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

Sandrina Dimitrijevic:

Ethical Consequences of Bounded Rationality in the Internet of Things

Abstract:

One of the main challenges that the arriving paradigm of Internet of Things brings to society is providing and securing individual privacy. There are lots of obstacles which prevents us from successfully confronting such a challenge. In this paper we are going to deal with one such obstacle, and that is the bounded rationality of humans as participants in the environment of Internet of Things. We argue that the ethical approach to the vision of the Internet of Things has to include the notion of bounded rationality. Bounded rationality of users impedes the possibility of giving informed consent. Informed consent is required when getting permission for collecting and using somebody's personal information. Lastly, we discuss the need for a paternalistic approach of maximum possible default privacy settings without asking for consent, given the seriousness of all potential risks.

Agenda:

Author:

MSc: Sandrina Dimitrijevic

- PhD candidate at the Faculty of Economics, Belgrade University
- anirdnas@gmail.com

ISSN 1614-1687

Development of information technologies is proceeding very fast, and one of the expected steps in such process is the arrival of Internet of Things. Internet of Things presents a scenario where multiple things we are surrounded with can communicate between each other, without people being aware of it. Such scenario has multiple possible benefits, but brings with itself a lot of challenges as well. The most important and critical challenge is the endangerment of personal privacy. The pervasive interconnectedness of smart objects makes privacy concerns larger than ever. In the paradigm of Internet of Things risks will be distributed much more widely compared to the present situation[1]. Some of the dark scenarios of new technologies include possibility of surveillance in real time or disappearance of the difference between public and private space[2].

For such reasons, proactive approach to design and implementations of such technologies is needed. Ethical issues should be evaluated carefully. Solving the challenges of new technologies will undoubtedly involve new ethical rules, standards and ways of behaviour, much different than the one which already exist in offline environment[3].

How can privacy be jeopardized in the Internet of Things?

Right to privacy has been recognised as one of the most essential human rights in society. It helps nurture democratic societies, ensures human dignity and freedom of speech and choice.

Information and communication technologies make things people perform every day far easier, and bridge the gap of space and time. Internet of Things is being made with the purpose of bringing greater benefit to human kind[4].

However, its longer term success might depend on how successfully the issue of privacy concerns is addressed[5]. Threat to privacy doesn’t come as a pre-planned intention, but is a result of inherent characteristics present in new technologies. However, there are views saying that technologies of smart things and ubiquitous computing are violent, pervasive and can turn things into surveillance objects[6].

People might become hesitant in accepting such technologies, if they feel their privacy is threatened[7]. Couple of main sources of privacy risk are being distinguished in the environment of the Internet of Things.

An unprecedented level of data sharing

The vision of Internet of Things includes a notion of smart objects which will be present everywhere. They could include things in our pockets or be integrated into our home and work environment. Sensors might exist in many physical objects people regularly pass by. As the number of smart objects increases, the amount of

[1] Atzori, Luigi, Antonio Iera, and Giacomo Morabito. "The internet of things: A survey." Computer networks 54.15 (2010): 2787-2805.

[2] De Hert, Paul, et al. "Legal safeguards for privacy and data protection in ambient intelligence." Personal and ubiquitous computing 13.6 (2009): 435-444.

[3] Maner, Walter. "Unique ethical problems in information technology." Science and Engineering Ethics 2.2 (1996): 137-154.

[4]Atzori, Luigi, Antonio Iera, and Giacomo Morabito. "The internet of things: A survey." Computer networks 54.15 (2010): 2787-2805.

[5] Hong, Jason I., et al. "Privacy risk models for designing privacy-sensitive ubiquitous computing systems." Proceedings of the 5th conference on Designing interactive systems: processes, practices, methods, and techniques. ACM, 2004.

[6] Araya, Agustin A. "Questioning ubiquitous computing." Proceedings of the 1995 ACM 23rd annual conference on Computer science. ACM, 1995.

