Journal of
Social and Administrative Sciences
www.kspjournals.org
Volume 7 March 2020 Issue 1

Attitudes towards privacy by design in e-government: Views from the trenches

By Anton Antonov GERUNOV †

Abstract. In light of increasing public pressure and strict regulation, issues of information security and privacy gain prominence in the e-government domain. A promising approach to ensure data protection is to embrace the Privacy by Design principles and practices in the public sector but this remains a major challenge for practitioners. This article leverages in-depth interviews with e-government stakeholders in Bulgaria to explore their opinions and preferences on data protection issues, thus outlining the main drivers and barriers for Privacy by Design implementations. The key insight is that increasing citizen demands and regulatory oversight engender a change in privacy thinking that defies the current status quo. Limited understanding, scarcity of best practices, legacy systems and insufficient financial and administrative capacity seem to be the main implementation obstacles.
Keywords. Privacy by Design, e-government, data protection, personal data.
JEL. C80, H10, H11.

1. Introduction

Recent decades have seen an increasing trend of process digitization that has produced an ever-increasing amount of data, now commonly characterized as "big data" (McAfee *et al.*, 2012; Davenport *et al.*, 2012). This trend is ubiquitous not only in the private sector but maybe even more so in the public sector as the processes for rolling out e-government solutions intensify data collection and processing (Kim *et al.*, 2014). A large proportion of this data needs to be personal or personally-identifiable data to adequately carry out the needs of key e-government applications ranging from e-health, through e-justice, e-procurement, all the way into e-democracy and e-participation (Veit & Huntgeburth, 2014). Naturally the question of privacy and data protection looms large with such vast amounts of highly sensitive data. A possible approach for increasing personal data protection is to introduce privacy controls from the very onset of system development, and to introduce privacy-enhancing technological and organizational methods in every phase of the information system lifecycle.

This approach is known as Privacy by Design (PbD) and has been initially introduced by Ontario's Information Commissioner (Cavoukian *et al.*, 2010; Cavoukian, 2011; Cavoukian, 2012a) and then taken up by privacy

† Sofia University, St. Kliment Ohridski, 125 Tsarigarsko Shosse Blvd. 1113, Sofia, Bulgaria.
☎. + ✉. gerunov@uni-sofia.bg

researchers and academics. This approach is also mandatory in the EU and is clearly enshrined in GDPR's Article 25, which mandates privacy by default and by design. However, the people tasked to engineer and apply privacy principles are reluctant to do so (Bednar *et al.*, 2019), which proses a major problem for implementing data protection in e-government projects. This articles aims to explore the apprehension of privacy by relevant stakeholders and outline the drivers and barriers to PbD in order to overcome personal and organizational resistance to its implementation. To this end we leverage in-depth qualitative interview with e-government stakeholders to elicit their attitudes and opinions about the needs and implementations of privacy by design in a realistic setting.

2. Literature review

The very concept of privacy, let alone its implementation by design, is challenging to define and operationalize (Langheinrich, 2001; Williams, 2009). For the purposes of this research we follow the definition of privacy as being "the right of individuals to control access or interference by others into their private affairs" (Brey, 2007). The concept of Privacy by Design is the organizational and technological manifestation of this right when it comes to designing and operating information systems. It is thus defined by Spiekermann-Hoff (2012) as "a pro-active engineering and management approach that is committed to selectively and sustainably minimize information systems' privacy risks through technical and governance controls".

2.1. Privacy by design principles

It is often more efficient to apply privacy principles at the design stage of a given IT artefact to minimize rework, increase artefact efficiency, improve security, and optimize cost; and the PbD principles aim to support this (Williams, 2009; Schaar, 2010, Hustinx, 2010). The foundational principles of PbD were defined as early as the 1990s and then successively refined by one of their first proponents – A. Cavoukian (Cavoukian *et al*, 2010; Cavoukian, 2011; Cavoukian, 2012a). They aim to provide the framework for system design that respects users privacy. The principles are as follows (ibid.):

1. *Proactive not reactive; preventative not remedial* – this principle corresponds to the need for proactive problem identification and solution definition that prevents a privacy issue from occurring in the first place.
2. *Privacy as the default setting* – it focuses on the need to have privacy-preserving defaults so that data subject's information is protected irrespective of whether they take action.
3. *Privacy embedded into design* – privacy needs to be introduced into the SDLC in such a way that the system functions as privately preserving by default, or even cannot function if privacy is not preserved.

