'Privacy lost - and Found?'
Some Aspects of Regaining Citizens' Privacy by Means of PET in the age of 'Big Data'

Drs John van de Pas, Dr Geert-Jan van Bussel
Senior researcher, Saxion University of Applied Sciences, School of Creative Technology, Deventer, The Netherlands
Associate Professor Digital Archiving & Compliance, HvA Amsterdam University of Applied Sciences School of Design and Communication, Amsterdam, The Netherlands
j.h.vandepas@saxion.nl
g.j.vanbussel@hva.nl

Abstract: In a world where rapid development of ubiquitous computing and 'the internet of things' are quickly leading to Big Data and Smart Cities, we are witnessing the emergence of Cyberspace as a transforming force in society. This transforming power may be seen perhaps nowhere more profoundly than in the field of citizens' privacy. At a conceptual level privacy is easily understandable. Privacy regulations state that privacy-sensitive information may be captured by organizations, provided 1] that the person the information is gathered about consents to the information being gathered and 2] the information is only used for the express purpose the information was gathered for. Any other use of this personal information without consent is prohibited by law; notwithstanding legal exceptions. When laws must be applied in Cyberspace, the rules and regulations need to be embedded in the code of used information and communication technologies (ICTs). Writing code involves information modelling. Compliance to laws depends on proper modelling of privacy laws and regulation in the development process of ICTs. If these are properly translated in written code, they will be part of the outcomes of the end product – the information system will therefore be privacy compliant. We are reporting the results of our exploratory desk research as an introduction to a more extensive research project on Privacy, Big Data and the Smart City. In this paper we attempt to take stock of the question whether privacy enhancing technologies (PETs) may be an answer to challenges posed by extended use of ICTs by both citizens and commercial companies in the age of Big Data.

Keywords: Privacy, Privacy Enhancing Technology, Digital Archiving, Information Value Chain, Big Data, Information Management

Introduction: Privacy and ICT

In this paper we will be exploring some interactions between information and communication technologies (ICTs) and Privacy. It is an issue that manifested itself prominently with the emergence of the 'Internet of Things' and 'Big Data'. Within the next few years, according to Mayer-Schönberger & Cukier (2013), we will be witnessing the final breakthrough of Big Data as a transforming force in our society. The Internet of Things will provide our environment 'with eyes and ears'. Information harvesting systems, fed by the upcoming abundance of all kinds of sensory systems that continuously capture information regarding human-environment interaction in the Smart City, lead to new challenges in the area of the privacy of citizens. For the purpose of this paper, we consider individuals as 'individuals-as-citizen', bestowed with citizens' rights that are to be respected by government institutions by law, among them the right to privacy (Rezgui, et al. 2003). Data, traditionally captured in ICTs by organizations, are breaking loose from the constraints imposed by separate information systems and are absorbed into a 'cloud'. All data in that 'cloud' are stored, analysed, transmitted and reprocessed in a continuous cycle of information management processes and algorithmic processing. The challenge of facilitating ICTs with proper and fail-proof systems to guarantee citizens' privacy during information processing is by no means new (Flaherty, 1989; Solove, et al. 2006; Etzioni, 2007; Kosinski, et al. 2013). Incidents involving privacy infringement are, likewise, not a new phenomenon, especially not in a time of ever more intrusive surveillance technologies and data analysis techniques (Wang & Petrison 1993; Lahlou, et al. 2005; Leese 2013). Attempts are made, however, to ameliorate the situation. Privacy infringement may be portrayed as 'natural' to the implementation of ICTs, but as Morozov (2013, p 20) points out organizations developing information systems make *choices*. There are therefore no 'inherent' properties of information systems. Organizations processing data choose to add or substract functionalities in their software. That means, that they may decide to implement Privacy Enhancing Technologies (PETs), thereby respecting citizens' privacy during their operations. There is a major problem however. Privacy is a legal concept from the real world, ruled by institutions manned by people. ICTs are also part of cyberspace, ruled by technology. Although some aspects overlap, at the same time it must be acknowledged that each environment comes with their own sets of rules and limitations. Laws 'work' best in the real world. And as can be witnessed on a daily basis:

real-world laws may not necessarily apply the same way in global cyberspace. The rule of law therefore cannot be translated directly from the one to the other, and the other way around (e.g., Solove 2004).

