‘Privacy Lost - and Found?’ The information value chain as a model to meet citizens’ concerns

John van de Pas[1] and Geert-Jan van Bussel[2]
[1]Saxion University of Applied Sciences, School of Creative Technology, Deventer, The Netherlands
[2]Digital Archiving & Compliance, HvA Amsterdam University of Applied Sciences, School of Economics and Management, Amsterdam, The Netherlands
j.h.vandepas@saxion.nl
g.j.vanbussel@hva.nl

Abstract: In this paper we explore the extent to which privacy enhancing technologies (PETs) could be effective in providing privacy to citizens. Rapid development of ubiquitous computing and ‘the internet of things’ are leading to Big Data and the application of Predictive Analytics, effectively merging the real world with cyberspace. The power of information technology is increasingly used to provide personalised services to citizens, leading to the availability of huge amounts of sensitive data about individuals, with potential and actual privacy-eroding effects. To protect the private sphere, deemed essential in a state of law, information and communication systems (ICTs) should meet the requirements laid down in numerous privacy regulations. Sensitive personal information may be captured by organizations, provided that the person providing the information consents to the information being gathered, and may only be used for the express purpose the information was gathered for. Any other use of information about persons without their consent is prohibited by law; notwithstanding legal exceptions. If regulations are properly translated into written code, they will be part of the outcomes of an ICT, and that ICT will therefore be privacy compliant. We conclude that privacy compliance in the ‘technological’ sense cannot meet citizens’ concerns completely, and should therefore be augmented by a conceptual model to make privacy impact assessments at the level of citizens’ lives possible.

Keywords: privacy, privacy enhancing technology, digital archiving, information value chain, big data, information management

1. Introduction: Privacy and cyberspace

Privacy and Information & Communication Technologies (ICTs) are often portrayed as opposites (Pogue, 2011; Morozov, 2013, Hofstetter, 2014). In this paper we will be exploring some interactions between ICTs and Privacy, with particular attention to the transition of privacy’s conceptual definition in the real world into cyberspace. Although concerns over citizens’ privacy are by no means new, the issue has manifested itself prominently with the emergence of the “Internet of Things”, “Big Data” and “Smart Cities”, and public outrage following releases of documents by Snowdon and Wikileaks. Hundreds of articles and books have been published by scientists, professionals, journalists, politicians and bloggers on this subject, giving some indication that statements like “You have zero privacy anyway – get over it” (Sprenger, 1999) may have to be reassessed.

Within the next few years, according to Mayer-Schönberger and Cukier (2013), we will be witnessing the final breakthrough of Big Data as a transforming force in our society. Information harvesting systems, fed by the upcoming abundance of all kinds of sensory systems that continuously capture information regarding human-environment interaction will lead to new privacy challenges. Data, traditionally captured in organizational ICTs, are breaking loose from its constraints and are absorbed into a “cloud”. While Big Data is most commonly associated with the stockpiled personal information of users of ICTs, the (predictive) data analysis technologies applied to that data are its true smartness (Siegel, 2013). These developments will make keeping information private and confidential particularly challenging (Wang and Petrison, 1993; Lahlou et al, 2005; Leese, 2013). Although the implementation of ICTs results, almost like a “Law of Nature”, in privacy infringement most of the times, Morozov (2013) points out that organizations developing ICTs do make choices. Organizations processing data define functionalities at the start of software development processes, and may decide to respect citizens’ privacy in their operations. Facilitating ICTs with proper and fail-proof systems to guarantee citizens’ privacy during information processing has, however, been described as hugely challenging (Flaherty, 1989; Solove et al, 2006; Etzioni, 2007; Spiekermann 2009; Kosinski et al, 2013). This can be traced back to the elusive character of the term “privacy”. Privacy is a social concept from the real world, that has been translated into laws and regulations, and is interpreted by people in social environments. ICTs, on the other

Reference this paper as: van de Pas J. and van Bussel G., “‘Privacy Lost - and Found?’ The information value chain as a model to meet citizens’ concerns” The *Electronic Journal Information Systems Evaluation* Volume 18 Issue 2 2015, (pp185-195), available online at www.ejise.com

hand, are part of cyberspace, ruled by technology, which is based upon modelled versions of real life concepts. Although modelling techniques allow for some overlap between the social, legal and technological realms, at the same time it must be acknowledged that each environment comes with its own sets of rules and limitations. Laws work best in real world environments, where letter and intent can be interpreted because human beings are involved. In information technology, it is possible for literal rules to be applied successfully, but it is difficult to apply the intent of a rule. As a consequence, direct translation of real-world laws to rules regulating global cyberspace may not be possible (Lessig, 2006, Solove, 2004).