4. *Full functionality* – positive-sum, not zero-sum – this principle underlines the need for creative design solutions that simultaneously satisfy business requirements and protect user privacy.

5. *End-to-end* security – full lifecycle protection – this calls for privacy controls along every phase of the data processing cycle – from collection through processing to deletion.

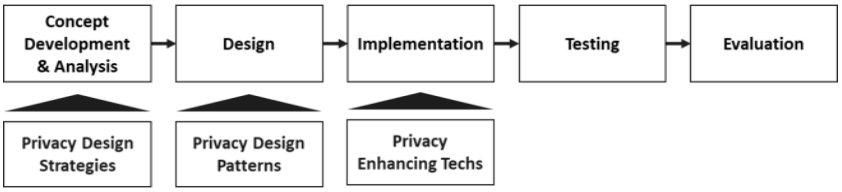
6. *Visibility and transparency – keep it open* – this underlines the need for accountability on the part of the data controller.

7. *Respect for user privacy – keep it user-centric* – the principles illuminates the imperative to focus on user's needs for information protection during system design.

While these principles are popularized under the heading PbD, they largely overlap with other information protection and privacy standards are guidelines. Most notably, PbD principles share a lot in common with OECD's Fair Information Practices (FIPs) and both US-American and European legislation (e.g. the Directive 95/46/EC to be superseded by the GDPR). This large overlap provides for a growing consensus on what privacy principles can form the basis for design decisions (Cavoukian, 2012a; D'Acquisto *et al.*, 2015; Rubinstein & Good, 2013; Cronk, 2018). There are, however, particular implementation challenges in e-government applications due to issues of will and capacity (Ebrahim & Irani, 2005), as well as possible distrust on the part of the general public (Almagwashi *et al.*, 2014).

2.2. Privacy implementation strategies and applications

Despite the growing agreement on the broad and overarching privacy principles, their practical implementation into systems development remains unclear (Spiekermann-Hoff, 2012; Dennedy *et al.*, 2014; Cronk, 2018). There seems to be little agreement as to a standardized methodology, tools, or design patterns that uniquely embody those principles (ibid.). As a way to overcome this, Hoepman and colleagues offer a number of privacy design strategies that include concrete system features (design tactics) aiming at improving privacy-friendliness (Hoepman, 2014; Colesky *et al.*, 2016). While some of these activities are more on the technological side (e.g. PETs), others fall on the organizational or social side (Klitou, 2014). Depending on the phase of the SDLC different privacy activities are appropriate (see Graph 1). During concept development and analysis, the architect may use generic privacy design strategies (e.g. minimize data collection or obscure data). During design, privacy design patterns can be utilized (e.g. distribute PII processing or feed only aggregated data). Finally, the implementation phase calls for privacy enhancing technologies (PETs) such as encryption.



Graph 1. *Software Development Life Cycle with Privacy Enhancement,*
Source: Hoepman (2014).

Hoepman (2014) thus proposes eight broad strategies to aid system development, and Colesky *et al.,* (2016) leverage a review of around 100 privacy patterns and fit those strategies using extant literature, as follows:

