Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2010 Proceedings

Americas Conference on Information Systems (AMCIS)

8-2010

Approaching the value of Privacy: Review of theoretical privacy concepts and aspects of privacy management

Ulrike Hugl
University of Innsbruck, ulrike.hugl@uibk.ac.at

Approaching the value of Privacy: Review of theoretical privacy concepts and aspects of privacy management

Ulrike Hugl
University of Innsbruck, Innsbruck School of Management
ulrike.hugl@uibk.ac.at

ABSTRACT

Privacy has become a common discussed issue involving technological, social, ethical, economic and political complexity. This paper reviews the current state of privacy concepts and theories reflecting scholarly work of diverse disciplines. It argues that in an environment of new technologies and surveillance opportunities with an increased potential of ubiquitous data collection and data combination, traditional privacy theories fall short in mainly concentrating on one single aspect of privacy. Hence, beside a presentation of general theoretical privacy aspects, this paper highlights existing 'multidimensional' privacy approaches considering responses to specific (technological) situations in different contexts. Finally, drawing on a more pragmatic and practical level, diverse short snapshots of concrete privacy management approaches, focusing on an individual, project oriented, organizational as well as legal and governmental level, are presented.

Keywords

Privacy theories, new technologies, multidimensional privacy approach, privacy management.

INTRODUCTION

In 2007, Privacy International (PI) as a British human rights group - founded in 1990 as a watchdog on surveillance and privacy invasions by governments and corporations published - a report measuring the extent of surveillance and privacy tendencies of 47 countries in the EU and the world. The key findings reflect an increased surveillance and declining performance on privacy safeguards. In detail, the results show that more and more governments try to collect data on communication, geographic and financial records of their citizens; a profitable surveillance industry emerged, dominated on the one hand by the creation of diverse international treaties that often operate outside judicial or democratic processes and on the other hand by global IT companies; surveillance initiated by the European Union caused a substantial decline in privacy across Europe; Germany slipped significantly, dropping from first to seventh place in Europe; the US is still the worst ranked country in the democratic world; and the highest ranked countries are Canada, Romania and Greece – the lowest continue to be China, Malaysia and Russia. (PI, 2007)

Based on this report, "the extent of surveillance over the lives of many people has […] reached an unprecedented level. Conversely, laws that ostensibly protect privacy and freedoms are frequently flawed – riddled with exceptions and exceptions that can allow government a free hand to intrude on private life" (PI, 2007). At the same time, technological developments, the globalization and especially increased interoperability between information systems have created pressure on several remaining privacy safeguards.

Since the beginning of the information age privacy has become a common discussed issue. The term privacy is used in philosophical, sociological, ethical, political, legal and the economic-oriented debate, but yet there exists no single 'entire' analysis, meaning or definition. For a huge spectrum of vital economic and social activities, "personal data have become an indispensable 'raw material'. For countless governmental and private organizations, crucial products, services, performances, and responsibilities require finely calculated use of data on the person concerned" (Rule, 2004). Existing technologies with potential and impact on privacy issues refer for example to video (CCTV) and online surveillance, data profiling, workplace monitoring, biometric identification, radio frequency identification, and global positioning system (GPS). In the scientific debate, scholars deal with privacy topics from the background of diverse fields - among others in marketing, e-health, artificial intelligence (AI), pervasive computing, social networks and e-government.

In information systems research an interdisciplinary background of dealing with privacy can be classified in the field of a philosophical perspective of interpretive research tradition, focusing on a broader "understanding of the context of the information system" (Walsham, 1993), and at the same time aiming on the complexity of human sense making, "concerned with the subjective understanding that individuals ascribe to their social situations" (Dhillon and Backhouse, 2001). Hence, beside the above-mentioned other disciplines dealing with privacy issues, "the information systems literature also has long recognised the threat posed to individual privacy by technological systems" (Carew, Stapleton and Byrne, 2008).

