Embedding Privacy in ICT architectures. The Citizen as Public Stakeholder in ICT Architecture Development

John van de Pas[1] en Geert Jan van Bussel[2]

[1] Senior Researcher, Saxion University of Applied Sciences, Media Technology Design
[2] Professor Digital Archiving & Compliance, HvA Amsterdam University of Applied Sciences, School of Economics and Management

'The public feel that they have lost control over their data and that there are enforcement and application problems'. (Hallinan, Friedewald, & McCarthy, 2012)

Introduction

According to Johnson & Grandison (2007), failure to safeguard privacy of users of services provided by private and governmental organisations, leaves individuals with the risk of exposure to a number of undesirable effects of information processing. Loss of control over information about a person may lead to fraud, identity theft, reputation damage, and may cause psychosocial consequences ranging from mild irritation, unease, social exclusion, physical harm or even, in extreme cases, death. Although pooh-poohed upon by some opinion leaders from search engine and ICT industries for over a decade (Sprenger, 1999; Esguerra, 2009), the debate in the wake of events like the tragic case of Amanda Todd could be interpreted as supporting a case for proper attention to citizens' privacy. Truth be told, for a balanced discussion on privacy in the age of Facebook one should not turn towards the social media environment that seems to hail any new development in big data analysis and profiling-based marketing as a breathtaking innovation. If the myopic view of technology pundits is put aside, a remarkably lively debate on privacy and related issues may be discerned in both media and scientific communities alike. A quick keyword search on 'privacy', limited to the years 2000-2015, yields huge numbers of publications: Worldcat lists 19,240; Sciencedirect 52,566, IEEE explore 71,684 and Google scholar a staggering 1,880,000. This makes clear that privacy is still a concept considered relevant by both the general public and academic and professional audiences. Quite impressive for a subject area that has been declared 'dead'.

Do Engineers value privacy?

In this paper we will be exploring the way the protection of privacy, viewed from the perspective of the citizen is addressed properly by system developers in the development process of new information systems, to be able to seek an answer to the question whether privacy protection is available for the unsuspecting individual that uses information sys-

tems in modern western society. Although the answer to the question might seem a no-brainer, in our research so far (Van de Pas & Van Bussel, 2014; Van de Pas, Van Bussel, Veenstra, & Jorna, 2015) we found that in the context of the subject of information gathering techniques, the perspective of the individual is quite underexposed in the debate on privacy. We will not delve into the various techniques available to provide privacy by privacy enhancing technologies, by policies, or by privacy impact analyses. We will analyze the underlying structures of the information technology application, that might in our view, be at least partly responsible for the state of affairs regarding the possibility of maintaining a private sphere as an individual in networked societies. We will analyze two available instruments in an attempt to determine if the privacy promised by their application will materialize.

Notwithstanding the fact that individuals freely disclose information of a sometimes highly personal nature on social media, regularly discussions in mainstream media and on the Internet are fuelled by changes in privacy policies, implemented by aggregators of information. In an overview article in Computer Law & Security Review Halinan et al (2012) present their research into the perceptions of European citizens on data protection. 'Surveys generally distinguished between state actors and private organisations. It is interesting to note that 'other individuals', whilst mentioned tangentially in relation to other questions such as those related to ID theft, were not seen as a body or entities worth of specific consideration. This is particularly interesting considering the key role played by the individual in the online environment and the individual nature of many perceived threats'. After their exploration of opinions and attitudes of both the general public and organisations regarding privacy issues they reach as an overall conclusion: 'The public feel that they have lost control over their data and that there are enforcement and application problems' (Hallinan, Friedewald, & McCarthy, 2012, p. 271).

Given the clearly expressed concern of the general public that it is losing control, it is instrumental to take a look at those responsible for programming the systems that seem to draw away control from the citizen towards public and private organisations. System engineers are developing and maintaining the systems that have had such a corroding effect on privacy of citizens. In our conversations with engineers it has become clear that they themselves show the same differing opinions on the issues of privacy protection as the general population does. Some express sincere concerns about the way information systems are negeatively effecting privacy, because they perceive themselves also as a citizen being objectified in information processing systems. Others convey some concern, but apply a pragmatic stance without which they probably would not be able to do their job; probably accepting that they are just a cog in the machine without much influence on the general course of things. And there is also a group of really unconcerned engineers, actively pushing the boundaries of total information technology control to the limits, enjoying every minute of their job. Engineers as a group are much like ordinary people, judging