Purpose and Research Method: An inventory of Thought on Privacy-aware Cyberspace
This paper explores the current state of affairs on the feasibility of a privacy-aware Big Data environment. As Big Data is fed by ICTs, our goal is to find out what current research has to say, if anything, on the concept of ICTs that are respectful towards citizens' privacy. While privacy and ICTs (and in its wake Big Data) are often portrayed as opposites (Pogue 2011; Morozov 2013), we intend to investigate whether citizens' privacy might still be upheld, while at the same time the benefits of Big Data analysis may be reaped by citizens and information processing organizations alike. We will do that by means of an inventory of a reasoned selection of recent literature on the development of technologies and procedures that may provide the means to create a privacy-sensitive ICT environment. Privacy laws and regulations intend to provide citizens with the right to privacy. In theory the working sphere of these laws extends to the real world and cyberspace alike. The way this may be put into practice in ICTs is explored in a PhD on the use of PETs by Borking (2010). He discusses problems of transforming and methods and techniques available to transform real-world law through 'programming code' into cyberspace. Another, more technological perspective is elaborated by Van Heerde (2010). This PhD provides an overview of available technological solutions to make information systems privacy-aware by looking at ways ICTs may be configured to yield data processing to the privacy laws and regulations from the real world. Besides these two fundamental publications, we collected literature with a key word search in Google Scholar and in the Digital Library of the University of Amsterdam (indexes on IT an information science / management) on the subject of PETs. Very important for our research were papers that allowed us a glimpse into technological solutions that might help solve ICT-induced privacy problems (e.g., Zeng, et al. 2013, Martínez-Ballesté, et al. 2013; Thierer, 2013; Kwecka, et al. 2014).

We will pay attention to some basic assumptions that underlie privacy regulations. These regulations intervene in the processing of information by prescribing the rules any organization has to adhere to while processing citizens' information. A closer look at the way information is processed by organizations, using the theory of the information value chain (IVC) (Van Bussel & Ector 2009; Van Bussel 2012), will allow for a structured way to implement privacy regulations within the organizational ICTs. It is during processing of citizens' privacy-sensitive information that violations of privacy (and henceforth of privacy regulations) may ensue. We will take a look at research that has been done towards making information processing systems compliant to privacy regulations. This leads to an inventory of PETs, that strive to make information systems privacy-aware. The feasibility of implementation of privacy regulations into ICTs should be put to the test by confronting PETs with a privacy-audit, as proposed by Mayer-Schönberger & Cukier (2013).

Privacy – an evasive concept
Privacy regulations are abundant, just like literature on the subject. The European Union privacy guideline 95/46/EC (1995), which protects individuals with regard to the processing and transmitting of personal data, has been in place since the closing years of the 20th century. It was amended by Directive 97/66/LC (EU 1997), expanding the scope to electronic services, and ulitmately replaced by the Directive on Privacy and Electronic Communications (EU 2002). Although local and national legislation is also in place, all EU member states should adhere to these regulations. Lessig (2006, p 5) wrote that 'In real space, we recognize how laws regulate - through constitutions, statutes, and other legal codes. In cyberspace we must understand how a different 'code' regulates - how the software and hardware (i.e., the 'code' of cyberspace) that make cyberspace what it is also regulate cyberspace as it is. […] this code is cyberspace's 'law'.' In cyberspace, in other words, 'code is law (Lessig 2006, p 5). The analysis of this phrase by Borking (2010, p 11) is based on the perspective of a real-world privacy authority, and explores ways in which Law, upheld by legal systems in the real world, may translate into *code* in cyberspace. He explores the way data service providers may make their hard- and software compliant to privacy guidelines and regulations. Van Heerde's (2010) information management approach concentrates on the implementation of those legal guidelines and regulations. Although focused on the technological possibilities of privacy-compliant ICTs, Van Heerde (2010) shares Borking's (2010) concerns when discussing the data analysis technologies of Google, Apple, Facebook, Twitter and Amazon, the largest data aggregators worldwide, and the fact that the price citizens pay for 'free' services is privacy-sensitive information about themselves. 'The market needs urgently to be regulated and, most importantly, to get transparent. […] Transparency is one of the key