[7] Atzori, Luigi, Antonio Iera, and Giacomo Morabito. "The internet of things: A survey." Computer networks 54.15 (2010): 2787-2805.

data being stored, shared and mined will keep rising like never before. Consequently, there will be a lot more opportunities for data to be compromised[8].

Data Mining and Profiling

The presence of tremendous and constantly increasing amount of data brings new risks, even if such data is completely anonymized. Publicly available and unprotected data can be mined and analysed through the use of special algorithms revealing patterns and sensitive personal information. For example, it has been shown that mining data about energy consumption can expose in-home activities, like sleep cycles, usage of appliances and more, which can be abused by criminals or marketers[9]. It doesn't even help if such data is anonymized because de-anonymizing techniques can be used to re-identify people[10].

Big Data and Analytics

The previously unimaginable amount of data is recognized as a great business opportunity[11]. Businesses and companies can use all available data to make better strategic decisions and further adjust their products and services toward customer needs. Such activities not only help improve profits and growth, but are beneficial for the customers as well. For example, data can be used to provide customers with recommendations which increase their overall contentment[12] or provide them with a more valuable personalized experience[13]. On the other side, it has already been remarked that such practices convey significant legal and ethical problems[14].

Unauthorized Access/Security

Data security is one more urgent issue which causes worries. As physical objects integrated into Internet of Things are often left unattended, and as their number increases the likelihood of unauthorized use is also growing[15]. Eavesdropping is easier in wireless communications. Communication between different objects might be intercepted and altered for unethical use[16]. Moreover, such data is likely to be standardized, as that is necessary for deriving the highest possible benefits of Internet of Things. Such standards are still being developed, but it can be argued that standardization imposes greater risk to security, as standardized data is easier to capture.

[8] Vermesan, Ovidiu, et al. "Internet of things strategic research roadmap."Internet of Things-Global Technological and Societal Trends (2011): 9-52.

[9] Lisovich, Mikhail A., Deirdre K. Mulligan, and Stephen B. Wicker. "Inferring personal information from demand-response systems." Security & Privacy, IEEE 8.1 (2010): 11-20.

[10] Narayanan, Arvind, and Vitaly Shmatikov. "De-anonymizing social networks."Security and Privacy, 2009 30th IEEE Symposium on. IEEE, 2009.

[11] Chen, Hsinchun, Roger HL Chiang, and Veda C. Storey. "Business Intelligence and Analytics: From Big Data to Big Impact." MIS quarterly 36.4 (2012): 1165-1188.

[12] Ricci, Francesco, Lior Rokach, and Bracha Shapira. Introduction to recommender systems handbook. Springer US, 2011.

[13] Eirinaki, Magdalini, and Michalis Vazirgiannis. "Web mining for web personalization." ACM Transactions on Internet Technology (TOIT) 3.1 (2003): 1-27.

[14] Caudill, Eve M., and Patrick E. Murphy. "Consumer online privacy: legal and ethical issues." Journal of Public Policy & Marketing 19.1 (2000): 7-19.

[15] Atzori, Luigi, Antonio Iera, and Giacomo Morabito. "The internet of things: A survey." Computer networks 54.15 (2010): 2787-2805.

[16] Atzori, Luigi, Antonio Iera, and Giacomo Morabito. "The internet of things: A survey." Computer networks 54.15 (2010): 2787-2805.

Technological Uncertainty

The cost of storing data keeps decreasing which means that such data might be stored somewhere on servers for indefinite time[17]. That carries further challenges as ttechnologies constantly keep changing. It is hard to predict what comes next and for that reason, there is a certain level of uncertainty in dealing with data. The current level of protection might make all data on server safe, but next year new procedures might be developed, which would manage to break the current security protection. When companies get approval for using data for a specified purpose, it would be hard to maintain the promise in the presence of high uncertainty.