2. Purpose and research method: an inventory of thought on privacy-aware ICTs

The subject of this paper was conceived during discussions about ways to find clear and unambiguous standards to make ICTs respectful of citizens' privacy. A keyword search on privacy and system development in both scientific and professional databases (EBSCO Academic Search Premier, Paperity.org and IEEE Xplore digital library) made clear that the debate on privacy-aware ICTs is lively, and covers the concept of privacy, the way that concept is translated into rules and regulations, the risks facing organizations and citizens and the methods and technologies available to make ICTs privacy-aware. While proper attention is being paid to different aspects of ICT development within the boundaries of organizational environments, the perspective of the citizen somehow seems to have got lost by a focus on regulatory and technological aspects by professional and scientific communities.

Although social media and technology pundits state that privacy is dead, a vast majority of citizens still considers personal information confidential. At the same time, an equal majority of citizens expects services to be tailor made, and service providers need detailed information about the user to provide those. Many people more or less willingly provide this information, for in many cases refusing to do so entails denial of service. However the citizen explicitly or tacitly expects the service provider to act responsibly when processing confidential and sensitive data for service personalisation. Commercial use of those data for other purposes is generally frowned upon, and, when found out, results in privacy scandals.

This ambiguity is complicating both provision of personalized services and respecting citizens' concerns towards privacy. The availability and use of privacy rules and regulations and the application of privacy enhancing technologies (PETs) have not made privacy infringements a thing of the past. This seems to point towards the conclusion that technological and regulatory measures fail to provide citizens with satisfactory privacy protection in ICTs. To identify possible reasons for this gap between reality and ideal, we have decided to choose a citizen's perspective as the starting point for our analysis of the attempts that are made to translate real life privacy into privacy-aware ICTs. For that purpose, we will use the concept of the information value chain (IVC) (Van Bussel, 2012ab), which describes the information life cycle in conceptual terms. The IVC will allow for a structured way to implement privacy regulations within organizational ICTs. Using that model, we will try to answer the question why, if regulations and technologies are available, privacy breaches by information technology still exist.

To do that, we will attempt to follow the translation of privacy-in-real life through the development process into privacy-aware ICTs one step at a time. Starting with Allen (2011), who scrutinizes the transformation of the concept as it passes from its' natural environment through legislation into practical application in ICT environments, and questions whether individuals are in a position to make informed choices on their privacy. Hofstetter (2014) provides a more belligerent viewpoint, as she explores the rise of intelligent machines and their impact on human freedom of choice, stating that the private sphere is under severe pressure and should be protected. Both views could have profound impact on the way ICT's may deliver privacy as intended by the citizen. The way laws may be put into practical application in ICTs is explored in a PhD thesis on the use of PETs by Borking (2010). He discusses methods and techniques available to transform "real-world" law through "programming code" into "cyberspace law". Another, more technological perspective is elaborated by Van Heerde (2010). His PhD thesis provides an overview of available technological solutions to make ICTs privacy-aware by looking at ways they may be configured to yield data processing to the privacy laws and regulations from the real world. The technological perspective is further elaborated by a selection of publications on technological solutions to ICT-induced privacy problems (Zeng et al, 2013; Martínez-Ballesté et al, 2013; Thierer 2013; Kwecka et al, 2014). Spiekermann and Cranor (2009) allow a look from the point of view of system developers, in their excellent overview of the state of affairs regarding engineering practices of privacy-aware systems, and the scope and limits of the technological community developing services in cyberspace.

And finally we will take a look at what is considered the touchstone for the feasibility of implementation of privacy regulations into ICTs: confronting PETs with a privacy-audit, as proposed by Mayer-Schönberger and Cukier (2013).