After this introduction, the next chapter highlights diverse privacy concepts and theories, presents aspects of privacy related to new technologies and reports scholarly work towards a more contemporary 'multidimensional' and 'cluster' conceptualization of privacy. In a next section, starting points for managing privacy from a practical point of view will be presented. Finally, the paper concludes with some recapitulating remarks.

CONCEPTUALIZING PRIVACY

Seen from a historical perspective, the concept of privacy grounds on philosophical discussions, mainly referring to Aristotle's differentiation between the private sphere of a person regarding his/her domestic and family life and the public sphere (the polis) of political activity. As time passed and mainly based on new technological developments, several new efforts and 'concepts of privacy' have been developed.

Approaching the concept of privacy involves technological, social, ethical, economic and political complexity. Solove (2008) states: "Currently, privacy is a sweeping concept, encompassing (among other things) freedom of thought, control over one's body, solitude in one's home, control over personal information, freedom from surveillance, protection of one's reputation, and protection from searches and interrogations." For Järvinen (2009), "privacy seems to be something of very great importance and something vital to defend, but also a matter of individual preference and culturally relative."

Privacy and technology

In 1890, Warren and Brandeis (1890) referred as one of the first to an increasing use of new technologies in those days. From a juristically background they expressed their concerns regarding widely distributed newspapers (sensational journalism) and possible reproductions of photographs and argued that "recent inventions and business methods call attention […] for the protection of the person, and for securing to the individual […]" (Warren et al., 1890). Their widely cited definition of privacy as "the right to be let alone" seems to be a poor interpretation of their intention: they argue this statement in connection with the claim to protect the privacy of one's "thoughts, emotions, and sensations". In a more broader meaning, "privacy rights are therefore one aspect of a broader interest in being left alone, which in turn finds its justification in an individual's inviolate personality" (Austin, 2003).

Nowadays, based on recent developments we have to deal with much more comprehensive technological opportunities. Solove (2008) notes some examples of activities typically related to privacy breaches: new X-ray devices can see through people's clothing, amounting to what some call a 'virtual strip-search'; the government uses a thermal sensor device to detect heat patterns in a person's home. Some other examples: A malicious insider sells a CD-Rom with customers' sensitive data; employees at a hospital access to diagnostic data via the patients' information system to spy out colleagues; a German telecommunication company monitors systematically communication connection data of managers and boards of directors. In general, there exist current tendencies to combine Internet records, DNA databases, medical diagnosis, geo-marketing and financial data (e.g. credit histories) etc. Based on such new opportunities of pervasive data combination, the ability for others to link and access databases increases and the ability of persons' control over information about themselves decreases and seems to be more difficult than ever before.

From the viewpoint of such transparency, back to the 1990ies some scholars claimed the 'death of privacy', arguing that privacy is no longer relevant and "our personal privacy may gradually be coming to an end" (Spinello, 1997). "You have zero privacy anyway. Get over it." This statement was brought up by Scott McNeally, chief executive officer of Sun Microsystems at a conference in 1999, in the course of an unveiling of his company's latest software Jini enabling the networking of a wide variety of devices. Based on widely known statements like the one from McNeally, but also based on legal and policy based governmental activities, authors discussed the 'destruction', 'total surveillance' and the 'end of privacy' (Brin, 1998; Etzioni, 2000; Garfinkel and Russel, 2000; Rosen, 2000; Sykes, 1999; Whitaker, 1999). Scholars deal with privacy in an environment that, based on the potential of new technologies, more and more allows comprehensive digital data pooling about persons to be (often in real time) queried and compiled. Mainly based on the work of Etzioni (2000) and Brin (1998), Langheinrich (2001) outlines several arguments and issues stated by these authors:

- Feasibility: What can technology in the best case prevent or achieve? Legal privacy regulations require enforceability. If privacy disregards are not verifiable, accountability becomes problematic.