foundations of privacy; it must be clear for the user how his or her data is being handled, stored, and to whom it will be disclosed. Asymmetry of power between users and service providers leads to privacy risks for the users, because service providers are in a better position to serve their interests' (Van Heerde 2010, p 6). Service providers, by their actions, shape privacy in the real world as much as real-world law is trying to shape privacy compliance in cyberspace (Tsiavos, et al. 2003). Ultimately, both actions are inherent to the way information systems are built. System developers building the data collection and analysis systems making Big Data possible determine what users can and cannot do with those ICTs. The 'rule of the code' leads to 'laws' being enforced by ICTs (Lessig 2006). This puts law enforcement powers in the hands of the code-writing system developer. In cyberspace, the system developer holds both legislative and executive power, which is undesirable because the code-making process defies proper democratic controls, deemed essential in a constitutional state (Borking 2010, p v).

Privacy in organizational information systems

There existed a relative sense of control on the aspect of privacy in organizational ICTs. Until a few years ago, information retention was deemed a matter of organizations that exploited their own ICTs. Organizations captured their business process information into a digital infrastructure, which didn't cross the borders of the organization's structure. Organizations controlled the information that was collected and retained within their ICTs. If privacy issues arose, a single point of interaction could be contacted by a citizen or privacy authority (Davenport & Prusak 1997). That 'point of control' became diffused with 1] the ongoing integration of processes between different organizations, stimulated by the sharing of information through (for instance) social media (McAfee 2006), and 2] the breakthrough of supply chain and ERP systems, causing information integration (Srinivasan & Dey 2014). As it became common practice to share data between different parties, it could become quite difficult to ascertain which of the integrated process-owners was responsible for a breach of privacy, if and when that occurred. A model of the information flow in and between organizations can be drawn using both interorganizational business process analysis and information flow analysis. Van Bussel and Ector (2009) introduced an innovative concept of the information value chain (IVC). The IVC is a process model that includes all processes within the information flow: generation or receipt, identify, capture, storage, processing, distribution, structuring, publication, (re-) use, appraisal, selection, disposal, retention, security, auditing and preservation (Van Bussel & Ector 2009; Van Bussel 2012). The IVC (see Figure 1) is instrumental in providing proper control on the performance of business processes, the provision of trusted information and the protection of privacy-sensitive data. Privacy issues in the information processing process must be assessed, to identify possible risks for the organization and take proper actions if breaches of privacy regulations may take place (Haller 2012).

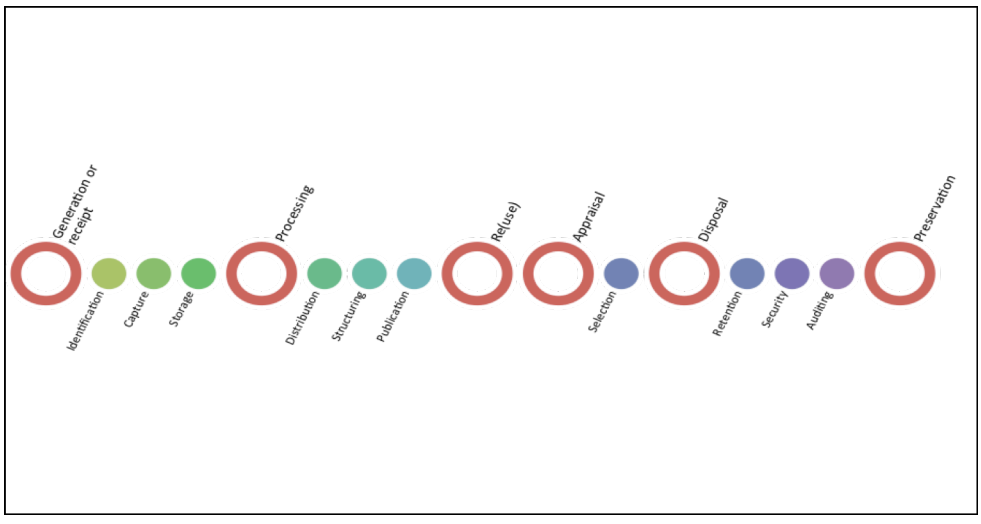

Figure 1 The information value chain (IVC) (Van Bussel & Ector, 2009, p. 13)
(Open circles: Start of stage, privacy-audit necessary)

Organizations need to take proper care of the information they are entrusted with by citizens, because any failure to do so leads to loss of trust, economic value or public support. Most organizations consider compliance with privacy guidelines primarily relevant at the point where information enters the

ICTs of the organization ('generation/receipt' in the IVC, the first 'open circle' in Figure 1). Looking at the IVC from a privacy risk perspective, risks of privacy infringement appear most explicitly at 6 moments, emphasized in Figure 1 as 'open circles': generation/receipt of information within the organization, processing, (re-)use, appraisal, disposal and preservation of information.