Bounded rationality as an obstacle for informed consent

In dealing with privacy of data shared with different services, it is often assumed that the ethical approach involves letting users know what data is being collected by the service and asking them to agree on that[18]. If users are not fully informed about such practices they simply need to be educated and ways of opting out from data collection procedures should be provided[19]. Similar scenario is being suggested for the use of RFID tags in smart objects. Users could specify their own privacy policies for all RFID tags, choose how to use them, disable or send them into the sleep mode[20][21].

However, such practices might be shown to be ineffective as it has been found that when making privacy related decisions people are not behaving rationally, as it is often assumed[22]. People report being concerned about their privacy, but keep behaving completely opposite[23]. Furthermore, some research has shown that user decisions of whether to share their data or not is highly sensitive to how question itself is framed[24].

Such behavior can be explained by the notion of bounded rationality. Concept of bounded rationality has been popularized and empirically investigated with the rise of behavioral economics, and it encompasses the notion that individuals are limited when making decisions by their computational power, cognitive bias, information and time[25][26]. Some authors have already argued that it might be the cause of unethical behavior in general decision making[27].

The importance of the concept of bounded rationality lies in the fact that it prevents informed consent, which is extremely important in ethical practices. Not only from a legal point of view, but also from ethical and moral one as well, it is a necessary condition to be fulfilled in situation when users are being asked to share their data

[17] Atzori, Luigi, Antonio Iera, and Giacomo Morabito. "The internet of things: A survey." Computer networks 54.15 (2010): 2787-2805.

[18] Milne, George R. "Privacy and ethical issues in database/interactive marketing and public policy: a research framework and overview of the special issue."Journal of Public Policy & Marketing 19.1 (2000): 1-6.

[19] Nowak, Glen J., and Joseph Phelps. "Understanding privacy concerns. An assessment of consumers' information-related knowledge and beliefs." Journal of Direct Marketing 6.4 (1992): 28-39.

[20] Molnar, David, Andrea Soppera, and David Wagner. "Privacy for RFID through trusted computing." Proceedings of the 2005 ACM workshop on Privacy in the electronic society. ACM, 2005.

[21] Juels, Ari. "RFID security and privacy: A research survey." Selected Areas in Communications, IEEE Journal on 24.2 (2006): 381-394.

[22] Acquisti, Alessandro, and Jens Grossklags. "Privacy and rationality in individual decision making." IEEE Security & Privacy 2 (2005): 24-30.

[23] Berendt, Bettina, Oliver Günther, and Sarah Spiekermann. "Privacy in e-commerce: stated preferences vs. actual behavior." Communications of the ACM 48.4 (2005): 101-106.

[24] Bellman, Steven, Eric J. Johnson, and Gerald L. Lohse. "On site: to opt-in or opt-out?: it depends on the question." Communications of the ACM 44.2 (2001): 25-27.

[25] Simon, Herbert Alexander. Models of bounded rationality: Empirically grounded economic reason. Vol. 3. MIT press, 1982.

[26] Kahneman, Daniel. "Maps of bounded rationality: Psychology for behavioral economics." American economic review (2003): 1449-1475.

[27] Palazzo, Guido, Franciska Krings, and Ulrich Hoffrage. "Ethical blindness." Journal of business ethics 109.3 (2012): 323-338.

with services and companies. If informed consent cannot be guaranteed, that undoubtedly creates an urgent ethical dilemma because such data can be misused with significant negative consequences for the individual and even the whole society. For attaining informed consent one needs to fulfill criteria of full disclosure, comprehension, competence, voluntarity and agreement[28]. That is not always the case in digital environment and indeed, the existence of informed consent for users of privacy-challenging technologies has already been challenged[29].

What are the main observed characteristics of human psyche which prevent users from behaving rationally?