- Convenience: In many cases benefits of a free flow of information exceed the personal risks. It is argued that only highly sensitive information might be worth protected – other data like preferences, shopping habits, contact and even health information might better be publicly known with the intention to get best services and protection possible.
- Communitarian: The 'greater good of society' needs to overrule personal privacy needs. Therefore, democratic societies may appoint trusted entities to monitor specific private matters and to improve life for the majority.
- Egalitarian: Because everyone has access to the same information the danger of misuse of a few well-informed may be downsized. The motto: Watchers have to be watched and information others hold over me is equally worth the information I hold about them.

A critical view on the mentioned assessments shows that nowadays - ten years after their creation - data collection possibilities as well as the potential of misuse in the field of privacy violations have increased; threats are widely spread and publicly communicated in media. Let me give one example from information systems security research: The current market downturn and possibly a difficult financial and 'emotional' situation of employees and managers (e.g. fear of dismissal, uncertain or existence-threatening situation of the employing organization etc.) may increase the potential and liability of malicious insider opportunities and acts and lead to expanded organization vulnerabilities. Specific studies from KPMG (2010), the Global Fraud Report of Kroll (www.kroll.com) and the latest CSI Computer Crime and Security Survey (Peters, 2009) may support such an estimation.

I agree with Langheinrich's (2001) critical review regarding the above-mentioned issues of Etzioni (2000) and Brin (1998). Especially from the background of ubiquitous systems he brings up some important questions (Langheinrich, 2001): "Just where are the borders of technical feasibility when it comes to protecting our personal information? Just how much of our personal data should we be allowed to give up? How are we to weight the greater good of society against our personal protection, and whom are we trusting with such sensitive issues? And […] how can we influence what will and what will not constitute acceptable social behavior in the future by designing our systems in a certain way that supports such behavior?"

Lessig (2000) refers to the requirement of free decisions of people what to do with their lives connected with their beliefs and interests and without fear of consequences and repression from others with the aim to ensure plurality of attitudes and ideas in a society. Based on Lessig's work, Langheinrich et al. (2005) identify several aspects of privacy related to new technologies and especially ICT:

- Privacy as empowerment: Regarding an informational aspect of privacy individuals should have the power to control and monitor the distribution of their personal data.
- Privacy as utility: Privacy can be seen as a utility giving more or less protection against abuses (following the privacy definition 'the right to be left alone').
- Privacy as dignity: This aspect of privacy focuses on unsubstantiated suspicion and equilibrium of information available between two individuals.
- Privacy as a regulating agent: Privacy regulations, laws and moral norms help to balance and keep in check the powers of the decision-making elite.

Meaning and value of Privacy

In his recent article 'Privacy, privacies and basic needs' Hayden Ramsay (2010) identifies from a philosophical point of view five forms of privacy and analyses them in their vary in moral significance. The first meaning of privacy refers to 'control over the flow of information'. For him, the basis of this privacy is far from clear. His two main arguments: First, "freedom and individuality are not the most important considerations in personal or social life"; there exist others, for example commitment to truthfulness, a rich inner life, and practical wisdom. And: "Thus even if loss of control over personal information does decrease freedom and individuality, it does not automatically follow that lack of privacy in this meaning is always a morally serious matter" (Ramsay, 2010). Second, privacy clearly means more than controlling information. If someone believes he or she is being spied upon, this person may have concerns about an invasion of privacy. But Ramsay (2010) argues regarding such a case: "'Back off!' does not indicate fear of loss of control over data, but anger at being observed and invaded, resentment at being shown no respect and not being permitted to be alone."

The second meaning of privacy is 'freedom from interference and observation' refers to a debate asking what contact is invasive, unreasonable or avoidable. Here a majority of writers argue with personal autonomy, generally understood as a retaining and developing control over one's choices and life. Ramsay (2010) highlights two critical arguments: "We might, for example, spy on someone to protect their own autonomy (perhaps from terrorists […]), or to protect the autonomy of all: spying as a servant and not a betrayal of autonomy. […] If autonomy is control, and privacy violations do not always threaten control, then the wrong of privacy violation cannot always be explained as undermining autonomy. […] But surely violations of privacy that leave autonomy unaffected can still be morally serious. In fact, the threat of loss of autonomy does not adequately explain the meaning of violation and danger people experience with the most serious attacks on their privacy."