Privacy and information security

Most organizations have implemented information security procedures in order to protect data integrity and to prevent unauthorized access to the information contained in their ICTs. Borking (2010) discusses these measures extensively, referring to the EU funded PISA research project (Privacy Incorporated Software Agent) (EU 2004). In PISA, researchers investigated the applicability of information security measures on privacy compliance. Table 1 shows the conclusions of that research: information security measures do not lead to compliance to privacy regulations that would render ICTs privacy-aware. Borking (2010, p 68) states it is not surprising that privacy is not met by the information security policy of an organization, due to the fact that 'information security and confidentiality surpass lawfulness completely'. Whether the information contained in the information system is put there lawfully is *not* subject of the information security policies. The conclusion is unavoidable that privacy compliance is not guaranteed by applying information security policies. It is quite clear *why* organizations have problems with developing their systems to be compliant to privacy law and regulations. Where information security may be controlled sufficiently, privacy proves to be too elusive and conceptual to implement in an automated system 'because of its subjective nature' (Van Heerde 2010, p 55).

		Privacy Criterion								
		Reporting of processing	Transparent processing	'As required' processing	Lawful basis for data processing	Data quality conservation	Rights of the parties involved	Data traffic with countries out-	Processing personal data by	Protection against loss and
Information Security	Availability									
	Confidentiality									
	Integrity									

Very strongly related
Strongly related
Moderately related
Weakly related
Not related

Table 1. PISA Information Security vs Privacy (Borking 2010, p 68)

Building Privacy-sensitive ICT systems

Defining the problem 'out of scope' is not a solution. An organization (when confronted with the risks of privacy breaches) has to accept the possibility of privacy issues arising from the use of citizens' information in ICTs, and needs to embed privacy compliance in its requirements analysis (in the case of new, to be developed ICTs) or in its auditing cycle (within existing ICTs). An organization has to embed privacy enhancement measures in its business processes. That means that organizations have to take ample precautions that privacy-sensitive information is being processed in such a way that risks of privacy-infringement are minimized and that privacy guidelines and regulations are respected within ICTs. They can use PETs: technologies that try to implement privacy-compliancy in ICTs. PETs have been studied extensively in the last decades (Wolfe 1997; Seničar, et al. 2003; Phillips 2004; Borking 2010; Van Heerde 2010; Zeng, et al. 2013; Kwecka, et al. 2014).

Van Heerde (2010) shows the possibilities of privacy aware data management. The focus of this research is on limiting the potential damage caused by a breach of data security by meticulously managing the data stored in ICTs. A technological solution is conceived to the technology-induced problem of data retention by owners of ICTs. According to this research it is 'possible to reason about retention periods so that not only service providers, but also users of those services will be satisfied' (Van Heerde 2010, p 152). The proposed solution is that after primary use of information, data preci-

sion is decreased automatically in different stages. Information may therefore be decreased automatically by automatic adjustment of data elements that provide precision in queries. The object is to degrade the data in an irreversible way (Van Heerde 2010, p 150). After an extensive analysis of scientific literature, Van Heerde (2010, pp 133-146) points towards five different possible ways of implementing data degradation techniques: service-oriented, ability-oriented and user-oriented data degradation, upgradable data degradation and external data degradation. Only user-oriented data degradation puts the citizen (not the service provider, as in the other data degradation techniques) in charge of the process of data retention. All other options imply some form of built-in system functionality. This means that (with the exception of external data degradation) these techniques rely on a single point of interaction with data retention (like in a classical database management system). The techniques of data degradation may be a solution to privacy issues in these 'monolitical', 'one point of interaction' ICTs, because the entire life cycle of information is managed within the system itself.