3. Privacy as a socio-cultural factor

One phrase about the rights of citizens from Warren and Brandeis (1890: 193) has become famous: "[…] now the right to life has come to mean the right to enjoy life, -- the right to be let alone; the right to liberty secures the exercise of extensive civil privileges; and the term "property" has grown to comprise every form of possession -- intangible, as well as tangible". Describing this 'right to be let alone' in legal terms has proven to be a mind-bending effort, partly due to the fact that privacy is a social construct like "trust" or "autonomy". Defining its meaning is difficult, due to the contextual character of the concept. Privacy depends on the specifics of the situation and the persons involved. What constitutes a breach of privacy is therefore not easily defined in general terms.

In "Unpopular privacy" Allen (2011) describes privacy as an "umbrella" concept incorporating several narrower concepts, including seclusion, solitude, secrecy, reserve, confidentiality and data protection, that denote modes of limiting access to people and personal information. Conly (2013) discusses the relevancy of protection of the public sphere in the context of government policies limiting exchange of information and imposing protective measures on individuals, market organisations and government agencies. Preventing undue disclosure of confidential information is essential when the harm that may be done may extend well beyond simple "personal embarrassment". Disclosure of personal information may affect our relationships with commercial organizations, it may affect the ability to get or hold jobs, it may happen without our permission, and it may happen through our voluntary activities, which have a reach we cannot foresee. Conly concludes that leaving control of information to the private sphere does not seem to offer adequate protection of personal information. Hofstetter (2014) links the right to confidentiality and secrecy directly with power, as she describes a "private sphere", based on the right of the individual to have and hold secrets. "Private sphere is the instrument to balance powers" (Hofstetter, 2014: 259). The idea that privacy is both tightly connected to the "private sphere", but also instrumental to the uses and procedures of information services, points towards mechanisms that exert influence on the outcomes of the discussion on privacy protection in cyberspace.

Spiekerman and Cranor (2009) quote research into attitudes concerning privacy in the general population and reports that roughly 25% of ICT users does not care about privacy; the rest of the population can be divided into a large group of "pragmatists" and a small group of "paranoids". Lopez (2010) reports roughly the same results of a survey into consumer privacy protection by Accenture, where internet users were asked whether they agreed with the proposition that consumers have a right to control information collected about them and their family. Only a quarter of the participants of that survey disagreed or strongly disagreed. The general view is that roughly 75% of the population does foster between mild and serious concerns about privacy in using ICTs. Finally, Dawes (2008) mentions outcomes from a research project mapping relevant issues concerning e-governance, in which specific attention was paid to human factors in ICT-enriched environments. The expectations of the general public when using ICT-based services were found to extend far beyond the notion of the application of technology. A wide range of social and cultural reactions were given: 'integrity of self, identity, autonomy, personal choice, privacy, trust, adjustment and learning are essential considerations without regard to any particular technology'. This statement was made in the context of e-government scenario development, but it may safely be assumed that citizens expect comparable levels of respect for the "private sphere" in their interaction with commercial organisations.

4. Regulations on privacy

Privacy regulations are abundant. 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 ultimately 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) 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 with 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: 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 ICTs 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 according to Borking is undesirable, because the code-making process defies proper democratic controls, deemed essential in a constitutional state (Borking, 2010). Information services providers, notwithstanding legal rules and regulations, seem to have the upper hand in the application of privacy regulations as they are major stakeholders in system development projects.

At the other hand, laws and regulations bestow 'ordinary' users with some legal rights that should be respected, as Coles-Kemp and Kani-Zabihi (2010) point out. In their view, the proper path leading to privacy-sensitive systems starts by paying proper respect to citizens' privacy by giving the user control over his or her data, and to support them in decision making on the usage of that data by the service provider. Service providers should empower users to make informed decisions by providing easily understandable information. In ideal terms, this would lead to a dialogue between empowered users and benign service providers, not a monologue with coercive traits from the part of the all-powerful service provider. But Coles-Kemp and Kani-Zahibi admit that the unlevel playing field makes it nigh impossible to exercise this form of what they call 'intuitive privacy: the ability a service user, or data "subject", has to control the disclosure of personal information and the presentation of their on-line identity'.