The 'maintenance of a sphere of inviolability around each person' constitutes the third meaning of privacy: "People are to be regarded as selves – as centres of awareness and interests who merit such interpersonal attitudes as recognition, respect, reverence and apology in our dealings with them"; in this meaning, privacy is seen as a substantial moral good: "unlike control of data or increase of liberty, it is a human good intimately connected to the concerns and status of the person and to the special form of value enjoyed by all persons. This helps to explain why privacy matters so much, even for people who do not much care about their personal information or their autonomy: invasion of privacy is invasion of the person, lack of respect for the value of persons." (Ramsay, 2010) As fourth meaning of privacy Ramsay's highlights 'our need for solitude' referring to the time to be by oneself, to rest, to think, to do so sincerely and honestly until the time comes to resume social life. And: domesticity as fifth meaning of privacy, asking for safety from observation and intrusion.

To summarize, privacy is a 'complex concept': within our generic need for privacy the five meanings have to be considered with their structural interrelations. "Thus the need to limit access to information is closely linked to our needs for freedom from interference, personal inviolability, solitude and a tranquil domesticity: in contemporary society where information systems are closely inter-linked data can easily slip away and as it does so threaten liberty, security, personal space and home life. […] the various elements of the concept of privacy suggested are most fully explained by citing their relations to each other: the generic need for privacy holds together as a single concept through the inter-relationship of its parts." (Ramsay, 2010) In this meaning, privacy is seen as human right, as common good (including control, inviolability, solitude, domesticity and freedom) required by individuals to achieve our well-being.

Daniel J. Solove's (2002) scholarly work as professor of law at the George Washington University Law School brings another point of view into attention, namely a combination of a philosophical and juridical resp. law-oriented background. He takes as a starting point a categorization and discussion of six widely known traditional privacy concepts—'the right to be let alone' (Warren et al., 1890), 'limited access to the self', 'secrecy', 'control of personal information', 'personhood' (individuality, dignity, autonomy and antitotalitarianism), and 'intimacy'. Subsequently, hereafter he refers to so-called 'clusters of privacy claims' (clustering together certain of the conceptions instead of considering only one single conception) and finally develops a 'pragmatic approach' outside from the mentioned other categorizations. In their philosophical analysis of privacy, Randy Kemp and Adam D. Moore (2007) the six privacy concepts of Solove (2002) are taken up and further analyzed, also including 'privacy as cluster concept'.—Instead of a detailed analysis of the above-mentioned stand-alone conceptions, I will focus in the following on approaches and thoughts which in my opinion are of feasible interest: first, the 'cluster concept', and second, Solove's (2002) 'pragmatic privacy approach', specifically concentrating on technology-related issues.

Privacy as cluster concept

For Austin (2003) "technology creates privacy issues that appear to fall outside the bounds of our traditional analysis […] we do need to sharpen and deepen our understanding of traditional concerns regarding privacy in order to respond to these new situations." A similar statement is brought by Solove (2004). Burgoon et al. (1989) claim for a multidimensional approach and define privacy as "the ability to control and limit physical, interactional, psychological and informational access to one's group or to the self". The physical dimension refers to how physically accessible an individual is to others. The psychological dimension relates to an individual's right with whom she or he shares personal information as well as the control of affective/cognitive inputs or outputs (e.g. non-verbal communication). The social dimension means the ability to control social interactions (controlling distance between persons). The informational privacy dimension refers to an individual's right to reveal personal information to others (not always under an individual's control). In a very early multidimensional approach, Laufer and Wolfe (1977) highlight three major elements of situations that have to be considered to understand a person's perception, invasions of privacy and experience of privacy: self-ego dimensions (individuals vary in their degrees of privacy concerns based on personal experiences), the environmental dimension (environmental elements may influence a person's ability to have, perceive and utilize diverse options), and the interpersonal dimension (related to experiences in daily life) with two elements, namely information management (choice of non-interaction with specified others) and interaction management (referring to (non-)disclosure of personal information).

