Valuing Privacy through Privacy by Design

Amsterdam Privacy Conference 2015

Susan Perry
American University of Paris
International Politics
Paris, France
sperry@aup.edu

Claudia Roda
American University of Paris
Computer Science
Paris, France
croda@aup.edu

Unmitigated enthusiasm for digital technology is the current norm, an orthodoxy shaped in part by the information technology industry through a strategy of sleek, easy-to-use products and robust marketing campaigns, and by a beleaguered public sector eager for quick, cost-saving solutions to pressing social problems. Yet, as French philosopher Edgar Morin reminds us, enthusiasm is not "normal" for any society (CNIL 2012, 47). It is a significant social marker that indicates a strong desire for the illusion of control, demonstrating the public's willingness in this case to view technology as a substitute for other values and concepts that appear out-dated in our world in transition. Such enthusiasm is at best temporary, since the sense of control engendered by digital technology is illusory. Nothing better illustrates the illusory nature of this control than the issue of online privacy, or what Helen Nissenbaum has called "the problem of privacy in public" (Nissenbaum 1998). This paper will argue that legally-mandated protection of online privacy represents a concrete manifestation of control that empowers the user in a public environment of virtual or imagined influence and should be accompanied by user education and appropriate technology design.

Protecting privacy is a complex problem that must be addressed within a framework that joins legal, educational and technical components. Europe has historically focused its privacy-protection framework on a regulatory system, currently based on the 1995 directive (subject to a margin of interpretation within each EU state) that protect citizens by defining how data can be collected, used and distributed. Unfortunately this approach has produced mixed results. On the one hand, laws and regulations have been difficult to enforce and companies have often chosen to operate from countries where privacy regulations are less restrictive; on the other hand, the 1995 directive needs to be updated to address new privacy threats generated by modern methodologies for data collection, processing and distribution. In the last twenty years, for example, it is now possible to identify individual users with far greater accuracy thanks to more sophisticated techniques for analysing metadata, the explosion of information posted by users on social networks, and advanced techniques for image recognition. The problems identified with the 1995 directive are being addressed by the new General Data Protection Regulation[1], which was adopted with a large majority in March 2014 by the European Parliament and will become applicable as soon as approved by the Council of Europe.[2] Although much has been written about the pro and cons of the proposed regulation, it is important to note that protecting privacy through the legal system has been

[1] While a "directive" is a legislative act that sets out a goal that all EU countries must achieve, a "regulation" is a legislative act that is binding on all member states. See http://europa.eu/eu-law/decision-making/legal-acts/index_en.htm

[2] http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//EN

and continues to be recognized as the main component of a privacy-protection infrastructure in Europe. This is not the case in countries with a more liberal tradition where the "market self-regulation" argument is applied to privacy protection. This means that privacy can be used as a marketing tool and users will select the products that respect their desired level of privacy. The obvious weakness of this argument is not only the disproportionately powerful legal and technical means that data controllers have at their disposal when compared to users, but also the unrealistic expectation that users, no matter how technically and legally savvy, will have sufficient cognitive resources available to evaluate the privacy-risks associated to the use of a given technology, in a given context. Even if we disregard the complexity and opacity of Privacy Statements currently available,[3] it is highly unlikely that users will always be able to make effective choices about their own privacy risk and privacy protection. Legal systems will not be able to protect users' privacy in all cases in which users provide information voluntarily and/or give explicit consent to its processing or distribution.

As both systems - those based on legal regulation and those based on "self-regulation" - will fail to protect user privacy under certain circumstances, it is only though a coordinated structure based on legal regulation, user education and appropriate technology design that suitable levels of privacy can be achieved. It becomes essential then that users are educated to understand both the privacy risks associated with the use of certain technologies and the limitations they face in evaluating risk; moreover, systems should be designed to "implement" regulation and facilitate the user's task of assessing risk. This joint edifice of legal, educational and technical components is realized within the privacy-by-design framework. The first part of this paper will examine the legal, educational and technical contours of Privacy by Design, discussing how user control that is embedded within the actual design of digital software and hardware enables users to choose their desired level of privacy while reinforcing the international human rights framework that protects individual rights. The second part of this paper will explore several of the more complex ethical challenges raised by user interaction with digital technology, namely the notion of trust, inequality of digital access, and the seminal question of agency,[4] positing that a privacy-by-design approach allows us to respond to these challenges in such a way as to enhance the value of privacy as a human right and ground our enthusiasm for digital technology within the parameters of user control.