Providing Privacy in an era of 'Cloud' and 'Big Data'

In a networked environment the problem of privacy compliance gets more complicated. The previous data degradation technologies do not work properly in a networked environment. As the majority of data in a mobile world is transported between different ICTs in which different sets of information are stored and processed, no 'single point of entry' to the management and retention of data exists. For those purposes Van Heerde (2010, p 144) puts external data degradation forward, but does not elaborate on this solution. In his opinion, external data degradation is binding the degradation policy to the data while the data is traveling through the network, and make network components degradation-aware. Network switches and routers can check the policy attached to each data item, and block (or remove) the data item from the stream if it does not comply with the degradation policy. Zeng et al. (2013) have tested a working proof-of-concept prototype of this kind of PET on user data in 'the cloud'. Their Self Destructing Data System (SeDas) protects data privacy from attackers who retroactively obtain, through legal or other means, a user's stored data and private decryption keys. The prototype irreversibly destroys sensitive information, such as account numbers, passwords and notes, without any action on the user's part.

Martinez-Ballesté (et al. 2013) add a holistic approach to the issue of privacy enhancement in networked environments. ICTs help governments to improve the management of operations of cities in a variety of areas: transportation, energy, sustainability, e-governance, economy, communications, etc. They analyze all available PETs that might mitigate the privacy-corroding effects of these developments: pseudonymizers, RFID privacy techniques, privacy-aware video surveillance, private information retrieval techniques, location masking, cloaking, anonymization, statistical disclosure control and privacy-preserving data mining (Martinez-Ballesté, et al. 2013, p 140). An interesting concept has been developed in Van Blarkom, Borking and Olk (2003, pp 33-49). In this concept, seven principles of PET are defined: [1] Limitation in the collection of personal data; [2] Identification, authentication, authorisation; [3] Standard techniques used for privacy protection; [4] Pseudo-identity; [5] Encryption; [6] Biometrics; and [7] Audit ability. These principles can be associated with the Common Criteria (CC) for Information Technology Security Evaluation (ISO/IEC 15408, 2009). We combined both PET principles and CC with the technologies mentioned in Martinez-Ballesté (et al. 2013) in Table 2 to generate an overview of PET solutions. This table shows that, although the technologies are in place, 'there is still a lot of work to be done to materialize the notion of privacy in smart cities' (Martinez-Ballesté, et al. 2013, p 136). In other words: many of those technologies are not used yet by organizations to protect the privacy of citizens. That there are no PETs in use for automatic security/privacy audits and for security management is a cause for concern.

CC	PET Principles	Technological Solutions
Security / Privacy Audit	Audit Ability	
Communication	Encryption	RFID privacy techniques
Cryptographic Support	Encryption	RFID privacy techniques
User Data Protection	Limitation in the collection Identification, authentication, authorization Standard Techniques	anonymization cloaking location masking private information retrieval techniques privacy-aware video surveillance privacy-preserving data mining statistical disclosure control

CC	PET Principles	Technological Solutions
Identification and Authentication	Identification, authentication, authorization Biometrics	anonymization cloaking location masking privacy-preserving data mining private information retrieval techniques statistical disclosure control
Security Management		
Privacy		
Anonymity	Standard Techniques	anonymization privacy-aware video surveillance privacy-preserving data mining private information retrieval techniques statistical disclosure control
Pseudonimity	Pseudo-identity	pseudonymizers
Unlinkability	Standard Techniques	anonymization cloaking location masking statistical disclosure control
Unobservability	Standard Techniques	privacy-preserving data mining private information retrieval techniques

Table 2. PET principles, CC and technological solutions

IDP: Privacy Protection embedded in ICTs

A method to protect users' privacy is a trusted third party, operating as an 'identity protector' (IDP). This IDP allows for privacy-aware fulfilment of the IVC. Borking (2010, pp 179, 201-202) shows the workings of this IDP in the technological environment of an ICT, realizing an overall view into the technology of privacy-aware processing of data. According to Mayer-Schönberger and Cukier (2013, p 173) providing proper privacy to citizens in an age of ubiquitous computing and Big Data remains to be a mind-bending problem. Traditional methods for privacy-safeguarding are no longer feasible. They propose privacy assessments, backed up by real authority (a sort of IDP?) that may impose the rule of privacy law on the organizations reaping the (huge) benefits of Big Data analysis. A formal assessment offers tangible benefits to data users: they will be free to pursue secondary uses of personal data in many instances without having to go back to individuals to get their explicit consent. By data users, to make matters clear, they mean the organization that exploits privacy-sensitive data, not the citizen-as-user. Implementing these assessments based on the IVC and the six steps therein to be audited could minimize privacy breaches. Table 2 indicates that this proposal for privacy assessments is correct.