As one of the main scholars who demand a 'clustering' of privacy, the philosopher Judith Wagner DeCew (1997) suggests a concept ranging over information, access, and expressions. She reflects a multidimensional nature of privacy and focuses on at least three dimensions – informational privacy, accessibility privacy, and expressive privacy – and therefore combines three theories of privacy: control over information, limited access, and personhood. Informational privacy refers to "control over information about oneself", "accessibility privacy focuses not merely on information or knowledge but more centrally on observations and physical proximity", and expressive privacy "protects a realm for expressing one's self-identity or personhood through speech or activity" (DeCew, 1997).—An example regarding social networks: information privacy overlaps with accessibility privacy when the acquisition of information additionally involves gaining access to a person. The reason: In social networks, authors can decide what personal information is available to the public or not – additionally, content may include facts that can lead another person directly to the author.

Privacy as 'pragmatic approach'

I agree with Solove's (2002) critique that cluster-oriented concepts "still circumscribe privacy based on the boundaries of each of the clustered conceptions". His 'pragmatic approach' draws from a few ideas from pragmatism: "recognition of context and contingency, a rejection of a priori knowledge, and a focus on concrete practices". From his point of view several issues have to be mentioned: privacy is a dimension of social practices (referring to customs, norms, activities and traditions, e.g. writing letters, making certain decisions, etc.) and "should be understood as part of these practices rather than as a separate abstract conception"; therefore, the protection of 'privacy' demands a "claiming to guard against disruptions to certain practices". Approaching privacy should focus on a 'web' of specific types of disruption of specific practices rather than searching for a common denominator that combines all of them. For Solove (2002), first, privacy is valued instrumentally, thus "valued as a means for achieving certain other ends that are valuable", whereas, ends are foreseen consequences which occur regarding an activity and are employed to deliver activity added meaning and route its further course; second, contrary to the tendencies to value privacy in an abstract way, privacy has to be valued contextually. Therefore: "Not all privacy problems are the same, and different conceptions of privacy work best in different contexts. Instead of trying to fit new problems into old conceptions, we should seek to understand the special circumstances of a particular problem. What practices are being disrupted? In what ways does the disruption resemble or differ from other forms of disruption? How does this disruption affect society and social structure? These are some of the questions that should be asked when grappling with privacy problems." (Solove, 2002)

In a current article, Solove (2008) again focuses on contextualization and suggests a taxonomy framing privacy in a pluralistic and contextual manner and calls for changes to surveillance laws. His taxonomy grounds on different kinds of activities that are connected with privacy and aims on supporting policymakers and courts to better balance privacy against countervailing interests by shifting "the focus away from the vague term privacy toward the specific activities that pose privacy problems". The taxonomy bases on four principal groups of activities (each with specific sub-activities): information collection, information processing, information dissemination, and invasion.

ASPECTS OF PRIVACY MANAGEMENT

Drawing attention on an even more practical level, in the following some selected aspect in the field of privacy management will be presented – focusing on an individual, project oriented, organizational as well as legal and governmental level.