1. Privacy in law and practice

Privacy is a core social value in democratic societies, solidly embedded in the national constitutions and legislation of European Union member states. Digital technology, like any new form of technology, is subject to the law in place, meaning that the information technology sector is not above the law and is consequently obliged to protect user privacy online. In two recent papers, we have explored the ways in which human rights law may be extended to the architecture and use of digital hardware and software,[5] and we present a summary of these arguments below. Several new legal opinions shed additional light on the

[3] If we select the case of social media, for example, we must recognize at least a model of bounded rationality (Simon 1957) when discussing the many ways in which affect may influence decision-making.

[4] These issues were among a series of challenges analysed in 2012 by Jeroen van den Hoven *et al.* in their work for the Ethics Subgroup on the Internet of Things under the auspices of the European Union's DG Connect initiative. This paper extends their research within a privacy-by-design framework.

[5] See Roda, C., Perry, S. (2014). Mobile Phone Infrastructure Regulation in Europe: Scientific Challenges and Human Rights Protection. *Environmental Science and Policy* 37(2014) 204-214, and Perry, S., Roda, C. (2014). Teaching Privacy by Design to Non-Technical Audiences. Cyber Security and Privacy (CSP) Forum 2014. *Springer CCIS Series*, Vol. 470.

subordinate place of digital technology within a rights-based system, a location that encourages the use of technology to empower individuals, rather than subject these same individuals to surveillance, manipulation or commercialization of their personal data. We will use these cases to demonstrate the trend towards legal recognition of the value of digital privacy as a human right.

1.1 The legal framework for privacy

Privacy is a relative late-comer to the pantheon of civil and political rights enshrined in the International Covenant on Civil and Political Rights (ICCPR). Warren and Brandeis' seminal article of 1890 treated privacy as a critical right, related to the full protection of person and property. (Warren & Brandeis 1890, 1) As the age of photography weakened control over one's personal image, the protection of intangible property and the right to prevent publication required legal protection that extended beyond intellectual property protection and protection from libel or slander. (*ibid*. 2) The "right to be left alone" was thus linked from its inception with the right to prevent publication, an important factor when we consider the development of privacy-by-design as it relates to digital technology. The Universal Declaration of Human Rights, promulgated by the UN General Assembly in 1948, includes specific privacy protections in article 12, taking up the ideas first expressed by Warren and Brandeis on the special protection of an individual's "honour and reputation". (UDHR 1948) The ICCPR renders privacy protection legally binding in international law. General Comment 16, drafted by the UN Committee on Human Rights, focuses on the obligation of States to use legislative tools to protect their citizens' privacy: "this right is required to be guaranteed against all … interferences and attacks whether they emanate from State authorities or from natural or legal persons." (General Comment 16, 1) Although the General Comment was promulgated in 1988, before the advent of the digital revolution, clearly the term "legal persons" is intended to mean business and consequently obliges States to guarantee the protection of user data by technology companies under their jurisdiction.

The Fourth Amendment of the US Constitution and articles 7 and 8 of the Charter of Fundamental Rights of the European Union rigorously uphold the value of privacy. Three seminal court decisions have recently recognized State or business obligations to protect user privacy. In May 2015, a three-judge panel of the 2nd Circuit U.S. Court of Appeals determined that the dragnet collection of American telephone call data does not constitute information relevant to terrorism investigations under Section 215 of the Patriot Act, stating that the program "exceeds the scope of what Congress has authorized" (*ACLU v. Clapper* 2014). The Second Circuit judges did not, however, move beyond statutory law in their decision, leaving a further discussion of the constitutional merits of protection from "unreasonable searches" under the Fourth Amendment to future case law. The European Court of Justice issued an advisory opinion in April 2014 declaring that the European Data Retention Directive of 2006 "interferes in a particularly serious manner with the fundamental rights to respect for private life and to the protection of personal data" (*Digital Rights* 2014). In May of the same year, the court determined in *Google v. Costeja González* that:

> *As the data subject may, in the light of his fundamental rights under Articles 7 and 8 of the Charter, request that the (online) information in question no longer be made available to the general public…, those rights override, as a rule, not only the economic interest of the operator of the search engine but also the interest of the general public in having access to that information upon a search relating to the data subject's name. (Google v. Costeja González* 2014).