This imbalance of power is particularly manifest in online environments, where negotiations about the levels of personal information required by the service provider, and to what extent they may be used, are being conducted between highly inequal parties. The single person-user trying to negotiate the use of his or her private information by proposing alternative terms in the privacy policies of Facebook or Google for example, will have a problem. A simple "denial of service" is evoked on the user unwilling to yield to some or all of the privacy policies of the service provider. The playing field between individuals and serice providers shows no signs of movement towards dialogue; the imbalance of power is reinforced (Oyomno et al, 2009). Spiekermann and Cranor (2009: 72) connect privacy compliance with acceptance of information systems and strike a note of warning against continued unrestricted privacy infringements by service providers, as they foresee a "customer back-lash over privacy issues. In order to protect companies from such volatility in customer perceptions, shown to be relevant to stock-market valuation, it may be advisable to build systems and follow privacy policies based on some baseline privacy protection".

5. Privacy in organizational information systems

Most organizations consider compliance with privacy guidelines an integral part of their responsibilities. They do accept the public expectation that organizations pay attention to the safe and correct storage, processing and disposal of the personal information they are entrusted with. To some extent, these privacy policies address issues that may arise in organizational information management. Implementation of privacy policies allows organizations to prove appropriate levels of care in the handling of confidential and sensitive information within business processes. Until a few years ago, information retention was deemed a matter of organizations that exploited their own ICTs. As such, both organisations and the general public could foster a

relative sense of control regarding their data. In the pre-networked computing environment, organizations captured their business process information into a digital infrastructure, that rarely crossed the borders of the organization's structure. Generally speaking, this lead to the widely supported conviction that organizations might be in control of the information that was collected and retained within their ICTs.

A model of the information flow in and between organizations can be drawn using both inter-organizational business process analysis and information flow analysis. Van Bussel (2012ab) introduced the innovative concept of the information value chain (IVC). The IVC consists of a process model that includes all processes within the information flow within an organization or a chain of organizations on a generic level, independent of the technologies used. The processes identified are: generation or receipt, identify, capture, storage, processing, distribution, structuring, publication, (re-) use, appraisal, selection, disposal, retention, security, auditing and preservation. The IVC (Figure 1) is deemed instrumental in providing proper control on the performance of business processes, the provision of trusted information and the protection of privacy-sensitive data. Whenever privacy issues arise, a single point of interaction can be contacted by a citizen or privacy authority (Davenport and Prusak, 1997), to request mitigating measures, post a formal complaint or claim damages.

Privacy issues in the information processing process must be assessed to identify possible risks for the organization and take proper actions if violations of privacy regulations may take place (Haller, 2012). Privacy risks emerge throughout the complete information value chain, as is shown in Figure 1. Due to aspects of efficiency and practicality, however, in most organizations privacy assessments are restricted to the point at which information enters the ICTs of the organization: the "generation/receipt" stage in the IVC. A privacy risk assessment of the IVC, however, may prove that the risk of privacy infringements emerges at six moments, emphasized in Figure 1 as 'open circles': generation/receipt of information within the organization, processing, (re-)use, appraisal, disposal and preservation of information. To make matters worse: the sort of risks the organization will have to take into account, varies both in the senses of impact and liability. In order to prevent privacy infringements completely and sufficiently, organizations will have to execute a detailed analysis of the impact on privacy aspects of each step in the IVC.

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, and sometimes refer to those policies when challenged on the aspect of privacy-compliance. It is relevant to evaluate if the assertion that privacy is guaranteed if security is under control, is correct. Borking (2010) discusses information security oriented 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, and therefore would not render ICTs privacy-aware. According to Borking (2010), those results are not surprising: 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. It is clear *why* organizations have problems with developing their systems to be compliant to privacy law and regulations. Privacy proves to be too elusive and conceptual to implement in an automated system (Van Heerde 2010).