In his Restricted Access/Limited Control (RALC) theory, Tavani (2007) defines privacy "in terms of protection from intrusion and information gathering by others (through situations or zones that are established to restrict access), not in terms of control over information". In his theory he tries to incorporate key elements of traditional privacy theories into one unified theory, offering "a procedure for determining whether and how to protect certain kinds of personal information that, arguably, have both private and public characteristics". He further distinguishes "between concerns having to do with the loss of privacy (in a purely descriptive sense) and claims alleging a violation or invasion of privacy (in a normative sense involving a right to privacy)" (Tavani, 2007). RALC differentiates the concept of privacy from both, the management of privacy and the justification. In the context of a situation, privacy is defined with respect to a protection from intrusion and information access by others. A person has normative privacy in a situation where he/she "is protected by explicit norms, policies, or laws that have been established to protect individuals in that situation". Hence, privacy focuses on restricted access and protection - the notion of control and adequate privacy policies (e.g. regarding peer to peer networks on the Internet) should provide individuals with the limited controls which are needed to manage their privacy. RALC can for example be used to "frame a comprehensive online privacy policy that could be applied not only to situations involving data mining but also to a wide range of privacy controversies associated with computer and information technologies" (Tavani, 2007).

As results of the EU-project PRISE (privacy enhancing shaping of security research and technology; 2006-2008; http://www.prise.oeaw.ac.at/), the Austrian Academy of Sciences developed a 'Criteria Matrix in practice' and a handbook for EU-projects in the field of security technology (European commission, FP7). The matrix consists of three stages, whereby each stage should be considered by an EU-project consortium applying for funding and also by evaluators reviewing a proposal. For example, "the proposal must indicate what kind of data is going to be collected and processed with the new security technology" and proposal writers should further discuss whether and how "the general concept of the new technology as well as specific features might infringe the privacy principles" of the country's legal requirements. Proposals also have to address the social impact of the research applying for.

Based on exchange theory, Järvinen (2009) developed a privacy management model in the field of patient-centered e-health (PCEH), proceeding on the fact that in a relationship between a costumer and a provider, more privacy means less services and vice versa. According to web applications, PCEH considers customer privacy (privacy-on-demand) related to a specific service (service-on-demand). Hence, "employing an interactive dialog by demanding or consenting, customers are able to choose from 'max service' to 'min service' to be polarized into the concept of privacy (i.e., 'min privacy' or 'max privacy' and vice versa)" (Järvinen, 2009). In this model customers have the opportunity to change between service-on-demand and privacy-on-demand functions. To ensure a better customers' ability to act, 'opt-in' privacy policies should be offered, requiring "Internet companies to ask people for permission to use their personal information" (Järvinen, 2009).

A further approach is presented by Pounder (2008). He discusses nine principles that can be used (not only but also) for the development of governmental surveillance-related policies, aiming on an assessment whether individual privacy of citizens is broadly considered. Pounder (2008) explains the interrelationship and the consideration of these principles as a whole in the course of a Britain ID Card project. His approach is based on a general human rights framework adopted from most European countries in their data protection laws. An interesting aspect also builds his critical view on the role of information commissioners (function considered in most European countries' data protection laws), stating that they normally are not powerful enough to really affect governmental policy making.

CONCLUSION

The main aim of this article has been to present an overview of the most important theoretical privacy concepts, mainly related to the usage of new technologies. While privacy is difficult to define and has been challenged on diverse grounds and technological developments, instead of highlighting and concentrating on one single and traditional privacy approach - e.g. the right to be alone, secrecy, limited access to the self, personhood or control of personal information - it is necessary to focus on an interrelationship of several approaches. Presented multidimensional approaches highlighting also situational and contextual influencing factors as well as considering social practices play an important role with regard to the usage of new technologies and its effects on several privacy aspects. By facilitating a wider engagement and further input from diverse disciplines, hopefully scholarly debate from such a multidimensional point of view will continue and bring further results. The same applies to the more practical level of privacy management considering different situational and contextual settings from diverse backgrounds as a second important issue in further privacy research.