Each of these cases provides important legal guidance on the contours of digital privacy. Although our sample is limited, we note that jurisprudence in the United States and Europe is evolving, in general, towards a reinforcement of online user rights that places the burden of privacy compliance on data controllers and governments.

1.2 Privacy-by-Design practices

The notion of privacy seems to be of little concern to an enthusiastic public ready to purchase the latest product on the market. Instead, the value of privacy appears to have diminished with the current pursuit of visibility on social networks and the emergence of digital tools that facilitate self-exposure of the user's private life; in this world, all that matters is grabbing the attention of other users, creating a buzz, remaining visible (CNIL 2012, 45). The value of privacy is temporarily lost in the thrill of a self-generated digital presence; the ease and rapidity of information transfer, the unremitting focus on the number of viewers reached, as well as the ability to narrate one's own existence at any time, create a heady cocktail of virtual control. Nonetheless, a 2015 Eurobarometer survey of 28,000 users across Europe reveals a significant level of mistrust concerning data protection; according to the survey, 81% of Internet users believe that they have little or no control over their online information, while 63% say they do not trust online businesses (Eurobarometer 2015). The impact of the Snowden revelations, along with a rich trove of user anecdotes concerning online privacy violations, have led users to demand greater control over their online data.

Privacy by Design offers a technical response to the contradiction of headlong pursuit of online exposure versus rising levels of public mistrust regarding the eventual use of online data. As participants in project PRIPARE (PReparing Industry to Privacy-by-design by supporting its Application in REsearch) sponsored by the European Commission, we are members of an eleven partner consortium to facilitate the application of a privacy and security-by-design methodologies to protect against Internet disruptions, censorship and surveillance and to foster a risk management culture through educational material targeted to a diversity of stakeholders.[6] Privacy by Design, or the integration of user data protection mechanisms at the very outset of any digital design initiative, remains one of the surest means to protect the user's digital footprint and prevent access to personal data without the user's express, and informed permission. Tools such as a Privacy Impact Assessment (PIA), a rigorous, rights-based evaluation of the impact of any software of information technology system during the planning phase (Wright *et al.* 2013), or Privacy Enhancing Technologies (PETs), including private information retrieval, selective disclosure credentials, or secure multi-party computation (Troncoso 2015), form an integral part of any privacy-by-design methodology.

Project PRIPARE has developed a holistic methodology (PRIPARE 2014 – D1.2) that addresses privacy and security (system security is a prerequisite of system privacy) aspects of business processes from the outset. The PRIPARE methodology is designed to merge with existing engineering or project management practices and covers the entire lifecycle of the system. PRIPARE fosters organizational-wide privacy awareness and, in the design, implementation, verification, and release phases of software and hardware development, ensures privacy and security risk assessment, privacy implementation and demonstration of privacy compliance. The methodology also extends to system maintenance and retirement. The PRIPARE methodology has been designed by integrating and adapting best practices from many methods and policies including the Advanced Open Standards for the Information

[6] www.priparepproject.eu

Society (OASIS) Privacy Management Reference Model (OASIS 2013), Privacy Impact Assessments (Wright *et al.* 2013), Microsoft Security Development Lifecycle (Microsoft 2012), (Privacy) Risk management, Privacy Enhancing Architectures (Kung 2014) and ISO standards. Recognizing the essential role of stakeholders' information and education about the risks, tools, best practices, rights and responsibilities associated with digital security and privacy, PRIPARE provides educational, information and reference material for the main stakeholders: the general public, ICT educators, ICT practitioners, policy makers, and governmental and non-governmental bodies acting for human rights protection (PRIPARE 2014 – D4.2 and D4.3).

2. The value of privacy

Privacy by Design is one way to value privacy in a digital universe. In an upcoming book, we argue that the framework for an overall safe, just and balanced use of digital technology can be found in the universal language of international human rights law (Perry & Roda, forthcoming 2016). The promulgation of binding treaty law for the implementation of human rights has continued apace since the end of the Cold War, alongside the proliferation of multiple channels of communication offered by the growth of information technology: a simultaneous acceleration of the development of the *formal* international human rights framework and the *informal* network of information technologies. Their juncture provides an opportunity to examine privacy from a set of new perspectives. Broader ethical challenges such as our notions of human trust, access, and agency in a digital environment both influence our understanding of privacy and are altered by our use of technology.

