IRIE
International Review of Information Ethics Vol. 22 (12/2014)

Caroline Rizza and Laura Draetta:

The "silence of the chips" concept: towards an ethics(-by-design) for IoT

Abstract:

In this position paper, we would like to promote the alternative approach positioned between the two extreme positions consisting in refusing any innovation or in adopting technology without questioning it. This approach proposes a reflexive and responsible innovation (von Schomberg, 2013; 2011; 2007) based on a compromise between industrial and economic potentialities and a common respect of our human rights and values. We argue that the "silence of the chips right" (Benhamou, 2012; 2009) is timely, relevant and sustainable to face ethical challenges raised by IoT such as protecting privacy, trust, social justice, autonomy or human agency. We believe this technical solution may support establishing an ethics of IoT embedded in the technology itself. Our position is not 'technocratic': we do not agree with discourses arguing technology can fix problems. Through the responsible research and innovation approach we promote the idea that only human agency and user empowerment constitute a valid answer to the ethical, legal and social issues raised by IoT.

Agenda:

Authors:

Caroline Rizza, PhD,

- Associate Professor, Economics, Management and Social Sciences Department, Institut Mines Telecom / Telecom ParisTech, I3 UMR 9217 – CNRS. 46 Rue Barrault 75634 Paris Cedex 13 - France
- ☎ + 33 - 145 - 81 81 35, ✉ caroline.rizza@telecom-paristech.fr
- Relevant publications:
  - Curvelo P, Guimarães Pereira Â, Boucher P, Breitegger M, Ghezzi A, Rizza C, Tallacchini M, Vesnic-Alujevic L (2014). The constitution of the hybrid world: How ICTs are transforming our received notions of humanness. EUR, VARESE: Luxembourg: Publications Office of the European Union, doi: 10.2788/58678
  - Rizza C, & Guimarães Pereira A, Ed.(2013)."Ethics of Social Networks for Special Needs Users". ETHICS AND INFORMATION TECHNOLOGY, Springer: Netherlands.
  - Rizza C, Curvelo P, Crespo I, Chiaramello M, Ghezzi A, & Guimarães Pereira Â (2011). Interrogating privacy in the digital society: media narratives after 2 cases. INTERNATIONAL JOURNAL OF INFORMATION ETHICS, vol. 16, p. 6-17.

Laura Draetta, PhD,

- Associate Professor, Economics, Management and Social Sciences Department, Institut Mines Telecom / Telecom ParisTech, I3 UMR 9217 – CNRS. Campus SophiaTech, 450 Route des Chappes - 06410 Sophia Antipolis – France.
- ☎ + 33 - 493 - 00 84 09, ✉ laura.draetta@telecom-paristech.fr http://email/
- Relevant publications:
  - Draetta L. et Delanoë A., 2012, RFID une technologie controversée. Ethnographie de la construction sociale du risque, Paris : Hermès-Lavoisier.
  - Licoppe C., Draetta L. et Delanoë A., 2013, « Des smart grids au quantified self. Technologies réflexives et gouvernement par les traces », Intellectica, N° 59
  - Draetta L. et al., 2007, Ecologie des infrastructures numériques, Paris: Hermès Sciences.

Introduction

In 2011, in the ERIE special issue on "Ethics of Online Social Networks", we addressed privacy concerns with regards to online social network's use and news media's way of framing events without considering the ethical issues raised by such practices (Rizza, et al., 2011). At that time, our main concerns were related to users' expectations with regards to technology. We showed that social networks, and more generally main parts of emergent technologies, do not protect users from involuntary exposure due to either mistaken uses, or lack of control over published personal information. In this context, we considered that initiatives such as technologies embodying "ethics-by-design" or "privacy-by-design" concepts, as well as proposals for placing changes in regulation such as Poullet's (2010) ideas of Internet as virtual dwelling, were constituting relevant solutions to protect users and citizens from technologies and promote "ethical machines" (Sarah Spiekermann's blog 2014[1]).