from their privacy concerns. The 'privacy types' seem to be mirrored in group classifications in the general population as reported by Lopez (2010) and Spiekermann & Cranor (2009). Based on surveys on privacy concerns, people can be divided in three groups: unconcerned (approximately 25% of the population), a larger group of pragmatists, who do care but in daily practice realise that denial of service is the punishment for refusal to give up private information, and finally a relatively small group of fundamentalists/paranoids, that show strong concern for their privacy and act accordingly by not using information services or trying to obfuscate their identity whilst using them. The 75% is not further divided, but it may be assumed that the pragmatists form the largest group by far, and only a small minority can be dubbed 'fundamentalist/paranoid'. But engineers are not completely free to do as they deem necessary in their daily development routines.

Spiekermann & Cranor scrutinize the state of affairs on 'privacy engineering'. Basically they point out the structure applied to engineering information systems. They show that ample methodology is available for system development to allow engineers to take proper stock of privacy issues. Two main ways of engineering privacy are available to the engineer: privacy by policy, and privacy by architecture. A subset of privacy by architecture is privacy by design, and in this toolbox Privacy Enhancing Technologies (PET) are available for application.

On a conceptual level, therefore, one could defend the position that the loss of control that the public experiences is not unavoidable. Control of his/her data to the citizen could be restored, if available methods and techniques were applied. The question if privacy engineering may lead to systems respecting privacy of citizens cannot be full heartedly answered positively, however. Privacy engineering attempts in the process of system conception are shown to be subjugated to the applied principles of engineering. First and foremost, the primary goal driving an engineering project must be the business case, that does not put a bonus on restraint in exploitation of privacy sensitive information. The opposite is true. An engineer not respecting the business case of his employer is not considered doing a good job. As business cases usually are part of the preliminary stages of system development, other concerns than business concerns play little part in the engineering stage of system development. The organisational and shareholder interests are being given utmost importance, at the cost of other stakeholders.

Most business cases in information technology projects revolve around furthering efficiency, efficacy, or both. This means that other concerns than those of an economical or process management nature in the engineering stage are almost impossible to implement. The business case is defined in an earlier stage in which the organisation commissioning the system has investigated the rationale of investment in a new system. During that process of system definition other concerns might well be addressed. If they are not expressed in that preliminary stage, they can't properly be inserted in a later stage of system

development, because the impact of those concerns is usually of a disturbing character. Moreover, collecting sets of rules and constraints the engineering process has to adhere to are defined in an earlier stage of the development process: the architecting stage. In the following, we will look at that stage to see if there are any opportunities to look beyond the narrow scope of return on investment.

System Architecture

System development typically starts with a definition of system functionalities to be delivered in the context of the organisation that commissions the system. Numerous development methods have been adapted in the long history of automated system development, but in every single method attention has to be paid to the parties that are going to use and are going to be subjected to the workings of a system. For ad-hoc system development these methods are generally loosely applied, but for development projects with higher impact (and hence higher financial, judicial, or functional breakdown risks) more effort is put into risk analysis and prevention. In environments where controlled risk-taking is essential, some form of system architecture is usually applied in order to give proper definitions as to the scope and reach of the system to be developed.

System architecture is a set of methods and prescriptions to make proper system development feasible. As such, architecture is normative in the sense that it describes practices that are good, versus practices deemed bad. ISO/IEEE/IEC (ISO & IEEE, 2011) states that for a correct architecture description three aspects have to be in order: [1] there should be a complete list of stakeholders that have an interest in the system, [2] those stakeholders should be able to express their concerns, and [3] the expressed stakeholder concerns should be translated into explicit viewpoints that should be taken into account in the blueprints for the system to be developed. Following this orientation phase, the system architect describes functional and non-functional system requirements, thereby defining the actions that should and should not be available in the exploitation of the system during its life cycle.

The architecting process may be represented as in Figure 1.