- *Minimize* focuses on collecting as little personal information as possible, thus decreasing the impact of privacy risks and streamlining protection. This can be done by using the patterns exclude (excluding data from processing, e.g. blacklisting), select (process only relevant subsets of data, e.g. partial identification), strip (remove sensitive fields, e.g. strip metadata), or destroy (delete data, e.g. limited data retention functionality).
- *Hide* prevents data exposure. The relevant patterns here are restrict (prevent unauthorized access, e.g. access control functionality), mix (random processing, e.g. mix networks), obfuscate (prevent readability, e.g. through encryption), dissociate (remove correlation between pieces of data, e.g. delayed routing).
- *Separate* prevents correlating data by isolating or distributing processing. The patterns here are isolate (independent processing of personal data, e.g. through physical privacy zones) and distribute (distributing data in different tables or databases, e.g. through privacy-sensitive architecture).
- *Abstract* limits details on personal data by processing only aggregated information. The two patterns for this strategy are summarize (extract and process commonalities, e.g. data abstraction through statistical summaries or correlations) and group (allocating into common categories, e.g. dynamic location granularity).
- *Inform* provides abundant information to data subject on all relevant aspects of processing. The patterns here are supply (provide information, e.g. privacy policy display), notify (proactively alerting data subjects of developments, e.g. data breach notification), and explain (improve accessibility of information through e.g. privacy icons).
- *Control* gives power to the data subject to decide on their data being processed. The patterns here are consent (only processing data after agreement, e.g. by obtaining explicit consent), choose (allowing choice for what data is processed, e.g. by discouraging blanket strategies), update (allowing persons to keep their data accurate, e.g. by providing reasonable level of control through web interfaces), and

retract (complete removal of personal data at request, e.g. invisible mode).

- *Enforce* ensures commitment for creating and maintaining policies, processes and controls. It consists of three patterns – create (acknowledge value of privacy and create corresponding policies, e.g. fair information practices), maintain (consider privacy in support and update, and maintain and improve data protection processes, e.g. through appropriate privacy feedback), and uphold (treat PII as an asset, e.g. through distributed usage control).
- *Demonstrate* provides evidence for the data processing activities. The patterns for this strategy are log (tracking and ensuring data integrity, e.g. through non-repudiation technologies), audit (monitor and investigate daily activities, e.g. through privacy audit trail), and report (analyse and review collected performance information, e.g. through procedures for building trust and credibility).

In terms of the practical implementation of the PbD principles, those strategies are common and accepted in practice, either through explicit reference to them, or implicitly via privacy implementation programs. Their applications range from implementing privacy by design for connectivity data (Aad & Niemi, 2010), emergency management information systems (Buscher et al., 2013), the cross-border flow of health information (Di Iorio *et al.*, 2012), sensitive health data (Kum & Ahalt, 2013; Kum *et al.*, 2019), protecting the data in a dynamic carpooling system (Friginal *et al.*, 2014), preserving student data (Hoel & Chen, 2016), social network activity (Islam & Iannela, 2011), gathering open source intelligence (Koops *et al.*, 2013), population data (Pencarrick Herztman *et al.*, 2012), big data analytics and social mining (Monreale *et al.*, 2014; Rajamäki & Simola, 2019), and others.

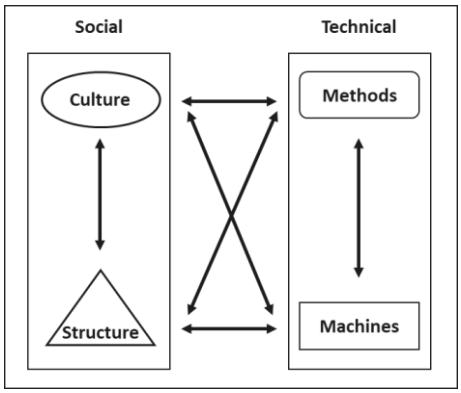
The analysis of relevant literature revealed that most PbD implementations to date stem from the public-sector information systems domain. This is natural as e-government applications regularly process extremely large quantities of PII (sometimes data on the entire nation) and often contain sensitive data to be used for key social and security purposes.

The key problem in the proliferation of PbD strategies lies in their practical application. While there is clear growth trend in research interest and a proliferation of reusable design patterns and elements (Caiza *et al.*, 2019), this is hardly enough to close the research gap in the privacy implementation area. This issue is largely underscored by the fact that engineers that are called upon to implement privacy-enhancing features do not perceive this as their responsibility, have limited control and autonomy and are generally reluctant to engage with legal issues (Bednar *et al.*, 2019).