Conclusion and further research

Electronic information retention, ubiquitous computing, and Big Data make issues of use of privacy-sensitive information major problems for both citizens and information processing organizations. With the movement from 'ownership-oriented' ICTs to service-oriented 'cloud' determination *who* needs to solve a privacy issue once it arises has become almost impossible. It is widely acknowledged that some of the most beneficial aspects of Big Data also give rise to the most influential and invasive breaches of citizens' privacy. NSA, GAFTA and citizens benefit from Big Data, but the citizens do not have the power of NSA and GAFTA. Rules and regulations are available. There are data authorities bestowed with ample powers to enforce privacy compliance. Rules can be translated into code that makes ICTs privacy-aware (or not). Technologies exist to implement privacy regulations, and even empower citizens by providing self-destructing data, embedded in the networking environment. As an answer to our research question: it is possible to make the Big Data information environment privacy-aware, providing citizens with the privacy they are entitled to by rights. At a conceptual level there is nothing preventing privacy-aware data. We are then, however, left with a puzzling problem. If no real legal and technological barriers for proper implementation of PETs seem to exist, why are they not being implemented? If there seem to be no legal or technological barriers preventing wide scale implementation of PETs, logic dictates that there might be other factors at play. The power distribution is in our view a likely candidate that might be responsible for putting up that blockade. We think this

'power aspect' might constitute a hitherto underexposed spot in the debate on PETs implementation. We deem it highly relevant to explore this line of investigation, as privacy infringements eat away at trust levels in society at large, with detrimental effects on society. In our view, chances are that the Key to Privacy in the era of Big Data might just be found there. Providing proper privacy to citizens is no matter of small concern.

References

Borking, J. (2010) *Privacyrecht is code. Over het gebruik van Privacy Enhancing Technologies,* Kluwer, Deventer.

Davenport, T. H. & Prusak, L. (1997) *Information ecology: Mastering the information and knowledge environment*, Oxford University Press, New York.

Etzioni, A. (2007) "Are new technologies the enemy of privacy?", *Knowledge, Technology & Policy*, Vol. 20, No. 2, pp 115-119.

EU (1995) *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*. [online], http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:-en:NOT

EU (1997) *Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector*. [online] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31997L0066:EN:HTML

EU (2002). *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).* [online], http://eur-lex.europa.eu/-LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML.

EU (2004) *Privacy Incorperated Software Agent: Building a privacy guardian for the electronic age*. [online], http://cordis.europa.eu/projects/rcn/53640_en.html.

Flaherty, D. (1989) *Protecting privacy in surveillance societies. The federal republic of Germany, Sweden, France, Canada, and the United States*, The University of North Carolina Press, Chapel Hill.

Haller, K. (2012) "Data-Privacy Assessments for Application Landscapes: A Methodology", Daniel, F., Barkaoui, K., & Dustdar, S. (eds.), *Business Process Management Workshops,* 2, Vol. 100 (Lecture Notes in Business Information Processing), pp 398-410.

ISO/IEC 15408-1 (2009) *Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model,* ISO, Geneva.

Kosinski, M., Stillwell, D. & Graepel, T. (2013) "Private traits and attributes are predictable from digital records of human behavior", *Proceedings of the National Academy of Sciences*, Vol. 110, No. 15, pp 5802-5805.

Kwecka, Z., Buchanan, W., Schafer, B. & Rauhofer, J. (2014) "'I am Spartacus': privacy enhancing technologies, collaborative obfuscation and privacy as a public good', *Artificial Intelligence and Law* (2014), pp 1-27.

Lahlou, S., Langheinrich, M. & Röcker, C. (2005) "Privacy and trust issues with invisible computers", *Communications of the ACM*, Vol. 48, No. 3, pp 59-60.