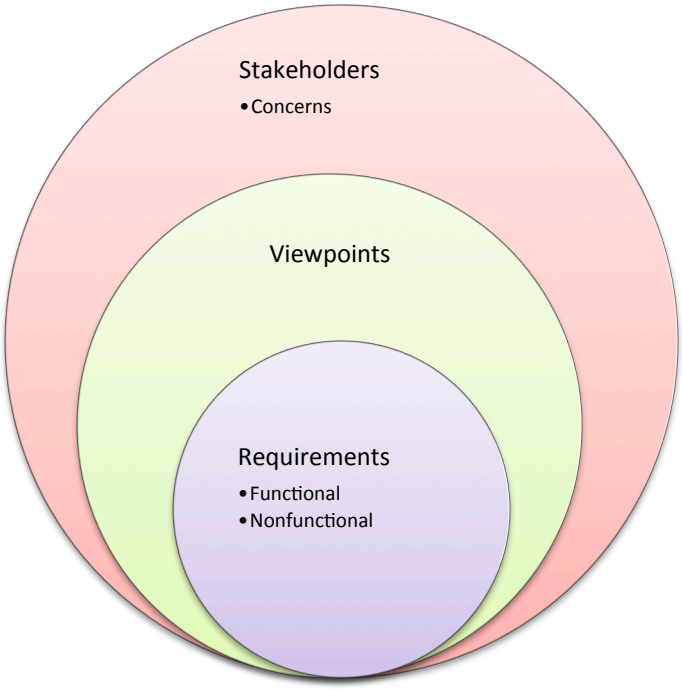

Figure 1: Graphical representation of defining stages during system architecting

The viewpoints lead to a set of well-described rules and constraints in the form of system requirements, on which the system developers base their translation of the concepts and ideas into actual system functionality in the working system that interacts with the environment. By far the most attention in literature on architecting is paid to the transformation of viewpoints into system functionalities.

Figure 1 shows the reductionist processes that inevitably result from the information modelling methods that are applied during system development. Modelling is by definition reductionist, as reliable functionality should be predictable, and therefore must abstain from real life ambiguities that lead to unpredictability in the outcomes of a systems workings on its environment.

The architecting process is operated in an environment, where decisions are made about the invited stakeholders' concerns. Our hypothesis is, that the stakeholder selection process that precedes the architecting process as described above, has been transformed from an open environment in which stakeholders are understood to include individuals in society at large, to a closed environment in which only a very specific set of stakeholders is allowed to have influence on the architecting process. This way, other voices and concerns are effectively silenced. In the proces, stakeholders that do have concerns are excluded and are defined irrelevant to the development process.

This is due to two separate, but interacting developments that may be summed up in short by the sentence 'you get what you pay for'.

No difference of opinion exists on the basic economic principle that first and foremost, exploitable functionality is emphasized in any development project. In leading project methodologies like PRINCE, the business case is given a central role, and business case evaluation is translated in constant attention to the underlying financial feasibility of the process. Testing Return on Investment is deemed to be an essential ongoing process in any project, and system development projects are no exception to that general rule. Without a business case, no allocation of resources is viable or feasible, so no system development will take place. And as functional system requirements relate directly to the uses and functionalities of the business case, it is clear that most attention is given to these aspects of system development. System developers should pursue those system aspects that lead to the realisation of the functional requirements. If the business case was the only relevant factor defining a project, the case would be open and shut. But in real life, next to functional requirements, there is always a certain amount of non-functional requirements to be realized. Based upon our own experiences in system development environments, we think there might be some justification to speculate that there is some sort of 'natural tendency' in the process to give prevalence to functional over non-functional requirements. We have noticed a certain engineering gratification in paying near exclusive attention to action-based 'positive' system functionalities, as opposed to the tedious and often complex modelling of restraint, labelled as 'negative' system functionalities. Privacy neatly fits the non-functional aspects, and they are among the first functionalities to be sacrificed if budgets are under pressure – which they are by definition. Most engineers find pleasure in modelling a system that works effects. It is not considered gratifying to develop system parts with the express purpose not to perform certain functions. So for most engineers the 'non-functional requirements' are contrary to the fun part of programming. And so it is not surprising that non-functional requirements are in general undervalued in the development of a project, and engineers are tempted to dub non-functional' as a synonym to 'irrelevant' . Especially in the case of elusive concepts like 'privacy' or 'societal impact', the lack of proper and all-encompassing, non-ambiguous definitions, makes for a tendency to declare the more 'tricky' non-functional requirements as irrelevant, or to bypass them completely under the assumption that no evil will be done by ignoring the issues.