Cognitive and Time Limits

From the point of common sense, it is simply reasonable to assume that users won't have enough time to read and contemplate on all available privacy policies and practices. Such behaviour is already observed in the context of internet privacy policies, as large number of users simply do not read them[30]. In the environment of Internet of Things, each of the smart things could have its own privacy policy or terms of use, but expecting that each of them will be thoroughly analysed before acceptance of use is unrealistic. Moreover, privacy policies can contain legal jargon, which is simply hard to understand[31]. Additionally, ordinary internet users are reported to have problems understanding common computer and Internet terms, their own behaviour or valuations[32]. As the concept of Internet of Things is even more complex such misunderstandings could only be more emphasized in the future. The percentage of users who would have troubles understanding what smart objects are doing and how can data be shared will without a doubt be significantly higher.

Hyperbolic Discounting and Self-Control

Even privacy concerned individuals are found to share their data for negligible benefit[33]. Human decision making is often automatic, and when individuals are faces with a trade-off of choosing between short term conveniences versus costs of reduced privacy in long term, they choose the convenience[34]. Such behaviour could be explained with a phenomenon of hyperbolic discounting, when individuals put a very low value on future reduced privacy costs at the current moment, but change that evaluation in the future[35]. It is also closely connected with the problem of self-control and impulsive behaviour which are well-known features of human psyche[36]. Given that human privacy preferences are not stable and time consistent, such behaviour might be problematic for service designer, because even if users have now accepted data sharing with smart things,

[28] Millett, Lynette I., Batya Friedman, and Edward Felten. "Cookies and web browser design: toward realizing informed consent online." Proceedings of the SIGCHI conference on Human factors in computing systems. ACM, 2001.

[29] Jensen, Carlos, Colin Potts, and Christian Jensen. "Privacy practices of Internet users: self-reports versus observed behavior." International Journal of Human-Computer Studies 63.1 (2005): 203-227.

[30] Jensen, Carlos, Colin Potts, and Christian Jensen. "Privacy practices of Internet users: self-reports versus observed behavior." International Journal of Human-Computer Studies 63.1 (2005): 203-227.

[31] Pollach, Irene. "A typology of communicative strategies in online privacy policies: Ethics, power and informed consent." Journal of Business Ethics 62.3 (2005): 221-235.

[32] Jensen, Carlos, Colin Potts, and Christian Jensen. "Privacy practices of Internet users: self-reports versus observed behavior." International Journal of Human-Computer Studies 63.1 (2005): 203-227.

[33] Spiekermann, Sarah, Jens Grossklags, and Bettina Berendt. "E-privacy in 2nd generation E-commerce: privacy preferences versus actual behavior." Proceedings of the 3rd ACM conference on Electronic Commerce. ACM, 2001.

[34] Acquisti, Alessandro. "Privacy in electronic commerce and the economics of immediate gratification." Proceedings of the 5th ACM conference on Electronic commerce. ACM, 2004.

[35] Acquisti, Alessandro, and Jens Grossklags. "Losses, gains, and hyperbolic discounting: An experimental approach to information security attitudes and behavior." 2nd Annual Workshop on Economics and Information Security-WEIS. Vol. 3. 2003.

[36] Baumeister, Roy F. "Yielding to temptation: Self-control failure, impulsive purchasing, and consumer behavior." Journal of Consumer Research 28.4 (2002): 670-676.

they can easily change their mind as time passes. Given that possible privacy risks are far greater in Internet of Things, we could argue that such future privacy costs might be even higher; causing outcry by users who have previously accepted such costs in exchange for short term convenience.

Status Quo Bias

Status quo bias describes the human propensity to prefer the current state of the things. Such cognitive bias affects decision in adjusting software or services default settings. Each piece of software or a service usually comes with a set of predefined settings, which are rarely being changed, even if they interfere with stated user preference[37]. Same is valid for privacy settings, which are seldom being changed[38]. Humans simply prefer the status quo situation.

Illusion of Control

An additional paradoxical phenomenon which has been observed in the context of privacy protection techniques is the control paradox. It explains type of behaviour when a mere feeling that individuals have control over publication of their data, makes them more inclined to disclose personal data, increasing the overall objective risk[39].