Four years after, our concerns, threats and fears are coming from an even more "powerful" and ubiquitous Internet, called the 'Internet of things' (IoT). As presented in the call for papers the very concept of IoT was originally proposed in 1999 by Asthon to address the advent of RFID technology. But today IoT refers to various aspects: *"(i) the resulting global network interconnecting smart objects by means of extended internet technologies, (ii) the set of supporting technologies necessary to realize such a vision (including, e.g. RFIDs, sensors/actuators, machine-to-machine communication devices, etc.), and (iii) the ensemble of applications and services leveraging such technologies to open new business and market opportunities"* (Miorandi, Sicari, De Pellegrini, & Chlamtac, 2012). By 2020, 50 to 80 billion objects will be connected and will organize our daily life. Consequently, the IoT will be based on various mass-disseminated miniaturized technological devices. Combined, or not, with Big Data capabilities, this mass-dissemination of even more numerous and miniaturized smart objects will not come without a certain impact on our environment, health, and way of living (Draetta & Delanoë, 2012): it already questions our policy makers and us, as researchers.

In this position paper, we would like to promote the alternative approach positioned between the two extreme positions consisting in refusing any innovation or in adopting technology without questioning it. This approach has been brought and supported by researchers, entrepreneurs, and regulators for years and proposes a reflexive and responsible innovation (von Schomberg, 2013; 2011; 2007) based on a compromise between industrial and economic potentialities and a common respect of our human rights and values. More specifically, responsible research and innovation *"is a transparent, interactive process by which societal actors and innovators become mutually responsive to each other with a view to the (ethical) acceptability, sustainability and societal desirability of the innovation process and its marketable products (in order to allow a proper embedding of scientific and technological advances in our society)"* (von Schomberg, 2011, p. 9). Applied to the IoT context, we present the "silence of the chips right" as defined by Benhamou (2012; 2009) and we argue that it is timely, relevant and sustainable to face ethical challenges raised specifically by IoT when protecting citizen rights and values such as privacy, trust, social justice, autonomy and human agency. We believe the "silence of the chips" technical solution may support establishing an ethics of IoT embedded in the technology itself. Our position is not 'technocratic': we do not agree with discourses arguing technology can fix problems. Through the Responsible research and innovation approach we deeply believe and promote the idea that only human agency and user empowerment constitute a valid answer to the ethical, legal and social issues raised by technology and, in this particularly case, by IoT.

The paper is structured as followed: First part presents the main aspects of the literature review with regards to the ethical, legal and social concerns raised by IoT, as well as the responsible research and innovation approach. Second part addresses the present European context of IoT and RFID technologies deployment, and highlights the relevance of the "de-activation tag" technical solution in this context. In a third part, we focus on the "silence of the chip" right and show how, through the de-activation tag technical solution, it could contribute to the users' empowerment and protection from the ethical, legal and social issues as they have been emphasized in the state of the art. Last but not least, the discussion we bring in the fourth part puts

[1] See : http://derstandard.at/r1326504100796/Die-ethische-Maschine

human agency and co-responsibility of societal actors and innovators at stake shedding light on why the ability to "shut down" the IoT chips should be implemented "by-design".

We conclude arguing that both the promotion of "the silence of the chips" right and its incorporation in IoT objects following an "ethics-by-design" approach, would allow us (as responsible citizens, researchers, regulators, etc.) to formulate an ethics for IoT, i.e. mainly focused on the ethical, legal and social challenges the IoT raises. In this context, the CIPRIoT research project is aiming at studying and – we hope so – stating the socio-technical viability of such concept.

State of the art

Ethical, legal and social concerns raised by the IoT

Technical papers in the field of IoT and ambient Intelligence underline the security and privacy issues raised by the deep penetration of technology in our everyday life associated with automation and remote interactions (e.g. Madeglia & Serbatini, 2010). Data collection, storage, mining and provision new capabilities combined with an increasing number of objects providing services, constitute so many possibilities of users' personal data collection (Ibid.).