Putting pressure on Return on Investment has led to a situation that the business case has been given paramount attention in system development processes, and this leads to an central role of the shareholder, at the cost of other stakeholders. So the stakeholder in system architecture is nowadays 'the shareholder, who benefits from the systems workings' and not 'the stakeholders, including society in which our system will have its effects'. In an overview article on stakeholder theory Moriarty (2014) has shown that this shift in general stakeholder definition in organisations has led to reduction of the stakes to near

exclusive attention to the Return on Investment viewpoint, by which all other stakeholders, including personnel, customers, or, in the case of governmental organisations, citizens dependent upon them for legal services for which there is no alternative, and society at large are more or less neglected. If the stakeholder is not invited to express his concerns in the early stages of system architecting, his concerns will not be translated in non-functional requirements, among which is system restraint on processing privacy-sensitive information without explicit consent of the individual concerned.

It is relevant to determine whether there are checks and balances that may prevent abuse of stakeholder power in the system development process. This is due to the fact that the role of the general public as a stakeholder might be defined, but may never be able to surpass the prevalence of the business case. Checks and balances are important for the prerogative of return on investment will remain a trump card that overrules all other requirements, especially those that are non-functional.

Regulations, privacy authorities and privacy assessments are put forward to remedy those dynamics in system development projects. We will conclude our research by looking at both these aspects, and see whether they put proper constraints on organisations if their business case is built upon harvesting information gathered by privacy infringements.

New regulations

The notion that citizens might turn away from information services they perceive as manipulative and only furthering the interests of the public-private partnerships exploiting them reducing their customers-citizens to objects-to-be-exploited, is not lost on governing bodies like the European Union. In an article on the possible application of citizens' privacy rights to legal persons, Van der Sloot sums up the upcoming transformation of privacy regulations and data protection. He states that in the proposed regime the citizen will be provided with more rights, so that informed consent to processing of information will be available by transparency of information processing organisations. The 'subject' will be allowed to get insight in storage periods, the right to get insight in the data processed, and the right to be forgotten. This means that 'subjects' may not only be informed, but can also demand correction of incorrect information about themselves, and even removal if information storage is deemed inappropriate from the point of view of the individual. The era of information harvesting without limits and no repercussions to information processing organisations might very well become a thing of the past, once this General Data Protection Regulation is passed. Maybe, just maybe, 'big brother' might be stopped (Sloot, 2015, p. 35).

It remains to be seen if, and when, these improved regulations will be put in practice. Given the resistance by the great information multinationals, their reluctance to apply rulings

by judges in different countries, and the interests that both marketers and security industries share with the repressive parts of governments and political spheres, it may prove very difficult to stem the tide of total transparency. Multi-billion dollar lobby budgets and a tendency to frame any discussion about protecting citizens' privacy in terms of security versus freedom for terrorists does not spell any good to the case for protection of the private sphere of the individual. For that is what privacy boils down to: is the citizen granted any autonomy in decision making, information retrieval and discretion in information dispersal. Is the private sphere to be respected by putting control over disclosure in the hands of the subject, than rules and regulations should be in place to grant the individual citizen those rights, enforced by real authority (Mayer-Schönberger & Cukier, 2013). Given the highly unbalanced playing field between the individual citizen and the informational mega-corporations, any attempt at negotiating an information policy that is more in the interest of the citizen, and gives corporate exploitation less of a free hand, is bound to fail.

There are, however, signs that the status quo is challenged. For that we may look at Germany, to our knowledge the only country in Europe that put a stop to Google Street View by legal means, as it protected the rights of German citizens not to be photographed in public space without their consent. Germany's high court has also ruled that the strict German privacy regulations apply to Facebook, notwithstanding the fact that Facebook tried to evade those regulations by stating that their European office is situated in Ireland, and the servers therefore would have to be subject to the much milder rule in that country. This resulted in an explicit exception for German users in Facebook's privacy policies.