2.1 Trust

The value of privacy is enhanced if individual privacy is protected in the public space. The Internet, at its inception, was intended to function as the ultimate public space, a computer-generated environment for communication and the sharing of information that was free and accessible to anyone with a telephone line and a modem. Over time, however, public and corporate actors have learned to control this virtual public arena. While the architecture of the Internet prevents any one government or corporation from fully claiming it, the Chinese government has been remarkably successful in determining how users access the Internet and, more importantly, how they behave online (Perry & Roda 2013). The attention economy is a rapid growth business sector, and the so-called GAFA (Google, Apple, Facebook and Amazon) generate sums equal to the GNP of small countries such as Denmark, ranked as the world's 35th economic power (FaberNovel 2014). More importantly for the purposes of this paper, the GAFA have manipulated personal data to sell targeted advertising and been fairly pliable in assisting the NSA's dragnet searches of user information, enabling the US government to accumulate a vast trove of stored data. Theses breaches of user privacy are massive, opaque and often illegal, impacting our sense of trust online in ways that are difficult to measure.

There is currently a range of scholarly opinion on the value of online privacy. Legal scholar Richard Posner argues that privacy is an overrated construct in a digital society (Posner 2013), while sociologist Richard Harper views our trust in technology as an evolving paradigm (Harper 2014, 10). Helen Nissenbaum's theory of privacy suggests that contextual integrity is at the core of privacy violations (Nissenbaum 2011). Nissenbaum's focus on contextual integrity indicates that our notions of trust are unlikely to adapt to digital technology. Rather, in order to trust the digital environment, users would be well-served to demand privacy-by-design guarantees, built in systems of protection that place digital technology within contextual parameters that value privacy. Users remain wary of the whole

scale spying and data commercialization policies that have become an integral part of the information technology sector. For many, these policies resemble a gigantic bank heist. A bank client knows, however, that even if his or her bank is robbed or subject to failure, obligatory federal or national banking insurance minimizes this type of risk for the user. By assessing the security of systems before they are built and by providing a selection of privacy enhancing tools to the user before he or she enters a data collection system, Privacy by Design functions much like insurance in the banking sector. Users are certainly aware that their privacy may be violated, but they are assured of a certain level of protection against data theft and retain the right to remove their data, render it anonymous or go off the grid altogether. Although the growing ubiquity of the Internet of Things will render trust increasingly problematic for the individual (van den Hoven *et al.* 2012, 11), simple, straightforward, obligatory protections embedded at the design stage of all digital products and systems can function as a form of insurance, returning a certain level of control, and possibly trust, to the user.

2.2 Digital access

When Facebook founder Mark Zuckerberg stated that he hopes to provide online access to all 7 billion members of the human species, he qualified his desire by revealing that he wants everyone to become "addicted to data" (Time 2014). Aside from the odd pairing of an admirable policy to bridge the digital divide and a discourse reminiscent of the tobacco industry, Zuckerberg's initiative raises important questions about digital access and user privacy. As van den Hoven *et al.* point out, we currently have no democratic institutional framework to evaluate the way digital networks distribute benefits, or how they may discriminate or provide differential access (van den Hoven *et al.* 2012, 6). Age, health, social class, and geographic location determine digital access in ways that are complex and, like trust, surprisingly difficult to measure.

Certain populations already made vulnerable by their immutable characteristics may find their frailties enhanced or diminished by digital technology. We have written on the issue of vulnerability and digital hardware, arguing that wireless technology has been rolled out by force, with scant attention paid to the potential long-term health impact of exposure to heightened electromagnetic wave pollution (Roda & Perry 2014). In response, the French government has recently passed legislation that mandates protection of citizens suffering from electromagnetic wave pollution (*Loi Abeille* 2015). The Swedish government recognizes electromagnetic sensitivity as a handicap and provides financial relief to that part of the Swedish population suffering from exposure to wireless technology.[7] But, for every child or adult who requires protection from electromagnetic pollution, there is a vulnerable individual clamoring for access to the digital universe. The elderly and the disabled can benefit from regular monitoring, robotic assistance with household tasks, and reduced isolation through online visits with family, e-learning, e-voting and enriched discussion platforms. As the cost of technology declines, the poor are able to take advantage of increased online access to information, education and State services, as well as the possibility of providing service skills long distance, without having to migrate or leave children in the care of relatives. Cabled access to digital systems with built-in privacy enhancing technologies may be one way to offer both protection and access to an array of vulnerable populations with very different needs. Rather than simply aim to provide digital access (and data addiction) to all citizens, policymakers should adopt a more nuanced position, one that evaluates the quality of user

[7] Sweden has been a pioneer in designating electrosensitivity as a handicap under the Swedish Act concerning Support and Service for Persons with Certain Functional Impairments and the Swedish Social Services Act.

experiences and whether core human rights are protected or enhanced in a digital environment.