Proposed solutions

Future scenario of the Internet of Things involves a vision of intelligent and smart objects and surfaces which can communicate in the background completely unnoticeably. At the same time, we have shown human beings are rationally bounded and unable to fully contemplate or control what is happening. Such a combination can have multiple unforeseen and dangerous consequences. Moral goals need to consider the complete nature of human beings[40].

The need for addressing this challenge is even more emphasized if we have in mind that information technology's designers themselves aren't interested in ethical consequences of their technologies[41]. Usually, the ethical worries appear as an ex-post problem. And even in such situations, as service designers are humans themselves, they might fail to view the ethical challenge or can find excuses for it[42]. Organizational structure can also hinder ethicality[43].

The discussion of dealing with the problem of privacy in the surrounding of humans and increasingly smarter things is ongoing. Currently proposed approaches of better authentication or encryption or increasing the

[37] Smith, N. Craig, Daniel G. Goldstein, and Eric J. Johnson. "Choice without awareness: ethical and policy implications of defaults." Journal of Public Policy & Marketing 32.2 (2013): 159-172.

[38] Gross, Ralph, and Alessandro Acquisti. "Information revelation and privacy in online social networks." Proceedings of the 2005 ACM workshop on Privacy in the electronic society. ACM, 2005.

[39] Brandimarte, Laura, Alessandro Acquisti, and George Loewenstein. "Misplaced confidences privacy and the control paradox." Social Psychological and Personality Science 4.3 (2013): 340-347.

[40] Gigerenzer, Gerd. "Moral satisficing: Rethinking moral behavior as bounded rationality." Topics in cognitive science 2.3 (2010): 528-554.

[41] Wakunuma, Kutoma J., and Bernd Carsten Stahl. "Tomorrow's ethics and today's response: An investigation into the ways information systems professionals perceive and address emerging ethical issues." Information Systems Frontiers (2014): 1-15.

[42] Tenbrunsel, Ann E., and David M. Messick. "Ethical fading: The role of self-deception in unethical behavior." Social Justice Research 17.2 (2004): 223-236.

[43] Kish-Gephart, Jennifer J., David A. Harrison, and Linda Klebe Treviño. "Bad apples, bad cases, and bad barrels: meta-analytic evidence about sources of unethical decisions at work." Journal of Applied Psychology 95.1 (2010): 1.

amount of control of users over their data[44] are not enough. There are also approaches suggesting the use of having privacy assistants directly incorporated into the software, which will warn users every time they are sharing sensitive information[45].

One potentially promising approach to addressing privacy concerns is the concept of privacy by design. Privacy by design is a term coined by Ann Chavoukin, Canadian privacy expert in 1997[46]. It encompasses a notion that all technologies with privacy-intrusive potential are required to provide maximum possible privacy settings by default, and such principle has to be respected from the first day of software design. Privacy by design principles could be especially important in the environment of ubiquitous computing, given its pervasivity and gravity of possible consequences[47]. We can argue that it would basically involve a paternalistic approach, which would mean the maximum achievable benefit for users, without asking for their approval. Paternalism has already been suggested as a solution for dealing with privacy-invasive technologies[48].

However, it is highly probable that companies will hesitate to implement such principles into their own systems, for the reason of high cost and loss of profit. In such case adequate legislation is needed[49], maybe even on international level[50].

References

Ackerman, Mark S., and Lorrie Cranor. "Privacy critics: UI components to safeguard users' privacy." CHI'99 Extended Abstracts on Human Factors in Computing Systems. ACM, 1999.

Acquisti, Alessandro, and Jens Grossklags. "Losses, gains, and hyperbolic discounting: An experimental approach to information security attitudes and behavior." 2nd Annual Workshop on Economics and Information Security-WEIS. Vol. 3. 2003.

Acquisti, Alessandro, and Jens Grossklags. "Privacy and rationality in individual decision making." IEEE Security & Privacy 2 (2005): 24-30.

Acquisti, Alessandro. "Privacy in electronic commerce and the economics of immediate gratification." Proceedings of the 5th ACM conference on Electronic commerce. ACM, 2004.