2.3. Importance of organization, perceptions and norms for applications

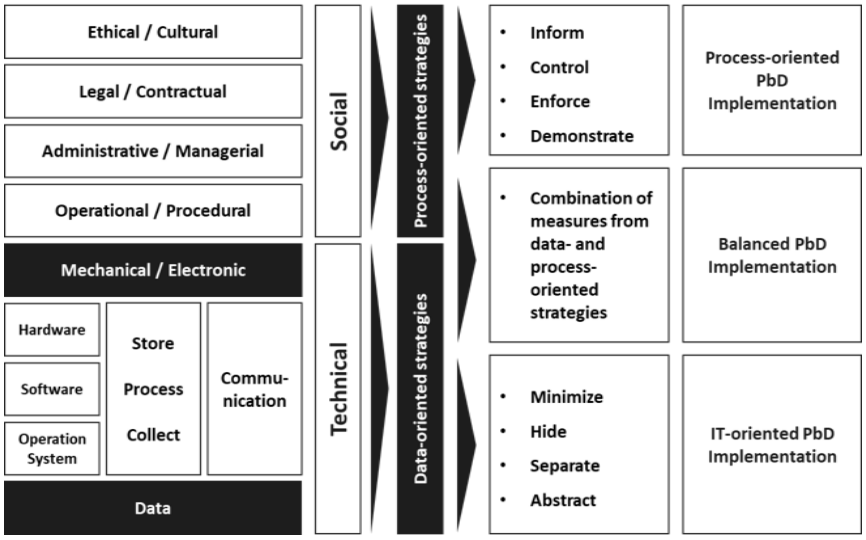
The wide range of possible approaches for implementing Privacy by Design in information systems development means that system architects

and their business stakeholders have numerous alternative design options they can choose from that can all reach this end result. It is therefore of interest to see what the drivers of specific design preferences are, and what perceptions different stakeholders have regarding the "right" way to achieve PbD. A starting point into this analysis is recognizing that a given IT artefact consists of both technical aspects but is also embedded into the organizational structure and its efficiency hinges upon social norms, behaviors and acceptance (Ebrahim & Irani, 2005). A suitable theoretical lens to study the privacy preferences are the socio-technical approaches (see e.g. Carew & Stapleton, 2005). Kowalski (1994) distinguishes two aspects of the social and two aspects of the technical dimension that can serve as analytical lenses for better understanding the operation of IT artefacts. Those are namely the structure and culture of the organization, and the machines and their operation methods, respectively (Graph 2).



Graph 2. *Socio-technical Model (STM),*
Source: Kowalski, (1994: p.10)

The STM can serve as a foundation to conceptualize security and privacy decision within a realistic organizational framework – something particularly pertinent in an e-government setting. Kowalski (1994) proposes a Security by Consensus (SBC) framework than can also be expanded to understand relevant privacy aspects. Again, it divides the aspects of the IT artefact operations into social (cultural, legal, administrative, operational) and technical (hardware, software, OS, communications, data) ones. This model can be fruitfully utilized to understand privacy issues as well. The type of approaches, measures and controls for building security and privacy tend to be similar, and the ideal types of privacy-enhancing strategies (Hoepman, 2014; Colesky *et al.*, 2016) can be intuitively mapped onto this model (Graph 3).



Graph 3. *Mapping between Security by Consensus Model and Privacy-Enhancing Strategies.*
Source: Kowalski (1994), Hoepman (2014), mapping by author.