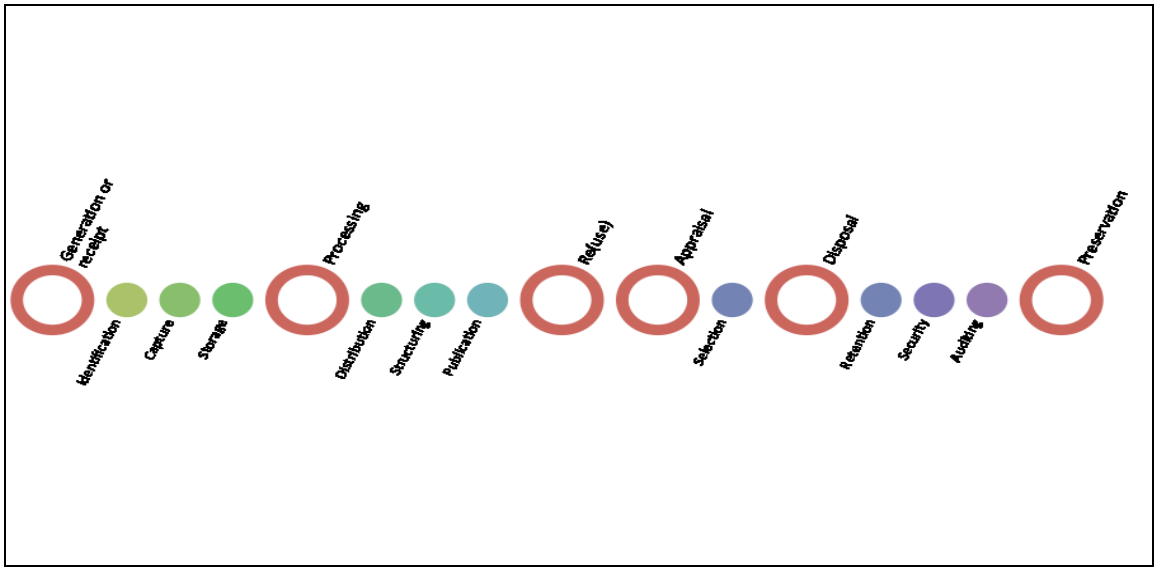

Figure 1: The information value chain (IVC) (Van Bussel, 2012ab) (Open circles: Start of stage, privacy-audit necessary)

		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 outside EU	Processing personal data by processor	Protection against loss and unlawful processing of personal data
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)

6. Building privacy-sensitive ICT systems

If information security measures implemented by organisations do not lead to privacy compliance, other measures need to be considered. In order for an information system to be privacy-compliant, the system development process must pay attention to the elements that may constitute a privacy hazard in an ICT. In this paper, we assume that there is no fundamental difference in system development methodology in public and in private environments. System development methodology is, so to speak, generic in character. Spiekermann and Cranor (2009) provide an integrated overview of methods and techniques available to provide systems under construction with proper privacy compliance. They make a distinction between Privacy-by-architecture and Privacy-by-Policy.

Privacy-by-architecture aims at intervening in the earliest possible stage in a system development project, minimising collection of personal data and implementing technologies that anonymize and protect data during the information life cycle. This means that the system architect analyzes the possible breaches of privacy once the system is delivered and takes proper precautions against it in the drawing board stage. The resulting blueprint for the system should contain specifications in the form of well-defined rules and procedures. That way, a system developer can avert the pitfalls of programming functionalities that inadvertently may breach future users' privacy. Privacy-by-design, in this classification, forms a sub-part of privacy-by-architecture. One of the results of privacy-by-architecture is the conceptual testing and development of Privacy Enhancing Technologies (PETs), that allow for implementation of privacy-compliance in ICTs. PETs have been studied extensively (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, that aims at limiting potential damages caused by a breach of data security by meticulously managing the data stored in ICTs. He concludes that 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: 152). The proposed solution is that after the primary use of information, data precision is decreased automatically in interdependent stages, ultimately to degrade the data in an irreversible way (Van Heerde, 2010: 150). Van Heerde points towards five different possible ways of implementing data degradation techniques: service-oriented, ability-oriented, user-oriented, upgradable, and external data degradation. User-oriented data degradation is the only one putting the citizen in charge of the process of data retention, all other options imply built-in system functionality. With the exception of external data degradation, the techniques discussed by Van Heerde all rely on a single point of interaction. 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. However elegant this method of system development may seem, the fundamental problem remains, that the system architect must be able to predict all possibilities for privacy breaches that will, can, may or even might ensue during the entire life-time of a system. Given the rapid developments in information technology, this level of overview must be classified as highly improbable. Besides that, the result of Privacy-by-Architecture will be that the user has no say whatsoever about his or her personal information, which will be seen as a very unwelcome outcome by a majority of citizens (Spiekermann and Cranor, 2009: 77).