Weber (2010) sheds light on the IoT security and privacy challenges from a legal point of view. To do so, he bases his analysis on the IoT architecture, i.e. an IT infrastructure composed by data communication tools (primarily RFID tagged objects) aiming at facilitating "communication" or "data flow" in a secure and reliable manner to provide a service. "Globality" – in the sense that the technology is used all over the world; "verticality" – due to the potential durability of the technical environment; "ubiquity" – referring to the technology possibility to be used ubiquitously to encompass persons, things, etc.; and "technicity" – due to the complexity of the tags, passive or active, and of the background device – characterize the IoT. These characteristics require new regulatory approaches guarantying privacy and security such as attacks' interception, data authentication, access control and guaranty of users' privacy (natural and legal persons). According to Weber (2010), IoT calls for a heterogeneous and differentiated legal framework: on one hand geographically limited national legislation does not seem appropriate; on the other hand, self-regulation may not be sufficient. Consequently, a solution could be the combination of a framework of key principals set at the international level combined with a more detailed regulation by the private sector (Ibid.).

As many others scholars, we consider that concerns about IoT go beyond privacy issues. IoT's event stresses more than ever a profiling logic of data identification, categorization and clustering without taking into consideration the context such data has been collected from (Hildebrandt & Gutwirth, 2007). Curvelo et al. (2014) warn against these "things" which collect and store data, forming a multiplicity of 'dossiers' on the user whereabouts that may be used in unexpected contexts. Consequently, the main question is not the "abuse" but the users' incapability to know whether and when their profiles are used or abused (Hildebrandt & Gutwirth, 2007).

In a hyper-connected era (Dewandre, 2013) where the promised interconnectivity through the IoT involves billions of smart human and non-human objects and transactions, "consent" may become an absurd concept (Curvelo, et al. 2014) and people may lose autonomy. According to Rizza (2014; 2006) the digital divide relies on several dimensions: access (to technology), digital competences in using in an accurate way technology to aim specific objectives, as well as supporting citizens' action. Some authors (e.g. Curvelo et al., 2014; Guimarães Pereira, Benessia, & Curvelo, 2013) consider IoT as an additional layer of divide between knowledgeable and skilled enough users to master the technology and to keep control, and disempowered users who do not question technology and do not protect themselves from abuse. Among the technological offer, empowered users are able to choose and even to drop-out a technology, whereas disempowered users become progressively more deskilled, disempowered and unknowledgeable. Consequently, IoT could compromise human agency through what Curvelo et al. (2014) call "consent fatigue": the rising divides in this case are not exclusively related to lack of skills to deal with the complexity of interactions, but also to additional challenges in terms of knowledge production, skills development and empowerment.

Responsible research and innovation and privacy/ethics-by-design approaches

Scholars have long demonstrated the co-evolution of technology and society (e.g. Latour, 1992; Jasanoff, 1995). Feenberg (2010) articulates this as a democratic paradox: "the public is constituted by the technologies that bind it together but in turn it transforms the technologies that constitute it". However, von Schomberg (op. cit.) argues that the classical ethical theory and the conventional ethical practice do not address both aspects of unintentional consequences and collective decisions that should be taken into account while considering the issues of ethical responsibility in scientific and technological developments. Consequently, the interplay between IoT and privacy is part of a broader and long-debate (e.g. De Hert, 2009; Hildebrandt & Gutwirth, 2007).