Araya, Agustin A. "Questioning ubiquitous computing." Proceedings of the 1995 ACM 23rd annual conference on Computer science. ACM, 1995.

Atzori, Luigi, Antonio Iera, and Giacomo Morabito. "The internet of things: A survey." Computer networks 54.15 (2010): 2787-2805.

Baumeister, Roy F. "Yielding to temptation: Self-control failure, impulsive purchasing, and consumer behavior." Journal of Consumer Research 28.4 (2002): 670-676.

Bellman, Steven, Eric J. Johnson, and Gerald L. Lohse. "On site: to opt-in or opt-out?: it depends on the question." Communications of the ACM 44.2 (2001): 25-27.

Berendt, Bettina, Oliver Günther, and Sarah Spiekermann. "Privacy in e-commerce: stated preferences vs. actual behavior." Communications of the ACM 48.4 (2005): 101-106.

[44] Atzori, Luigi, Antonio Iera, and Giacomo Morabito. "The internet of things: A survey." Computer networks 54.15 (2010): 2787-2805.

[45] Ackerman, Mark S., and Lorrie Cranor. "Privacy critics: UI components to safeguard users' privacy." CHI'99 Extended Abstracts on Human Factors in Computing Systems. ACM, 1999.

[46] Cavoukian, Ann. "Privacy by design." Take the Challenge. Information and Privacy Commissioner of Ontario, Canada (2009).

[47] Langheinrich, Marc. "Privacy by design—principles of privacy-aware ubiquitous systems." Ubicomp 2001: Ubiquitous Computing. Springer Berlin Heidelberg, 2001.

[48] Smith, N. Craig, Daniel G. Goldstein, and Eric J. Johnson. "Choice without awareness: ethical and policy implications of defaults." Journal of Public Policy & Marketing 32.2 (2013): 159-172.

[49] Langheinrich, Marc. "A survey of RFID privacy approaches." Personal and Ubiquitous Computing 13.6 (2009): 413-421.

[50] Weber, Rolf H. "Internet of Things–New security and privacy challenges."Computer Law & Security Review 26.1 (2010): 23-30.

Brandimarte, Laura, Alessandro Acquisti, and George Loewenstein. "Misplaced confidences privacy and the control paradox." Social Psychological and Personality Science 4.3 (2013): 340-347.

Caudill, Eve M., and Patrick E. Murphy. "Consumer online privacy: legal and ethical issues." Journal of Public Policy & Marketing 19.1 (2000): 7-19.

Cavoukian, Ann. "Privacy by design." Take the Challenge. Information and Privacy Commissioner of Ontario, Canada (2009).

Chen, Hsinchun, Roger HL Chiang, and Veda C. Storey. "Business Intelligence and Analytics: From Big Data to Big Impact." MIS quarterly 36.4 (2012): 1165-1188.

De Hert, Paul, et al. "Legal safeguards for privacy and data protection in ambient intelligence." Personal and ubiquitous computing 13.6 (2009): 435-444.

Eirinaki, Magdalini, and Michalis Vazirgiannis. "Web mining for web personalization." ACM Transactions on Internet Technology (TOIT) 3.1 (2003): 1-27.

Gigerenzer, Gerd. "Moral satisficing: Rethinking moral behavior as bounded rationality." Topics in cognitive science 2.3 (2010): 528-554.

Gross, Ralph, and Alessandro Acquisti. "Information revelation and privacy in online social networks." Proceedings of the 2005 ACM workshop on Privacy in the electronic society. ACM, 2005.

Hong, Jason I., et al. "Privacy risk models for designing privacy-sensitive ubiquitous computing systems." Proceedings of the 5th conference on Designing interactive systems: processes, practices, methods, and techniques. ACM, 2004.

Jensen, Carlos, Colin Potts, and Christian Jensen. "Privacy practices of Internet users: self-reports versus observed behavior." International Journal of Human-Computer Studies 63.1 (2005): 203-227.