"Notice and choice" is central to Privacy-by-Policy, the second concept distinguished by Spiekermann and Cranor. This approach aims at providing information to users about the information processes the organisation executes, in the form of privacy policies, notices and notifications. Moreover, users themselves are allowed to make proper choices on the primary and secondary uses of their data by the organization. These "choice and consent" centred policies are common practice in information services today. Spiekermann and Cranor (2009) point out that multiple problems are connected with this approach. The most obvious being the application of notoriously incomprehensible and extremely extensive privacy policy documents that are close to illegible to the vast majority of users. It is, however, the most popular privacy-approach to date, because it does not interfere with business models that rely on extensive use of personal information.

7. Providing privacy in an era of "cloud" and "big data"

The massive application of supply chain and ERP systems, leading to information integration across organizations (Srinivasan and Dey, 2014), turned data silos into data nodes in networked environments. Further stimulated by the sharing of information through social media (McAfee, 2006), data ownership can hardly be claimed anymore. In networked environments the problem of privacy compliance thus gets more complicated, as private information is exposed to covert acquisitions without the owner's knowledge or consent. It is predicted that users will increasingly be victim of significant privacy breaches that are intractable, costly to repair and increase the reluctance to engage (Oyomno et al, 2009). 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 remains. For those purposes Van Heerde (2010) puts forward external data degradation, but does not elaborate on this solution. In his opinion, external data degradation is achieved by binding degradation policies to data, and make network components degradation-aware. Network switches and routers can check the policy attached to each data item, and block or even remove a 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 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 protection in networked environments, necessary because of the emergence of smart cities, that can only be achieved if massive amounts of information about individual citizens, their movements and their lives are harvested and processed. In smart cities, information-driven technologies are being applied to enhance effectivity and efficiency of transportation, energy, sustainability, e-governance, economy and communications, with many new, as yet inconceivable services expected to be developed in the near future. The privacy-corrosive potential of these "smart city" technologies is acknowledge, and Martinez-Ballesté et al list technologies available today to mitigate these negative effects: pseudonymizers, RFID privacy techniques, privacy-aware video surveillance, private information retrieval techniques, location masking, cloaking, anonymization, statistical disclosure control and privacy-preserving data mining. In addition, a likewise promising concept has been developed in Van Blarkom et al (2003), who provide seven principles of PET: limitation in the collection of personal data; identification, authentication, authorisation; standard techniques used for privacy protection; pseudo-identity; encryption; biometrics; and auditability. These principles can be associated with the Common Criteria (CC) for Information Technology Security Evaluation (ISO/IEC 15408, 2009). A final method worth mentioning to protect users' privacy is making use of a trusted third party, operating as an "identity protector" (IDP), which allows for privacy-aware fulfillment of the IVC. Borking (2010) shows the workings of this IDP in the technological environment of an ICT, by which he provides an overview of privacy-aware processing of data.
Table 2 shows our combination of both PET principles and CC with the technologies mentioned.

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	anonymisation cloaking location masking private information retrieval techniques privacy-aware video surveillance privacy-preserving data mining statistical disclosure control
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

Although the technologies are available, and in most cases even in place, many of those technologies are not applied to protect the privacy of citizens (Martinez-Ballesté et al, 2013). This conclusion is in line with Mayer-Schönberger and Cukier (2013), who state that 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. Mayer-Schönberger and Cukier (2013) propose privacy assessments, backed up by real authority that may impose the rule of privacy law on the organizations reaping the (huge) benefits of Big Data analysis. The assessments' workings revolve around a formal assessment, that offers tangible benefits to service providers: 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. 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. As neither Spiekermann and Cranor (2009) nor Monreale et al (2014) give any guarantee that PET (especially in Smart City and Big Data environments) will save citizen's privacy, it is possible that audits are the only methodology left that might work.