De-activation tag technical solution in the European context

While the global market for RFID applications and IoT objects is expected to grow (Das & Harrop, 2014), an ongoing public debate is questioning the ethical, legal, and social implications of such ambivalent technology, whose technical features constitute its main challenges with regard to its co-construction with society (Draetta & Delanoë, op. cit.). For instance, the new European Norms and standards on RFID Privacy Impact Assessment and RFID Signage adopted last July[2], in completion with EU Data Protection rules and the Commission's 2009 recommendation on RFID, aim to help RFID and smart chips users and to protect European citizens/consumers while supporting at the same time this new market development. Nevertheless, surveillance - through traceability and technological opacity - and radiofrequencies emission when functioning, place RFID technology at the center of emerging controversies (Thiesse, 2007) with regards to major risks and concerns about privacy, public health and environmental impact.

Some initiatives are attempting to deal with current critique of technology contempt of ethical and societal concerns (e.g. Rizza, et al., 2011) by developing for instance technology embodying "ethics-by-design" or "privacy-by-design" paradigms (EC, 2010, p. 12), or by placing changes in regulation that currently implement traditional ethical concerns. In our context, a very practical example of this approach is the de-activation of RFID tags. Experiments are underway to test the possibility of de-activation tags attached to retailer goods after the sale. Indeed, RFID opponents consider that users' privacy infringement (individuals or enterprises) constitutes one of the main threats of RFID large-scale deployment due to RFID tags' invisibility and opacity. Conjointly, the social viability of smart tags' large-scale deployment strongly depends of public confidence with respect to the data protection the technology supports. So far, "killing" the chip was the only technical solution to protect users: once a product bought, the consumer is advised to destruct the tag initially placed in the product for inventory management or commercial reasons. Nevertheless, this solution does not fit the industrial opportunities chips could offer in terms of panel of services for users, and does not support IoT deployment. Consequently, instead of "killing" the chips, the systematic and reversible tag de-activation could constitute a sustainable technical and business solution.

The "silence of the chips" concept: towards an ethics(-by-design) for IoT?

Following the "deactivation tag" idea, Benhamou (op. cit.) presents the "silence of the chips right" as a means to establish trust between the different stakeholders: policy makers and industrials, on the one hand, users/citizens on the other hand. Indeed, the "silence of the chip" concept allows to face and master chips' specificities

[2] European Commission, IP/14/889, 30/07/2014: http://europa.eu/rapid/press-release_IP-14-889_en.htm

such as their "durability", their "increasing numbers", and the data flow "opacity" they support. In this part, we then argue that the "silence of the chips right" (Ibid.) is timely, relevant and sustainable to face ethical challenges raised by IoT in terms of citizen rights and values protection such as privacy, trust, autonomy and human agency. By including "by-design" the "silence of the chip" concept in IoT, technology could support an ethics of IoT embedded in the technology itself.

Nevertheless, the 'silence of the chips' concept is at the center of a social-political and scientific controversy[3]. Some stakeholders suggest it is 'obsolete' due to the technical impossibility of erasing citizens' digital traces and due to "the paradigm shift" in the technology-society interactions (e.g. Ganascia, 2011). They propose to forget the "silence of the chips" concept and to adapt to the irrevocable pervasiveness of digital traces at the time when publishing and sharing one's own performance data have become the every-day life natural conditions of the "homo numericus" (Doueihi, 2008). To do so, they advocate a legal modification of the privacy concept as well as the promotion of citizens' resilience and empowerment.

Between the two extreme positions consisting in adopting this technocratic approach or in refusing any innovation and possibility of compromise, we think – as suggested by von Schomberg (op. cit.) - that responsible research and innovation constitutes another way-of-doing which would fully apply on the IoT context. By proposing a reflexive and responsible innovation based on a compromise between industrial and economic potentialities, and a common respect of our social contract's pillars such as Freedom, Education, Health, or Environment, and our human rights and values (Draetta, Musiani, Tessier, 2014), this approach would support us elaborating and applying a thoughtful response from both research and society to a field which is far from being just technical.

Following Benhamou's (op. cit.) idea, we consider the "silence of the chips right", i.e. the technological possibility to make the chip "silent" by de-activating it, a technical solution to both promote the IoT market development and support/protect "by-design" citizens' rights and human values.