On the whole, on a world wide scale, the picture looks pretty grim for privacy as a line of defence of the individual citizen against unsolicited interventions of public-private cooperation, be they openly or covert. Which does not go without notice from experts on computer law, as Bart van der Sloot sums up: 'In conclusion, both with regard to privacy and to data protection, there seems to be a shift from an obligation based doctrine, emphasizing rules of good governance and duties of care, to a rights based model, from a doctrine that aims at safeguarding societal interests, such as the legitimacy of the state (not abusive of its power) and the integrity of data processing systems, to a model that aims at preserving specific individual interests, and then from a doctrine that is aimed at intrinsic limits on the use of power by either the state or the data controller to a model in which the individual interest is increasingly weighed and balanced against the societal interest, such as security and economic welfare. This has had a clear impact on the scope of both the right to privacy and that of data protection'. (Sloot, 2015, pp. 35-36). In our view, the difficulties in grasping the playing field and the actors in the privacy debate, with all their different and opposing interests and concerns, are reflected in the highly complex description that Van der Sloot gives here. It is no easy matter to define privacy protection properly; and therefore implementation of this particular kind of protection into actual systems, is very complex indeed, and possibly even too complex to achieve. But at the same

time, privacy authorities seem to project a certain sense of confidence in being able to provide the same privacy protection we discussed above. For a test case of the effectiveness of the instruments available, we will discuss two instruments: the international norm on Architecture description; and the Privacy Impact Assessment (PIA) quality label.

Discussion: can citizens' privacy be protected by architecture description & PIAs?

There is nothing wrong with ISO/IEE/IEC 42010 (2011) *Systems and software engineering – Architecture description*, and if applied fairly and with an open view on the privacy concerns of the general public, it may very well play an important role in re-instating the citizen as a public stakeholder. The underlying assumption seems to be, that writing down that stakeholders should be selected with proper care and attention to the interests of all parties concerned, makes it a realistic possibility, and that rational organisations act accordingly. Following this line of reasoning, for a rational system architecting process, interests of the general public are meticulously balanced against economic interests of stakeholders, and stakeholders show restraint if confronted with opportunities to earn huge sums of cash by exploitation of privacy-sensitive information of their customers which is not completely within the boundaries of the laws and regulations. Moreover, in this world privacy policies are transparent, private information is never processed without consent, and organisations are eager to abide both letter and intent of privacy laws, and are constantly looking out for ways to show proper respect to individuals' privacy rights. Breaches of privacy are never intentional, always circumstantial, and when prompted by an individual, organisations swiftly better their ways and repair any resulting damages from the infringement on the individuals privacy without any discussion. The citizens' concern is equally important as the businesses' concern, because mutual trust is paramount and based on precise data management that never crosses the lines.

The real world is different, of course. The idea that most organisations will truthfully try to abide by the law, but some will act as 'cowboys', is not lost on authorities, who are constantly looking at ways to keeping the playground safe for all, not letting things slip into an information wild west. Privacy regulations and instalment of Privacy authorities are the result, because some things can clearly not be left to the market alone as they result in highly unbalanced negotiating positions, where the individual citizens' concerns are at risk of being crushed by more powerful entities. Those interventions on behalf of the citizen do not go unnoticed by the information processing industry. Their response to the threat that highly lucrative business models may be halted by laws and law enforcement, lead to some pretty nifty interventions.

According to David Wright, there is 'growing interest in Europe in privacy impact assessment (PIA). UK introduced the first PIA methodology in Europe in 2007, and Ireland follow-