8. Discussion: will it work?

Service providers are not completely 'free' in their actions. The environment in which they operate is changing rapidly, because of massive transformation of business models. Since the breakthrough of social media services, more emphasis has been laid on the exploitation of personal information of system users. But at the same time, social media users provide information about people in their personal environment, thereby unwittingly disclosing information that may be of a highly sensitive nature. The use of cloud environments and predictive analytics undo the privacy protection that PET aim to provide. Service providers require personalisation of services to meet users' demands, and this makes return on investment in cyberspace utterly dependent on harvesting and processing huge amounts of personal data. Sensitive information is instrumental to the success of the internet companies. Without the obligation for users to give up their informational privacy, few current business models would remain profitable. Privacy rules and regulations pose a serious threat to the business models of internet companies like Google, Apple, Microsoft and Amazon, whose accumulated billions of dollars make them powerful forces to be reckoned with.

The emphasis on ICT as the solution to possible privacy issues, however, forgoes the notion that this may not solve the entire problem, as social and cultural aspects are inextricably intertwined in the privacy experience of users. Given the conditional and personal factors that defy modelling privacy-enhancing services at a sufficiently detailed level, reinstating some form of negotiation regarding consent to information processing in cloud environments is an idea worth pursuing.

Privacy-aware information management forms a major problem for all parties involved: citizens, information processing organizations and legislators. With the movement from 'ownership-oriented' ICTs to service-oriented 'cloud' environments, finding the right entity that is able to solve privacy issues has become close to impossible. PET allow for legal and technological aspects to be relatively well-attended, but can do so only in isolated parts of the IVC. In real life situations, responsibility rests for some part on assignable actors like the user and the recipient, but may also be shared between parties. Having applied privacy-by-design or privacy-by-architecture procedures and methods does therefore not cover the subject sufficiently and completely. This may be due to the fact that development methods by definition cannot address the inextricable key aspect of privacy, that is found in the sense of control individual subjects have over who may or may not access information about themselves. Looking at the meaning of the term in the social and cultural environment that the subject lives in, it becomes clear that real-life-interactions regarding the sharing of privacy-sensitive information defy proper modelling, because of the highly contextual and volatile character that define social interactions. It may well be concluded that privacy is so inconclusive and implicit that 'a computer' may not be able to grasp the subtleties that are connected to the concept in real life. That may exonerate system developers, by asserting that developing a system that will solve all possible privacy problems by technology alone, is not feasible given the current state of technology.

Maybe we should stop talking about "privacy-aware" systems, as the best we seem to be able to do is developing "access-aware" or "privacy-audited" systems, most of which have not left the proof of concept stage yet. Facing the fact of the current unlevel playing field might be a first step towards true "informed consent", instead of yielding to the "blind trust" systems that are giving citizens almost no control on who may access, process and disclose sensitive and confidential personal information.

9. Conclusion and further research

In our view "Intuitive" privacy and ICT privacy policies are clearly at odds, but legislators, service providers and the general public concur in valuing privacy as essential to acceptance of information technology-based services. Providing proper privacy to citizens is therefore no matter of small concern. Making clear to all parties involved that their respective responsibilities cannot be delegated to ICTs is crucial. Governmental, service providers' and citizens' concerns should be properly addressed to retain the privacy levels that form the essence of civil liberties and maintain freedom in society. To create a truly privacy-aware IVC, a holistic approach is needed in finding methods to shift control over information back towards the citizen. Taking the IVC from a citizen's perspective as a starting point would allow for a first step towards a true impact analysis of ICTs on what is considered a building block of free societies.

References

Allen, A.L. (2011) *Unpopular privacy. What must we hide?*, Oxford: Oxford University Press.

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

Coles-Kemp, L. and Kani-Zabihi, E. (2010) 'On-line privacy and consent: a dialogue, not a monologue', *Proceedings of NSPW'10*, Concord (MA), pp. 95-105

Conly, S. (2013) *Against autonomy. Justifying coercive paternalism*, Cambridge: Cambridge University Press.