Juels, Ari. "RFID security and privacy: A research survey." Selected Areas in Communications, IEEE Journal on 24.2 (2006): 381-394.

Kahneman, Daniel. "Maps of bounded rationality: Psychology for behavioral economics." American economic review (2003): 1449-1475.

Kish-Gephart, Jennifer J., David A. Harrison, and Linda Klebe Treviño. "Bad apples, bad cases, and bad barrels: meta-analytic evidence about sources of unethical decisions at work." Journal of Applied Psychology 95.1 (2010): 1.

Langheinrich, Marc. "A survey of RFID privacy approaches." Personal and Ubiquitous Computing 13.6 (2009): 413-421.

Langheinrich, Marc. "Privacy by design—principles of privacy-aware ubiquitous systems." Ubicomp 2001: Ubiquitous Computing. Springer Berlin Heidelberg, 2001.

Lisovich, Mikhail A., Deirdre K. Mulligan, and Stephen B. Wicker. "Inferring personal information from demand-response systems." Security & Privacy, IEEE 8.1 (2010): 11-20.

Maner, Walter. "Unique ethical problems in information technology." Science and Engineering Ethics 2.2 (1996): 137-154.

Millett, Lynette I., Batya Friedman, and Edward Felten. "Cookies and web browser design: toward realizing informed consent online." Proceedings of the SIGCHI conference on Human factors in computing systems. ACM, 2001.

Milne, George R. "Privacy and ethical issues in database/interactive marketing and public policy: a research framework and overview of the special issue."Journal of Public Policy & Marketing 19.1 (2000): 1-6.

Molnar, David, Andrea Soppera, and David Wagner. "Privacy for RFID through trusted computing." Proceedings of the 2005 ACM workshop on Privacy in the electronic society. ACM, 2005.

Narayanan, Arvind, and Vitaly Shmatikov. "De-anonymizing social networks."Security and Privacy, 2009 30th IEEE Symposium on. IEEE, 2009.

Nowak, Glen J., and Joseph Phelps. "Understanding privacy concerns. An assessment of consumers' information-related knowledge and beliefs." Journal of Direct Marketing 6.4 (1992): 28-39.

Palazzo, Guido, Franciska Krings, and Ulrich Hoffrage. "Ethical blindness." Journal of business ethics 109.3 (2012): 323-338.

Pollach, Irene. "A typology of communicative strategies in online privacy policies: Ethics, power and informed consent." Journal of Business Ethics 62.3 (2005): 221-235.

Ricci, Francesco, Lior Rokach, and Bracha Shapira. Introduction to recommender systems handbook. Springer US, 2011.

Simon, Herbert Alexander. Models of bounded rationality: Empirically grounded economic reason. Vol. 3. MIT press, 1982.

Smith, N. Craig, Daniel G. Goldstein, and Eric J. Johnson. "Choice without awareness: ethical and policy implications of defaults." Journal of Public Policy & Marketing 32.2 (2013): 159-172.

Spiekermann, Sarah, Jens Grossklags, and Bettina Berendt. "E-privacy in 2nd generation E-commerce: privacy preferences versus actual behavior." Proceedings of the 3rd ACM conference on Electronic Commerce. ACM, 2001.

Tenbrunsel, Ann E., and David M. Messick. "Ethical fading: The role of self-deception in unethical behavior." Social Justice Research 17.2 (2004): 223-236.

Vermesan, Ovidiu, et al. "Internet of things strategic research roadmap."Internet of Things-Global Technological and Societal Trends (2011): 9-52.

Wakunuma, Kutoma J., and Bernd Carsten Stahl. "Tomorrow's ethics and today's response: An investigation into the ways information systems professionals perceive and address emerging ethical issues." Information Systems Frontiers (2014): 1-15.

Weber, Rolf H. "Internet of Things–New security and privacy challenges. "Computer Law & Security Review 26.1 (2010): 23-30.