REFERENCES

1. Austin, L. (2003) Privacy and the Question of Technology, Law and Philosophy, 22, 2, 119-166.
2. Brin, D. (1998) The Transparent Society: Will Technology Force Us To Choose Between Privacy and Freedom, Addison-Wesley, Reading, MA.
3. Burgoon, J. K., Parrot, R., LePoire, B. A., Kelley, D. L., Walther, J. B. and Perry, D. (1989) Maintaining and restoring privacy through communication in different types of relationship, Journal of Social and Personal Relationships, 6, 131-158.
4. Carew, P. J., Stapleton, L. and Byrne, G. J. (2008) Implications of an ethic of privacy for human-centred systems engineering, AI & Society, 22, 3, 385-403.
5. DeCew, J. (1997) In Pursuit of Privacy: Law, Ethics, and the Rise of Technology, Cornell University Press, Ithaca.
6. Dhillon, G. and Backhouse, J. (2001) Current directions in IS security research: towards socio-organizational perspectives, Information Systems Journal, 11, 2, 127-153.
7. Etzioni, A. (2000) The Limits of Privacy, Basic Books, New York.
8. Garfinkel, S. and Russel, D. (2000) Database Nation: The Death of Privacy in the 21st Century, O'Reilly & Associates, Beijing, Cambridge.
9. Järvinen, O. P. (2009) Privacy Management of Patient-Centered E-Health, Patient-Centered E-Health, 81-97.
10. Kemp, R. and Moore, A. D. (2007) Privacy, Library Hi Tech, 25, 1, 58-78.
11. KPMG (2010) Wirtschaftskriminalität in Deutschland 2010 (Economic espionage in Germany 2010), 1-32.
12. Langheinrich, M. (2001) Privacy by Design - Principles of Privacy-Aware Ubiquitous Systems, Ubicomp 2001: Ubiquitous Computing Lecture Notes in Computer Science, 273-291.
13. Langheinrich, M., Coroama, V., Bohn, J. and Mattern, F. (2005) Living in a Smart Environment - Implications for the Coming Ubiquitous Information Society, Telecommunications Review, 15, 1, 132-143.

14. Laufer, R. S. and Wolfe, M. (1977) Privacy as a Concept and a Social Issue: A Multidimensional Development Theory, Journal of Social Issues, 33, 3, 22-42.
15. Lessig, L. (2000) Code and other Laws of Cyberspace, New York.
16. Peters, S. (2009) 14th Annual CSI Computer Crime and Security Survey. Executive Summary, 1-17.
17. PI (2007) The 2007 International Privacy Ranking.
18. Pounder, C. N. M. (2008) Nine principles for assessing whether privacy is protected in a surveillance society, Identity in the Information Society, 1, 1, 1-22.
19. Ramsay, H. (2010) Privacy, Privacies and Basic Needs, The Heythrop Journal, 51, 2, 288-297.
20. Rosen, J. (2000) The Unwanted Gaze: The Destruction of Privacy in America, Random House, New York.
21. Rule, J. B. (2004) Toward Strong Privacy: Values, Markets, Mechanisms, and Institutions, University of Toronto Law Journal, 54, 2, 183-225.
22. Solove, D. (2004) The digital person: Technology and privacy in the information age, New York University Press, New York (NY).
23. Solove, D. J. (2002) Conceptualizing privacy, California Law Review, 90, 1087-1156.
24. Solove, D. J. (2008) Understanding Privacy, GWU Legal Studies Research Paper No. 420 (Harvard University Press), 1-24.
25. Spinello, R. (1997) The end of privacy, America, 176.
26. Sykes, C. (1999) The End of Privacy, New York.
27. Tavani, H. T. (2007) Philosophical Theories of Privacy: Implications for an adequate Online Privacy Policy, Metaphilosophy, 38, 1, 1-22.
28. Walsham, G. (1993) Interpreting Information Systems in Organizations, Wiley, Chichester.
29. Warren, S. D. and Brandeis, L. D. (1890) The Right to Privacy, Harvard Law Review, 4, 5, 193-220.
30. Whitaker, R. (1999) The End of Privacy: How Total Surveillance is Becoming a Reality, New Press, New York.