2.3 Agency

Long before the advent of digital technology, filmmaker Stanley Kubrick imagined a universe hijacked by computers in *2001: A Space Odyssey*. Despite current concern with killer robots run amok,[8] we think that Kubrick's world will remain imaginary, at least for the foreseeable future. Human intelligence, although far less precise than artificial intelligence, is wide ranging and incorporates the ability to question, create and reflect, qualities that machines cannot produce with the same rapidity as humans (Littman 2015, 13). Nonetheless, the digital environment challenges our notion of human integrity, a characteristic that van den Hoven *et al.* describe as the ability to make autonomous decisions and exert control over one's environment (van den Hoven *et al.* 2012, 11). When we speak of integrity, we often think of the concept of agency – the ability to choose our own thoughts and actions. Although agency is encumbered by a long philosophical history centred on the issue of free will, the challenges poses by advances in neuroscience and psychology (Appourchaux 2014), bolstered by post-modern scepticism (Pereboom 2014), encourage us to think about the role of human agency in a digital environment. But, how can we exercise agency if we offload our decision-making capacity to a machine? The misuse of personal data, large scale spying and the dominant discourse of "smart" machines threaten our integrity and our ability to choose how we interact with the technology that surrounds us.

Yet, according to the free will theorem developed by mathematicians John Conway and Simon Kochen, our agency exists and influences everything around us, ranging from other humans to the smallest particles in the universe. While at first glance it may seem unusual to link mathematical theory with the ethics of online privacy, Conway and Kochen's work demonstrates that at any given moment the universe is not constrained by its past, but is free to evolve (Delahaye 2009). Thus, two scientists engaged in the same experiment in two different laboratories might not come up with the same results. It is the infinite variety of human traits (psychological or physical), rather than any pre-determined history, that informs our choices (Conway & Kochen 2006). The potential ramifications of the free will theorem on our use of digital technology are striking. In essence, technological determinism, or a world run by machines, is the reverse side of unmitigated enthusiasm for a fully digitized environment (CNIL 47). Neither is set in stone, as each individual has the potential to modify his or her understanding and use of technology. Moreover, Conway and Kochen insist that "the stage is still being built while the show goes on" (*ibid*. 27), a notion which, when applied to digital technology, empowers an individual to modify his or her use of machines, as well as the architecture and function of the technology itself. Privacy-by-design methods enhance our ability to influence the construction of the digital stage, allowing users and non-users alike to re-think notions of trust, access and agency and to determine their evolution in a digital world.

Conclusion

The value of privacy is perhaps most appreciated once it has been lost. No simple solutions are available, however, to address the questions and trade-offs that the design and use of digital technology pose to individuals and society - the problem of privacy in public. We have argued that a privacy-by-design approach, which joins legal, educational and technical components within a holistic framework, allows us to respond to these challenges in

[8] See: http://thefutureoflife.org

such a way as to enhance the value of privacy as a human right and ground our enthusiasm for digital technology within the parameters of user control.

BIBLIOGRAPHY

Appourchaux, K. (2014). *Un nouveau libre arbitre*. Paris: Editions CNRS.

CNIL (2012). *Vie privée à l'horizon 2020: paroles d'experts*. Cahier n°1. Cahiers IP: innovation et prospective.

Conway, J., Kochen, S. (2006) The Free Will Theorem, *Foundations of Physics* 36 (10): 1441.

Delahaye, J.-P. (2009). Libre arbitre et mécanique quantique, *Pour la Science*, N°386, December.

European Commission (2015). *Data protection Eurobarometer Factsheet*. June: http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_eurobarometer_240615_en.pdf

FaberNovel (2014). *GAFAnomics: new economy, new rules*. 24 November: http://fr.slideshare.net/faberNovel/gafanomics

Grossman, L. (2014). Inside Facebook's Plan to Wire the World, *Time Magazine*. 15 December.

Harper, R. (*ed.*) (2014). *Trust, Computing and Society*. London: Cambridge University Press.