Hoepman's (2014) data-oriented strategies overwhelmingly coincide with the technical aspects of the STM/SBC models, and his process-oriented strategies largely parallel the social aspects. Thus leveraging mostly process-oriented strategies, the system architect will reach a Process-oriented PbD implementation. Relying predominantly on technical aspects, the architect will tend to devise an IT-oriented PbD implementation, and if measures are drawn from both aspects – a balanced PbD implementation can be obtained. This conceptualization is also consistent with relevant practical security standards and thus has the benefit of easier recognition and acceptability. We note that the socio-technical aspects are easy to map to the ISO security and other relevant standards (Tarimo, 2006; Ma *et al.*, 2008; Rost & Bock, 2011), and that this approach can be fruitfully used to understand the e-government domain (Ihmouda *et al.*, 2014). The utility of such socio-technical models lies both in their ability to guide and elucidate design choices in the protection of data subject privacy as well as the ability to avoid unintended consequences of IS operations (Harrison *et al*, 2007; Sahama *et al.*, 2013). Further, the horizontal focus on privacy that these methodologies engender is similar in vein to aspect-oriented programming whereby horizontal concerns (aspects) figure prominently to optimize certain design choices (Magableh & AlSobeh, 2018). Summarizing, the privacy mapping onto an STM enables one to systematically study stakeholder preferences regarding a PbD implementation and elucidate which privacy features are more salient and desirable within an e-government setting.

2. Methodology

The interview approach is suitable for this kind of research as it is able to collect a large amount of rich qualitative data, indicative of respondents'

experiences and perceptions, and this is particularly true for more in-depth interview (Gill *et al.*, 2008; Denscombe, 2010, p.173). Since there seems to be little consensus on, or sometimes even awareness of, data privacy principles and implementation possibilities, a personal interview may serve to clarify the concepts, elucidate informants, and draw a nuanced perspective of the issues under research. Experts are to share their thoughts and opinions on what constitutes best practice in privacy design, and more importantly, why this should be the case. This can be achieved during in-depth semi-structured interviews with relevant stakeholders that are aware of both technological possibilities and legal requirements for e-government applications. The current research goal is very much focused on eliciting preference drivers regarding the real-life implementation of a given concept (privacy) within the SDLC that are later to be used in the design phase.

The relatively limited number of privacy professionals and their geographic dispersion necessitates a purposive sampling strategy. Purposive sampling is defined as "the deliberate choice of a participant due to the qualities the participant possesses" (Etikan *et al.*, 2016). The researcher's personal contacts with e-government experts (public officials, consultants, and vendors) allows for the selection of a number of relevant informants that are willing to participate in this research in exchange for the right to use the results produced in their daily work. In particular, 10 relevant stakeholders were contacted via e-mail or phone regarding this study, and of them 6 agreed to participate. The participants form a diverse group featuring both career civil service officials in charge of implementing security and privacy in e-government, as well as consultants, vendors, and academics. The informants are as follows:

- *Informant 1* – a high-ranking civil servant, currently at the SEGA with more than 10 years of experience in public administration and e-government
- *Informant 2* – an e-government vendor and Managing Director at a company developing electronic health solutions with more than ten years of experience in information security
- *Informant 3* – an IT security consultant and e-government advisor, working on privacy and data protection implementations in Bulgaria and the EU for more than ten years
- *Informant 4* – an academic, researcher and consultant with experience in both the private sector and as a political appointee in the e-government domain with more than twenty years of experience
- *Informant 5* – a mid-level civil servant, currently project leader at the SEGA with more than fifteen years of experience in e-government
- *Informant 6* – an academic and researcher who switched to academia from the public sector after more than five years of experience with e-government.