Discussion: co-responsibility and human agency at stake

The state of the art allows to frame the ethical legal and social concerns related to the IoT advent. From a technical point of view, the increasing number of IoT objects combined to their ubiquity, their durability and complexity (Weber, op. cit.) raises security challenges to preserve users' privacy (Madeglia & Serbatini, op. cit.; Weber, Ibid.). IoT constitutes an additional technical capability in collecting, storing and processing users' personal data for economic and commercial purposes. But, overall, the IoT data-flow opacity does not allow users controlling their own data. As suggested by Curvelo, et al. (op. cit.) and Hildebrandt & Gutwirth (op.cit.), in the IoT context users are not protected from any abuse due to their incapability to know whether, when and where their data is used.

In this context, we claim that, so far, IoT has been implemented in a technocratic way disempowering users from their capability to question, choose or even drop out the technology. So far, in this 'new' market the IoT constitutes, IoT objects are proposed and sold to fix everyday 'little' problems citizens are facing: everything can be monitored through sensors to simplify users' life. As an illustration, during the Leroy Merlin workshop "Inhabitants, housing and digital data: towards a new and controlled porosity of the housing borders?"[4], Blandine Calcio Gaudino shed light on the simplistic way elderly is explained how IoT is implemented in their own home and is asked to not being worried about anything since sensors will "take care" of "everything". We consider that present technocratic discourses coming with the IoT implementation simplify the IoT complex

[3] See: The Observatory for Responsible Innovation workshop's follow-up on "La RFID à l'épreuve de l'innovation responsable", 14/03/2014: http://www.debatinginnovation.org/?q=node/116

[4] Leroy Merlin third conference on housing - Workshop "inhabitants, housing and digital data: towards a new and controlled porosity of the housing borders?" – speakers Calcio Gaudino B., Desbiey O., Rizza C., & Sadde G., 11/02/2015: http://leroymerlinsource.fr/savoirs-de-l-habitat/chez-soi/assise-de-lhabitat-2014/

reality and contribute at the same time to disempower users, expending without their own knowledge the digital divide.

In some way, the new European Norms and standards on RFID Privacy Impact Assessment and RFID Signage (July 2014, op. cit.) constitutes a first attempt to make aware citizens/users about the RFID or IoT chips presence in an object. This is not about modifying the legal definition of privacy in order to “respond” to the new and irrevocable technical capability in tracing and profiling users, but it is all about making transparent what was not anymore visible in order to empower users and to protect them.

In this context, we argue that, by giving the possibility to users to make silent the chips embedded into the technologies or objects they are using or owning, the "silence of the chip" concept makes possible – again – human agency. Indeed, the “silence of the chip” concept allows users to give consent to their data’s transmission/collection – responding to the first privacy concern raised in the literature review. But more specifically, the silence of the chip concept induces users’ awareness about the presence of a ‘smart’ chip in the object they are using. Consequently, it makes visible processes which were no longer transparent. Doing so, it contributes to a better understanding on what is going on through the IoT object or technology, reducing IoT use’s complexity but, first of all, preventing users from “abuse”. Second, giving users the ability of silencing the chip requires them to assess opportunities of activating or de-activating tags with regards to their uses and needs: they are not anymore passive in front of a technology managing their environment and “fixing” their problems. Consequently, the “silence of the chip” concept also addresses concerns related to users’ autonomy. It supports users’ empowerment with regards to IoT technology.

