informed users who, through their consent, choose to disclose information for a very specific purpose, and the practice by which data is disclosed and used on the internet. In response to this challenge, several have argued that, as a supplement to consent, data protection should be context-specific standards that stipulate limits for what information can be collected and shared.

Nissenbaum (2010; 2011) in particular has described a model for data protection based on "contextual integrity". The point here is that the need for protection should be determined by the context rather than by an attribute incorporated in specific data. Data is increasingly exchanged between different contexts, and for many different purposes, in ways that are impossible to understand for the individual user. Therefore, the point of departure is that each context should be linked to standards distinguishing between appropriate and inappropriate information sharing. On the basis of these standards, which will be more or less formalised depending on the specific context, it will be possible to stipulate requirements for how companies and authorities process personal

information such that the primary responsibility for data protection is defined on the basis of the context rather than user consent. One of the arguments is that the dominant metaphor of a market place, based on assumptions of the free market and the free user, is not adequate to define and enforce standards for fundamental societal functions on the internet (Nissenbaum 2011: 42). Instead, we have to specify that functions at the core of the democratic life of society, such as access to the internet, facilitating information searches on the internet and availability of a social infrastructure, are expected to meet independent quality standards in line with professional standards linked to specific professions, irrespective of whether these functions are managed by public or private players (Anderson 1995: 147). In other words, the point is that important societal functions have to be controlled by quality parameters, in addition to an economic premise, which are anchored in normative standards linked to fundamental rights, including transparency and due process. However, the challenge in Nissenbaum's model is that it is difficult to see how it can be implemented in practice. Who is to define which rules should apply in which contexts? What about contexts that are not clearly defined or delimited? Should the respective sets of standards be realised in legislation? And who should monitor whether they are being observed or not? While current data protection is based on a simplified and rational view of control of personal information, the contextual model allows for a complexity which is hard to translate into practice.

Conclusion

We are currently facing huge challenges with regard to online privacy. There are no binding international regulations, and the EU rules, which in global terms are the most well developed, are still based on consent as the central control mechanism. This is despite the increasing scepticism as to the value and effect of consent, especially for online services. There are alternative proposals for regulation of the area, not least Nissenbaum's proposed contextual approach to data protection. The idea of a more differentiated regulation, based on analyses of standards in different situations, in contrast to a one-size-fits-all philosophy for privacy, seems to be a sensible response to the current challenges. However, as outlined above a number of unanswered questions remain, which make it difficult to see the model translated into practice".

References

Anderson, Elizabeth (1995). *Value in Ethics and Economics*. Cambridge, MA: Harvard University Press.

Bechmann, Anja (2014). Non-informed Consent Cultures: Privacy Policies and App Contracts on Facebook. *Journal of Media Business Studies* 11(1): 21-38.

Digital Rights Ireland and Seitlinger and others, April 8, 2014, Joined Cases C-293/12 and C-594/12, http://curia.europa.eu/juris/document/document.jsf?text=&docid=153045&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=430603 [Accessed 10 October 2016].

European Digital Rights (2011). US Lobbying against Draft Data Protection Regulation. 22 December 2011. Retrieved 21 May, 2015, from https://edri.org/us-dpr/.

Jørgensen, Rikke Frank (2014). The Unbearable Lightness of User Consent. *Internet Policy Review* 3(4), http://policyreview.info/articles/analysis/unbearable-lightness-user-consent [Accessed 10 October 2016].

Lane, Julia, Victoria Stodden, Stefan Bender, Helen Nissenbaum eds. (2014). *Privacy, Big Data, and the Public Good :Frameworks for Engagement*. New York: Cambridge University Press.

Marwick, Alice E. (2012). The Public Domain: Social Surveillance in Everyday Life. *Surveillance & Society,* 9(4): 378-393.

Matzner, Tobias (2014). Why Privacy Is Not Enough: Privacy in the Context of "Ubiquitous Computing" and "Big Data". *Journal of Information, Communication and Ethics in Society,* 12(2): 93-106.

Maximillian Schrems v Data Protection Commissioner, 6 October 2015, Case C-362/14, http://curia.europa.eu/juris/document/document.jsf?docid=169195&doclang=en [Accessed 10 October 2016].

Mayer-Schönberger, Viktor & Cukier, Kenneth (2013). *Big Data : A Revolution That Will Transform How We Live, Work, and Think*. Boston, MA: Houghton Mifflin Harcourt.

Nissenbaum, Helen (2011). A Contextual Approach to Privacy Online. *Dædalus, the Journal of the American Academy of Arts & Sciences,* 140(4): 32-48.

OECD (1980/2013). Guidelines for Protection of Privacy and Transnational Data Flow http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm [Accessed 10 October 2016].

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=EN [Accessed 10 October 2016].

Rössler, Beate (2007). The Value of Privacy, pp. 39-44 in Stocker, Gerfried & Schöpf, Christine (eds.) *Goodbye Privacy – Ars Electronica 2007*. Ostfildern-Ruit, Germany: Hatje Cantz Verlag.

UNHRC (2012). United Nations Human Rights Council, The Promotion, Protection and Enjoyment of Human Rights on the Internet. A/HRC/20/8. 16 July 2012. Geneva, United Nations.

Warren, Samuel D. & Brandeis, Louis D (1890). The Right to Privacy. *Harvard Law Review* IV (5), 15 December No. 5, http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html [Accessed 10 October 2016].