Kung, A. (2014). "PEARs: Privacy Enhancing Architectures", Privacy Technologies and Policy in Lecture Notes in Computer Science, Volume 8450, 2014, pp. 18-29. http://link.springer.com/chapter/10.1007%2F978-3-319-06749-0_2

Littman, M. (2015). Humanity-Centered Robotics Initiative, *Brown University Alumni Monthly*, March-April.

LOI n° 2015-136 du 9 février 2015 relative à la sobriété, à la transparence, à l'information et à la concertation en matière d'exposition aux ondes électromagnétiques ("Loi Abeille"), JORF n°0034 du 10 février 2015, page 2346, texte n°1.

Microsoft (2012). Security Development Lifecycle (SDL) Process Guidance, version 5.2, May. http://download.microsoft.com/download/3/4/3/343BAFCB-C685-4A70-9639-FF76BCBB609C/Microsoft%20SDL_Version%205.2.docx

Nissenbaum, H. (2011). A Contextual Approach to Privacy Online, *Daedalus* 140 (4), Fall: 32-48.

Nissenbaum, H. (1998) Protecting Privacy in an Information Age: the problem of privacy in public, *Law and Philosophy*, 17: 559-596.

OASIS. (2013). Organization for the Advancement of Structured Information Standards (OASIS), Privacy Management Reference Model and Methodology (PMRM), Version 1.0. July. http://docs.oasis-open.org/pmrm/PMRM/v1.0/PMRM-v1.0.pdf

Office of the High Commissioner for Human Rights, CCPR General Comment No. 16: Article 17 (Right to Privacy) The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation. Adopted at the Thirty-second Session of the Human Rights Committee, 8 April 1988.

Pereboom, D. (2014). *Free Will, Agency, and Meaning in Life*. Oxford: Oxford University Press.

Perry, S., Roda, C. (2016 forthcoming). *Human Rights and Digital Technology*. London: Palgrave MacMillan.

Roda, C., Perry, S. (2014a). Mobile Phone Infrastructure Regulation in Europe: Scientific Challenges and Human Rights Protection. *Environmental Science and Policy* 37(2014) 204-214.

Perry, S., Roda, C. (2014b). Teaching Privacy by Design to Non-Technical Audiences. Cyber Security and Privacy (CSP) Forum 2014. *Springer CCIS Series*, Vol. 470.

Perry S., Roda C. (2013). Paper on *Conceptualizing and Contextualizing the Changing Nature of Internet Usage in China.* China and the New Internet World: The Eleventh Chinese Internet Research Conference (CIRC11) - Oxford Internet Institute, Oxford, June.

Posner, R. (2013) "Privacy is Overrated", *New York Daily News*. 28 April.

PRIPARE 2014, Deliverable 1.2 “Privacy and Security-by-design Methodology”, ICT-610613 - http://pripareproject.eu/research/

PRIPARE 2014, Deliverable 4.2 “Initial Educational Material”, ICT-610613 - http://pripareproject.eu/research/

PRIPARE 2015 (Forthcoming), Deliverable 4.3 “Final Educational Material”, ICT-610613 - http://pripareproject.eu/research/

Simon, H. (1957). "A Behavioral Model of Rational Choice", in Models of Man, Social and Rational: Mathematical Essays on Rational Human Behavior in a Social Setting. New York: Wiley.

Troncoso, C. (2015). Privacy-preserving tools to support privacy-by-design, *Security Engineering Forum*. 30 January: http://www.securityengineeringforum.org/blog

Van den Hoven, J., Guimarães Pereira, A., Dechesne, F., Timmermans, J., Vom Lehn, H. (2012). *Fact sheet – Ethics Subgroup IoT*, Report for DG Connect, version 4.0.

Universal Declaration of Human Rights, G.A. res. 217 A (III), adopted by the U.N. Doc. A/810 (December 10, 1948).

Warren, S. and Brandeis, L. (1890) “The Right to Privacy”, *Harvard Law Review*. Vol. IV, No. 5.

Wright, D. & Friedewald, M. (2013) Integrating privacy and ethical impact assessments, *Science and Public Policy* 40, 755–766.

Caselaw

ACLU v. Clapper, US Court of Appeals, 2d Circuit, Docket No. 14-42-cv, 7 May 2015.

European Court of Justice (2014) Judgment of the Court (Grand Chamber) in *Google v. Costeja González*, C‑ 131/12, 13 May, Ruling 4.

European Court of Justice (2014) *Judgment in Joined Cases C-293/12 and C-594/12 Digital Rights Ireland and Seitlinger and Others*, 8 April.