Last but not least, following the responsible research and innovation approach (von Schomberg, op. cit.), we would like to insist on societal actors’ and innovators’ co-responsibility when developing and implementing a technology. “By-design” a technology should embed the human values we (as innovators, researchers, entrepreneurs, policy makers, citizens/users) would like to defend and promote in our society: “by-design” the IoT should respect and promote user’s privacy, autonomy, social justice, etc. But, as we have already claimed, we also deeply consider that a technology cannot fix users’ problems, cannot replace “human” action. If sensors can ‘allow’ elderly to stay home instead of being hospitalized, an elderly cannot be responsible in case something happens during a moment the chip would have been switched off: technology, in this case sensors, has to be implemented to support a team helping an elderly to stay home, but under no circumstances has to substitute human agency. Another relevant illustration is the French case emerged in the early 2000 when clinics asked future parents to sign a disclaimer if they refused their newborns were equipped with electronic tagging to prevent any rapt. Users and stakeholders (social actors, policy makers, entrepreneurs, etc.) are co-responsible when implementing or using a technology in a specific context and use. Users’ empowerment cannot be a motive of releasing stakeholders from their responsibility. “By-design” giving to users the means to question technology and to act (through the de-activation/re-activation tag possibility) will make IoT ethically acceptable and socially desirable[5].

Conclusion

Studying online social networks, Walther (2011) has shed light on Internet online users’ misplaced presumption: 1) that online behaviors were private; 2) that the Internet nature was incommensurate with privacy as we have known it; and 3) that private online “conversations” remained as such. At that time, already, we agreed with the idea that Internet and emergent technology were not protecting their users, and that technology should “by-design” include concepts, values, we would like to promote and protect. Four years after, the “hybridation” of real and virtual worlds through the IoT constitutes again more than ever a threat for these values – e.g. privacy, autonomy, social justice, human agency. More than ever, a responsible research and innovation promoting technology embedding by design our human rights and values is timeline. In some way, the silence of

[5] Please note that von Schomberg’s definition of responsible research and innovation also includes a “sustainable” dimension we have not taken into consideration in this paper.

the chip concept based on the deactivation tag technical solution would support what the new European Norms and standards on RFID Privacy Impact Assessment and RFID Signage (supra) is attempting to implement: protecting citizens' privacy and raising their awareness while promoting the European RFID and IoT market development. This is why, in a shared co-responsible approach of innovation, we consider that both promoting "the silence of the chips" concept and incorporating it through the de-activation tag technical possibility in IoT technologies following an "ethics-by-design" approach, would allow us (as responsible citizens, researchers, regulators, etc.) to formulate an ethics for IoT, i.e. mainly focused on the ethical, legal and social challenges it raises.

In this context, we started last January, a sociological research project in order to assess the socio-technical viability of the "silence of the chips" concept in RFID systems for IoT contexts. The CIPRIoT project[6] aims at:

1) Bringing elements of scientific knowledge in the field of hybridization phenomena between technological innovation, social innovation and value creation;
2) Proposing to policy makers and industry recommendations and guidelines in order to understand societal implications of RFID and IoT technologies, as well as promote a responsible and sustainable innovation based on users' protection through an "ethics-by-design" R&D.

To do so, we are conjointly studying the social demand and the operational viability of the "silence of the chip" concept through three analysis levels: 1) macro level: scientific and socio-political controversies as they emerge in the scientific and mainstream literatures as well as digital spaces; 2) Meso level: industrial R&D projects in the RFID and IoT fields through a documentary analysis and interviews with industrials project leaders; 3) Micro level: "smart home" use case.

References

Benhamou, B. 2012. Les mutations économiques, sociales et politiques de l'internet des objets. Cahiers Français – Documentation Française, 4 décembre 2012.

Benhamou, B. 2009. Internet des objets. Défis technologiques, économiques et politiques, Revue Esprit, Mars-Avril.

Curvelo P. et al. 2014. The constitution of the hybrid world: EU Scientific & political report. Publications Office of the European Union.

Das R. and Harrop, P. 2014. "RFID Forecasts, Players and Opportunities 2014-2024", IDTechEx report, July: http://www.idtechex.com/research/reports/rfid-forecasts-players-and-opportunities-2014-2024-000368.asp

Dewandre, N. 2013. Rethinking the Human Condition in a Hyperconnected Era, The Online Manifesto, DG Connect, European Commission.

Doueihi M. 2008, La Grande conversion numérique, Paris : Le Seuil.