ed in 2010. PIAs provide a way to detect potential privacy problems, take precautions and build tailored safeguards before, not after, the organisation makes heavy investments in the development of a new technology, service or product' (Wright, 2012, p. 54). PIA is defined as 'a methodology for assessing the impacts on privacy of a project, policy, programme, service, product or other initiative and, in consultation with stakeholders, for taking remedial actions as necessary in order to avoid or minimise negative impacts' (Wright, 2012, p. 55). PIA is aimed, to make matters clear, at the interests of stakeholders of an organisation that is about to commit itself to the development process of a new system. Although it is strongly recommended that among the stakeholders the public (Wright, 2012, p. 58) be engaged in the process, and examples from actual PIA projects are mentioned in the article, a warning voice is raised: 'If an organisation tries to 'fix' a consultation by consulting only 'safe' stakeholders, that will go along with its point of view, it actually does itself a disservice, not just by making a sham of the process, but also by not achieving the advantages and benefits of a consultation which is aimed at identifying risks, obtaining fresh information and finding solutions, in other words achieving a 'win-win' result so that everyone benefits' (Wright, 2012, p. 59). This seems to hint at PIA being sort of a blunt instrument, as the repercussions for the organisations 'stacking the deck' seem extremely mild indeed. Next to that, Wright (2012) limits its attention to 'win-win' situations that might exist in the real world. However, for a truly balanced discussion of the beneficial aspects of PIA, we deem it essential to also discuss a win-lose situation. In those situations the real impact of PIA on 'the public' that stands to lose its privacy in those particular instances may be properly assessed. We deem this relevant, as we think it is safe to assume that organisations do not tend to invest in systems that lead to a lose-situation at their end of the bargain. The omission of problematic aspects of the outcomes of this instrument regarding citizens' privacy might just be a chance omission, that should not be given too much attention. But combined with the fact that PIA is developed by the industry themselves, some critical attention may be in order. Critical reading of Wright (2012) leads to some quite insightful aspects as to the underlying purpose of PIA. As Wright (2012, p. 56) writes: 'We assume regulators are likely to be more sympathetic towards organisations that undertake PIA's than those that do not. A PIA is a self- or co-regulatory instrument which may obviate the need for 'hard' law'. Combine this with the information hidden in footnote 7 in the same article, which reads: 'The organisation may not be able to eliminate privacy risks completely, despite its best efforts. Indeed, even after making some noble efforts, a company may decide the *residual risk is worth accepting in view of the benefits the project may deliver* [our emphasis – JP/GJB], and these benefits might be not only to a company's bottom line, but also in a service that's genuinely valued by a wide swathe of society' (Wright, 2012, p. 55). The idea that in the balancing act of interests the individual's rights might rightfully be sacrificed to the larger stakes of benefits to companies bottom line or 'wide swathes of society' seems to be echoed in the new proposed European regulations, that we saw voiced by Van der Sloot. In our view it is worth investigating whether PIA's are

being implemented as instruments that in fact are mainly geared towards the privacy-as-a-risk factor from the point of view of public-private organisations, meanwhile spreading a sense of security by uncritical observers. Attempts at derailing regulations by lobbying and implementing blunt instruments is a common technique to prevent authority with teeth being installed. Concluding, a PIA communicates that the organisation takes privacy serious, unless there is money to be made, obviously.

In our view this particular instance of privacy impact assessment leads to an at least partially misleading 'label'. We do not try to answer the question here whether this is a question of linguistic spin, or inherent to the definition of the instrument, which was possibly not meant to protect citizen privacy in the first place. The latter leaves us with the puzzling question why the label is dubbed privacy impact assessment, and not privacy risk assessment, which covers the actual workings of the instrument itself in a much more concise way. But perhaps it is part of a broader movement in which assessments and audits are put forward in lieu of real interventions. Audits in themselves do not lead to actions that repair privacy breaches, as Mayer-Schonberger and Cukier put forward in their discussion of privacy audits as an instrument for protecting citizens' private sphere. They state that privacy protection authority 'without teeth' does not force organisations to be privacy-law-abiding. The purely administrative approach that auditing actually is, in its final analysis, can only be turned into an effective instrument if reported wrongdoings are followed by justice that is swift and harsh.

Panopticon Redux?

Jeremy Bentham, champion of permanent supervision as an instrument in a civilizing offensive for the benefit of both overseers and the overseen, points towards the trait that is inextricably bound up with a system that places persons in what he calls a *panopticon*. 'Another very important advantage, whatever purposes the plan may be applied to, particularly where it is applied to the severest and most coercive purposes, is that the under keepers or inspectors, the servants and subordinates of every kind, will be under the same irresistible control with respect to the head keeper or inspector, as the prisoners or other persons to be governed are with respect to them' (Bentham, 1791, p. 15). The inspector of the inspection-house is under the same observation as the prisoner – and the head inspector is able to see for himself the circumstances that the prisoners are living in, thereby making even the inspectors, his subordinates, transparent to his piercing gaze. The essence of the civilizing offensive Bentham proposed to further by means of building the inspection-house is not inspection – it is the total transparency that is achieved by the design of it that makes it into the panopticon. All are scrutinized at all times, by unseen inspectors that are inspected accordingly in turn. According to Bentham, the total

transparency achieved by his design served as a satisfactory answer to 'the most puzzling of political questions – quis custodiet ipsos custodies?' (Bentham, 1791, p. 15).

In 220 years not much seems to have changed in this regard, as transparency is still put forward in the debate as the most promising solution to provide safety to society. However, transparency does not seem to work both ways. According to some researchers (Vrhovec, Hovelja, Vavpotič, & Krisper, 2015), citizens seem to be under growing obligation to be completely transparent to organisations, while organisations may decide for themselves whether information is made available to the citizens. Given the fierce debate on transparency and governance, driven to the edge by whistle blowers like Assange, Snowden and Manning, there seems to be ample ground for drawing the conclusion that the autonomous striking of a proper balance between confidentiality and transparency for individual citizens is rapidly becoming impossible in the age of networked information structures.