Before the beginning of the first round of interviews all of them were presented the informed consent form and were informed of the goal, scope, and implications of the study. Once consent was given, informants were asked their opinions and preferences about PbD implementations, allowing them to volunteer clarifying questions. They informants a vast amount of rich unstructured information regarding their opinions, experiences and preferences in respect to data protection. This data is was qualitative in nature and called for a more sophisticated approach to analysis. Thematic analysis is a suitable approach in such cases at it allows for the identification, analysis, and reporting of patterns in qualitative data (Braun & Clarke, 2006). Thematic analysis begins by assigning initial codes to meaningful chunks of the text (word, sentences, paragraphs) and then proceeds by iteratively improving their clarity and precision (Burnard *et al.*, 2008; Saldana, 2015). Those codes are then grouped into larger caterogies for similar codes, and finally those categories are summarized in overarching themes (ibid.). Braun & Clarke (2006) propose a six-step methodology for applying thematic analysis, consisting of the following phases: familiarization with the data, generation of initial codes, search for themes, themes review, naming and further definition of themes, and reporting. This approach is similar across other authors with only slight variations (Burnard *et al.*, 2008; de Casterle *et al.*, 2012) and is the one used for analyzing informant responses.

4. Results and discussion

The large amount of qualitative data resulting from the in-depth interviews with e-government stakeholders was subjected to a detailed thematic analysis. It revealed three major themes that gain significant salience in the e-government domain – the New Privacy Reality, Current State-of-the-Art, and Implementation Challenges.

The *New Privacy Reality* theme deals with the tectonic shift in terms of privacy and data protection that has come as a results of changing citizen perceptions and increased regulatory pressures.

"Data protection is important, and this importance is constantly increasing." – Informant 2

The category Privacy Culture deals with the importance of protecting data but also recognizes the need to change organizational cultures and practices. Informants were also conscious of the wide and divergent views on privacy held across different cultures and jurisdictions. The two codes recurring most often deal with the need to engender new ways of thinking about personal data protection and to focus on educating the wider public of the potential benefits. Geopolitical differences and the operational aspects of introducing Privacy by Design into the standard Software Development Lifecycle for e-government are also salient topics on the minds of the respondents.

"This topic [of privacy] requires a new way of thinking, necessitates new models that are difficult to reconcile with current administrative practice." – Informant 1

Privacy enablers were a second major category that outline the incentives for privacy – the value of information, the sanctity of the personal space, the enabling technologies, and the avoidance of harm. This category deals with major drivers and techniques for introducing privacy-conscious information systems in the public sector.

Table 1. *Thematic Analysis Results: Main themes, categories and initial codes*

Themes	Categories	Total	Initial Codes	Mentions
The New Privacy Reality	Privacy Culture	29	New ways of thinking	7
			Educate public of the benefits	6
			Geopolitical differences	5
			Operational aspects	4
			High importance of data protection	3
			Are data needed?	2
			Difficulty of changing mentality	1
			Currency	1
	Privacy Enablers	28	Value of information	5
			Personal space	4
			Technical measures	4
			Possible harm to people	4
			State collects sensitive data	3
			Protection from surveillance	2
			Use existing solutions	2
			Privacy ROI	2
			Public sector accountability as driver	1
			Possibility for wrong decisions	1
	Legal Obligations and Controls	27	Legal requirements	18
			Compliance checklist	4
			Need for legal changes	3
			Security checklists	1
			Sanctions not effective	1
	Risks and Potential Harm	14	Excessive surveillance	4
			Human-related risks	3
			Insight into consumers	3
			Data compromise through social engineering	2
			E-services delivered without data protection	1
			Limited freedoms	1
Current State-of-the-Art	Privacy-enhancing Processes	41	Preliminary security analysis	9
			New business processes for data protection	7
			Adherence to good practice	7
			Logging activity	6
			Need for stricter control on projects	4
			Organizational measures more important	2
			Auditing	2
			Need for detailed project requirements	1
			Need for data flow inventory	1
			Need for continuous improvement	1
			Physical security	1
	Privacy-	30	Access controls	11

	enhancing Technologies		Encryption	5
			Technical measures more important	4
			Secure components	3
			Data protection in transit	3
			Authentication	2
			Data protection at rest	2
Implementation Challenges	Knowledge and Competences	11	Lack of understanding	5
			Limited and expensive knowledge for PbD	3
			Lack of knowledge in private sector	3
	Privacy Barriers	23	Insufficient financial resources	4
			Legacy systems	3
			Technology limitations	2
			Trust issues	2
			No pressure from citizens	2
			Lack of clarity in regulations	2
			Limited understanding	2
			Problems with processes	1
			No PbD process	1
			No pressure from business	1
			Insufficient legal requirements	1
			Lack of concrete good practice	1
			Focus on material assets	1
	Privacy Requirements	21	Need for administrative capacity	7
			Need for best practices	5
			Need for training	2
			Need for balanced approach	2
			Standards	2
			Need for IT solutions	2
			Need for high-level support	1