Draetta L. et Delanoë A., 2012, RFID une technologie controversée. Ethnographie de la construction sociale du risque, Paris : Hermès-Lavoisier

Draetta L., Musiani F., Tessier D., 2014, RFID and responsible innovation: towards a positive compromise?, Debating Innovation, Vol. 4(1): 9-15.

European Commission, 2010. "A comprehensive approach on personal data protection in the European Union", COM(2010) 609 final, Brussels, 4.11.2010

Feenberg A. 2010. Between reason and experience: essays in technology and modernity. Cambridge MA: The MIT Press.

[6] "Use information, hide the trace: CItizen's Privacy in RFID and IoT contexts. Exploratory study for the socio-technical viability of the 'silence of the chips' concept " Research project funded by the Foundation Mines-Telecom.

Ganascia J.-G. 2011. The new ethical trilemma: Security, privacy and transparency, Comptes Rendus Physique, vol. 12 (7), pp. 684-692.

Guimarães Pereira A., Benessia A., & Curvelo P. 2009. Agency in the Internet of Things, JRC Scientific and Policy Report, Publications Office of the European Union.

Hildebrandt M. and Gutwirth S. (Eds). 2007. Profiling the European Citizen. Cross-disciplinary perspectives, www.fidis.net

Jasanoff S. 1995. Science at the Bar: Law, Science, and Technology in America, a Twentieth Century Fund book, Cambridge, MA: Harvard University Press.

Latour B. 1992. Where are the Missing Masses? The Sociology of a Few Mundane Artifacts, in: Shaping Technology/Building Society: Studies in Sociotechnical Change, Bijker, W.E. and Law, J. (Eds), MIT Press, USA, 225-258.

Madeglia, C.M. & Serbatini, A. 2010. An overview of privacy and security issues in the Internet of things. In: D. giusto et al. (eds.), The Internet of things: 20th Tyrrhenian Workshop on digital communications, DOI 10.1007/978-1-4419-1674_38

Miorandi, D., Sicari, S., De Pellegrini, F., & Chlamtac, I. 2012. Internet of things: vision, applications and research challenges. Ad Hoc Networks. http://dx.doi.org/10.1016/j.adhoc.2012.02.016

Poullet Y. 2010. About the E-Privacy Directive: Towards a Third Generation of Data Protection Legislation? In: Data Protection in a Profiled World, Springer Netherlands: 3-30.

Rizza C. et al. 2011. Interrogating privacy in the digital society: media narratives after 2 cases, International Journal of Information Ethics, vol. 16; p. 6-17.

Rizza C. 2014. Digital divide. In: Alex C, Michalos, Encyclopedia of Quality of Life and Well-Being Research. p. 1619-1621, DORDRECHT: Springer.

Thiesse, F. (2007), "RFID, privacy and the perception of risk: A strategic framework", The Journal of Strategic Information Systems, 16(2): 214–232.

Von Schomberg R. 2007. From the ethics of technology towards an ethics of knowledge policy/knowledge assessment. Publication series of the Governance and Ethics unit of DG Research. Brussels, European Commission.

Von Schomberg R. 2011. Prospects for Technology Assessment in a framework of responsible research and innovation. In: M. Dusseldorp and R. Beecroft (eds). Technikfolgen abschätzen lehren: Bildungspotenziale transdisziplinärer Methode, p. 39-61, Wiesbaden: Springer VS.

Von Schomberg R. 2013. A vision of Responsible Research and Innovation, in Owen R. et al. (eds.), Responsible Innovation, London: Wiley, 51-74.

Walther, J. B. (2011). Introduction to Privacy Online. Privacy Online: Perspectives on Privacy and Self-disclosure in the Social Web. S. Trepte and L. Reinecke. Heidelberg, Springer: 3-8.

Weber, R.H. 2010. Internet of Things – New security and privacy challenges, computer Law and security Review 26(2010) pp. 23-30.