Bibliografie

Antunes, G., Barateiro, J., Becker, C., Borbinha, J., & Vieira, R. (2011). Modeling contextual concerns in enterprise architecture. *2011 15th IEEE International enterprise distributed object computing conference workshops* (pp. 3-10). IEEE.

Bentham, J. (1791). *Panopticon; or, The Inspection-House* (Dodo Press, 2008 ed.). s.l.

Esguerra, R. (2009, december 10). *Google CEO Eric Schmidt Dismisses the Importance of Privacy.* Retrieved june 24, 2015, from EFF: Electronic Frontier Foundation. Defending your rights in the digital world: https://www.eff.org/deeplinks/2009/12/google-ceo-eric-schmidt-dismisses-privacy

Hallinan, D., Friedewald, M., & McCarthy, P. (2012). Citizens' perception of data protection and privacy in Europe. *Computer law & security review, 28*, 263-272.

Heesch, U. v., Avgeriou, P., & Hilliard, R. (2012). Forces on architecture decisions - a viewpoint. *2012 Joint working conference on software architecture & 6th European conference on software architecture* (pp. 101-110). IEEE.

Hilliard, R., Malavolta, I., Muccini, H., & Pelliccione, P. (2012). On the composition and reuse of viewpoints across architecture frameworks. *2012 Joint working conference on software architecture & 6th European conference on software architecture*, (pp. 131-140).

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 & IEEE. (2011). ISO/IEC/IEEE 42010:2011(E) Sytems and software engineering - Architecture description. Geneva, CH & New York, USA: International Organisation for Standardisation & Institute of Electrical and Electronics Engineers, Inc.

Johnson, C., & Grandison, T. (2007). Compliance with data protection laws using Hippocratic Database active enforcement and auditing. *IBM systems journal, 2007*(Vol. 46 No. 2), 255-264.

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

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

Moriarty, J. (2014). The connection between stakeholder theory and stakeholder democracy: an excavation and defense. *Business & Society, 53*(6), 820-852.

Nord, R., Clements, P., Emery, D., & Hilliard, R. (2009). Reviewing architecture documents using question sets. *Joint Working IEEE/IFIP Conference on Software Architecture 2009 & European Conference on Software Architecture 2009* (pp. 325-328). IEEE.

Pas, J. v., & Bussel, G.-J. v. (2014). 'Privacy lost - and Found?' Some Aspects of Regaining Citizens' Privacy by Means of PET in the age of 'Big Data'. *ECIME, 8th European Conference on Information Systems Management and Evaluation.* Ghent, Belgium.

Pas, J. v., Bussel, G. v., Veenstra, M., & Jorna, F. (2015). Digital Data and the City. An exploration of the building blocks of a Smart City Architecture. *Digital Information Strategies: from applications and content to libraries and people*.

Sloot, B. v. (2015). Do privacy and data protection rules apply to legal persons and should they? A proposal for a two-tiered system. *Computer law & security review, 31*, 26-45.

Spiekermann, S., & Cranor, L. (2009). Engineering privacy. *IEEE Transactions on software engineering, Vol. 35, No. 1*, 67-82.

Sprenger, P. (1999). *SUN on Privacy: "Get Over It"*. Retrieved may 23, 2015, from Wired: http://archive.wired.com/politics/law/news/1999/01/17538

Stach, C., & Mitschang, B. (2014). Design and implementation of the privacy management platform. *2014 IEEE 15th international conference on mobile data management* (pp. 69-72). IEEE.

Thierer, A. (2013). Privacy, Security, and Human Dignity in the Digital Age: The Pursuit of Privacy in a World Where Infor-mation Control is Failing. *Harvard Journal on Law & Public Policy, vol. 36*(no. 2), 409-455.

Vrhovec, S., Hovelja, T., Vavpotič, D., & Krisper, M. (2015). Diagnosing organisational risks in software projects: stakeholder resistance. *International journal of project management, 33*, 1262-1273.

Wright, D. (2012). The state of the art in privacy impact assessment. *Computer law & security review, 2012*(28), 54-61.