Those fears are also mirrored in the category Risks and Potential Harms where informants focus on the possible negative consequences of privacy breaches, most notably the risks of excessive surveillance. The characteristics of the collected information neatly mesh together with Orwellian fears of a surveillance society – the possible harms through state monitoring of sensitive data figure prominently among almost all respondents' concerns. There are even two mentions of potentially leveraging citizen personal data for social engineering initiatives.

"People need to be trained and informed that Big Brother may be watching…" – Informant 6

Finally, the category Legal Obligations and Controls shows how the changes in social needs and perceptions get codified and thus reflected in e-government operations. It is worth noting that Legal Requirements for Privacy is the single most often mentioned consideration when it comes to data protection implementations and was universally discussed by all the informants on multiple occasions. Legal or security checklists is another topic mentioned by multiple informants as a concrete compliance tool.

The second identified broad theme was the *Current State-of-the-Art,* where experts focused on privacy-enhancing processes and technologies. The theme Privacy-enhancing Processes focuses on four main

organizational measures to achieve a higher level of privacy: conducting a preliminary security analysis, introduce specific data protection processes, employ good practices and standards (e.g. ISO 27001) and use of extensive logging of user activity for legal and forensics purposes. The need for stricter control over e-government projects also surfaces as a distinct concern. On the technological side, the category Privacy-enhancing Technologies (PETs) underlines two major approaches that our respondents would rely on for protecting data – granular access control to personal data and data encryption. There also seems to a bias in informants with technical background to prefer technical to organizational measures.

"We need to have maximum encryption, wherever possible. And to control access both at the application layer and the database layer." – Informant 3

"We can use technical measures to solve at least some of the process problems." – Informant 5

The procurement of secure components receives relatively less attention. On the other hand legislation such as the GDPR and practices surrounding it seem to color the thinking of the interviewees as they explicitly references "data protection at rest" and "data protection in transit" which are not technologies but rather generic labels for activities to ensure privacy.

The third uncovered theme was Implementation Challenges and it deals with the concrete roadblocks for implementing a privacy solution in the field of e-government. The first category Knowledge and Competences revolves around the insufficient understanding of privacy, as well as limited know-how about its implementation. Unexpectedly, informants report this not only for the public but also for the private sector. The major current implementation blockers (category Privacy Barriers) are the insufficient financial resources and the existing legacy systems that cannot easily accommodate date protection additions.

"Older systems were created with little regard to privacy. Only when a problem appears do we realize that we need to consider security as well." – Informant 4

Respondents also mention the environmental complexity surrounding such projects, mentioning unclear regulatory framework, trust issues, lack of sufficient pressure from citizens and business, as well as process problems. The final category here is the Privacy Requirements where informants report a need for greater administrative capacity and the introduction of, and reliance upon, clear practices and standards to implementing privacy in e-government information systems. Surprisingly, over the interviews there was only a single mention of the need for high level support which may be interpreted that the topic of introducing privacy is relatively uncontroversial.

The overall results of the analysis shed light on a few important PbD implementation aspects. First, the context has changed towards a new reality that makes privacy necessary and widely accepted. This necessitates large involvement on the part of stakeholders that can both improve the

solution, educate the public of project benefits, and ensure wider buy-in (Axelsson *et al.*, 2010; Goldkuhl & Perjons, 2014). Second, the main measures for baking in privacy in the e-government information systems are rather classic. On the organizational side they are preliminary security analysis, adherence to good practices, introducing new data protection processes. On the technological side they are mostly reliance on granular access control, extensive logging and monitoring, and data encryption at rest and in transit. These measures also seem to be in line with the recommendations of existing legislation such as the GDPR. Finally, the challenges for introducing privacy by design in the public administration IT systems revolve around problems with human and financial resources, legacy systems, technological limitations, and challenges with transforming operations. This insight replicates existing literature about general issues of information security in e-government. This leads to the conclusion that while Privacy by Design may be a relatively new concern in e-government, its implementation will likely be plagued by the existing and familiar problems of implementing general information security solutions.