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

Dawes, S.S. (2008) 'Governance in the information age: a research framework for an uncertain future' *Proceedings of the 9th annual international digital government research conference, Montreal,* pp. 290-297

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].
Available: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:NOT (23 May 2015).

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].
Available: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31997L0066:EN:HTML (23 May 2015).

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].
Available: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML (23 May 2015).

EU (2004) *Privacy Incorperated Software Agent: Building a privacy guardian for the electronic age*, [Online].
Available: http://cordis.europa.eu/projects/rcn/53640_en.html (23 May 2015).

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

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

Hofstetter, Y (2014), *Sie wissen alles. Wie intelligente Maschinen in unser Leben eindringen und warum wir für unsere Freiheit kämpfen müssen*, München: C. Bertelsmann Verlag,

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

Kosinski, M., Stillwell, D. and 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.

Kost, M. and Freytag, J-C. (2012) 'Privacy analysis using ontologies', *CODASPY 12 Proceedings of the Second ACM Conference on Data and Application Security and Privacy,* ACM, pp. 205-216

Kwecka, Z., Buchanan, W., Schafer, B. and 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. and 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.*, New York: Basic Books.

Lopez, B. (2010) 'Privacy rights in the age of street view', *SIGCAS Computers and society*, vol. 40, no. 4, pp. 62-69

Martínez-Ballesté, A., Pérez-Martínez, P. A., and 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., and Cukier, K. (2013) *Big data. A revolution that will transform how we live, work and think*, London: John Murray.

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*, New York: PublicAffairs.

Monreale, A, Rinzivillo, S., Pratesi, F., Giannotti F. and Pedreschi, D. (2014) 'Privacy by design in big data analytics and social mining', *EPJ Data Science*, vol. 10, pp. 1-26

Oyomno, W., Jäppinen, P. and Kerttula, E. (2009) 'Privacy implications of context-aware services', *Proceedings of COMSWARE 2009, june 16-19* Dublin, Ireland, pp. 1-9

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., and 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., and Klobučar, T. (2003) 'Privacy-enhancing technologies - approaches and development', *Computer Standards & Interfaces*, vol. 25,nNo. 2, pp. 147-158.

Solove, D.J. (2004) *The Digital Person. Technology and Privacy in the Information Age*, New York, London: New York University Press.

Solove, D.J., Rotenberg, M., and Schwartz, P.M. (2006) *Privacy, information, and technology*, New York: Aspen Publishers Online.

Siegel, E. (2013) *Predictive analytics. The power to predict who will click, buy, lie or die*, Hoboken (NJ): Wiley.

Spiekermann, S. and Cranor, L.F. (2009) 'Engineering privacy', *IEEE Transactions on software engineering*, vol. 35, no. 1, pp. 67-82

Sprenger, P. (1999) 'Sun on Privacy: "Get Over It"', *Wired,* [online].
Available: http://archive.wired.com/politics/law/news/1999/01/17538 (23 May 2015)

Srinivasan, M. and 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*, Berlin-Heidelberg: Springer, 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., and 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. and Poulymenakou, A. (eds), *Organizational information systems in the context of globalization*, Deventer: Kluwer, pp. 355-370.

Van Blarkom, G.W., Borking, J.J, and Olk, J.G.J. (2003) *Handbook of privacy and privacy-enhancing technologies. The case of Intelligent Software Agents*, The Hague: Privacy Incorporated Software Agent (PISA) Consortium.

Van Bussel, G.J. (2012a) *Archiving should be just like an Apple™ en acht andere, nuttige (?) stellingen*, Amsterdam: Amsterdam University Press.

Van Bussel, G.J. (2012b) "Reconstructing the Past for Organizational Accountability", *The Electronic Journal of Information Systems Evaluation,* vol. 15, no. 1, pp. 127-137.

Van Heerde, H. (2010) *Privacy-aware data management by means of data degradation. Making private data less sensitive over time*, Enschede: CTIT Twente University

Warren, S. and Brandeis, L.D. (1890) 'The right to privacy', *Harvard law review*, vol. 4, no. 5, pp. 193-197.

Wang, P. and 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., and 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.