Leese, M. (2013) "Blurring the dimensions of privacy? Law enforcement and trusted traveler programs", *Computer Law & Security Review*, Vol. 29, No. 5, pp 480-490.

Lessig, L. (2006) *Code, version 2.0.*, Basic Books, New York.

Martínez-Ballesté, A., Pérez-Martínez, P. A., & Solanas, A. (2013) "The Pursuit of Citizens' Privacy: A Privacy-Aware Smart City Is Possible", *IEEE Communications Magazine,* vol. 51, No. 6, pp 136-141.

Mayer-Schönberger, V., & Cukier, K. (2013) *Big data. A revolution that will transform how we live, work and think,* John Murray, London.

McAfee, A. (2006) "Enterprise 2.0: the dawn of emergent collaboration", *MIT Sloan Management Review*, Vol. 47, No. 3, pp 21-28.

Morozov, E. (2013) *To save everything, click here. The folly of technical solutionism,* PublicAffairs, New York.

Phillips, D. J. (2004) "Privacy policy and PETs. The influence of policy regimes on the development and social implications of privacy enhancing technologies", *New Media & Society*, Vol. 6, No. 6, pp 691-706.

Pogue, D. (2011) "Don't worry about Who's watching', *Scientific American*, Vol. 304, No. 1, p 32.

Rezgui, A., Bouguettaya, A., Eltoweissy, M.Y. (2003) "Privacy on the Web: facts, challenges, and solutions", *IEEE Security & Privacy,* Vol. 1, No. 6, pp 40-49.

Seničar, V., Jerman-Blažič, B., & Klobučar, T. (2003) "Privacy-enhancing technologies - approaches and development", *Computer Standards & Interfaces*, Vol. 25, No. 2, pp 147-158.

Solove, D.J. (2004) *The Digital Person. Technology and Privacy in the Information Age*, New York University Press, New York, London.
Solove, D.J., Rotenberg, M., & Schwartz, P.M. (2006) *Privacy, information, and technology*, Aspen Publishers Online, New York.
Srinivasan, M. & Dey, A. (2014) "Linking ERP and e-Business to a Framework of an Integrated e-Supply Chain". Martínez-López, F.J. (ed.), *Handbook of Strategic e-Business Management,* Springer, Berlin-Heidelberg, pp 281-305.
Thierer, A. (2013) "Privacy, Security, and Human Dignity in the Digital Age: The Pursuit of Privacy in a World Where Information Control is Failing", *Harvard Journal on Law & Public Policy,* Vol. 36, No. 2, pp 409-455.
Tsiavos, P., Hosein, I.R., & Whitley, E.A. (2003) "The footprint of regulation: How information systems are affecting the sources of control in a global economy", Korpela, M., Montealegre, R. & Poulymenakou, A. (eds), *Organizational information systems in the context of globalization,* Kluwer, Deventer, pp 355-370.
Van Blarkom, G.W., Borking, J.J, & Olk, J.G.J. (2003) *Handbook of privacy and privacy-enhancing technologies*. *The case of Intelligent Software Agents*, Privacy Incorporated Software Agent (PISA) Consortium, The Hague.
Van Bussel, G.J. (2012) *Archiving should be just like an Apple™ en acht andere, nuttige (?) stellingen*, Amsterdam University Press, Amsterdam.
Van Bussel, G.J. & Ector, F. (2009). *Op zoek naar de herinnering. Verantwoordingssystemen, content-intensieve organisaties en performance.* Helmond: Van Bussel Document Services.
Van Heerde, H. (2010) *Privacy-aware data management by means of data degradation. Making private data less sensitive over time,* Twente University, CTIT, Enschede.
Wang, P. & Petrison, L.A. (1993) "Direct marketing activities and personal privacy. A consumer survey", *Journal of Direct Marketing*, Vol. 7, No. 1, pp 7-19.
Wolfe, H. B. (1997) "Privacy enhancing technology", *Computer Fraud & Security*, Vol. 1997, No. 10, pp 11-15.
Zeng, L., Chen, S., Wei, Q., & Feng, D. (2013) "SeDas: A Self-Destructing Data System Based on Active Storage Framework", *IEEE Transactions on magnetics,* Vol. 49, No. 6, pp 2548-2554.