5. Conclusion

The concept of Privacy by Design (PbD) is the organizational and technological manifestation of the human right to privacy when it comes to designing and operating information systems. Despite the growing agreement on the broad and overarching privacy principles, their practical implementation into systems development remains unclear. There seems to be little agreement as to a standardized methodology, tools, or design patterns that uniquely embody those principles. This is in some part due to the engineers reluctance to fully embrace and implement those privacy principles in the systems they design and develop (Bednar *et al.*, 2019), which is a problem of particular salience when it comes to e-government applications. If the introduction of privacy-enhancing e-government solutions is to be accelerated, then it is of paramount importance to explore the attitudes and opinions of relevant stakeholders regarding PbD principles and their real-life implications.

To this end, we conducted a detailed qualitative analysis of the problem domain by conducting in-depth semi-structured interviews with six relevant e-government stakeholders. The resultant thematic analysis underlines the major drivers, barriers, and requirements when it comes to privacy implementations in the public sector. Most notably, respondents outline that they perceive a change in mentality brought about the new privacy reality, driven jointly by regulations and public perceptions. Participants also underlined the current state-of-the-art in data protection as a set of important tools to overcome privacy implementation challenges. While some of those challenges are familiar from e-government and information security literature, others are novel and interesting, such as the trust issues, the lack of clarity in privacy regulations, and the currently insufficient good practices in protecting personal data. These results

underline the pivotal importance of empowering e-government professionals.

References

Aad, I., & Niemi, V. (2010). NRC data collection and the privacy by design principles. *Proc. of PhoneSense*, pp.41-45.

Almagwashi, H., Tawileh, A., & Gray, A. (2014). Citizens' perception towards preserving privacy in e-government services: a cross-sectional study. In: *Proceedings of the 8th International Conference on Theory and Practice of Electronic Governance* (pp.24-27). ACM.

Bednar, K., Spiekermann, S., & Langheinrich, M. (2019). Engineering privacy by design: Are engineers ready to live up to the challenge?. *The Information Society*, 35(3), 122-142. 10.1080/01972243.2019.1583296

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2), 77-101.

Brey, P. (2007). Ethical aspects of information security and privacy. *In* M. Petković & W. Jonker (Eds.), *Security, Privacy, and Trust in Modern Data Management*, (pp.21-36), Springer Berlin Heidelberg.

Burnard, P., Gill, P., Stewart, K., Treasure, E., & Chadwick., B. (2008). Analysing and presenting qualitative data. *British Dental Journal*, 204(8), 429-432. 10.1038/sj.bdj.2008.292

Buscher, M. Wood, L. & Perng, S.Y. (2013). Privacy, security, liberty: informing the design of emergency management information systems. In: *10th International Conference on Information Systems for Crisis Response and Management*. KIT, Karlsruhe.

Caiza, J.C., Martín, Y.S., Guamán, D.S., Del Alamo, J.M., & Yelmo, J.C. (2019). Reusable elements for the systematic design of privacy-friendly information systems: A mapping study. *IEEE Access*, 7, 66512-66535. 10.1109/ACCESS.2019.2918003

Carew, P.J., & Stapleton, L. (2005). Towards a privacy framework for information systems development. In: *Information Systems Development* (pp.77-88). Springer, Boston, MA.

Cavoukian, A. (2011). Privacy by design in law, policy and practice. *A white paper for regulators, decision-makers and policy-makers*. [Retrieved from].

Cavoukian, A. (2012a). Privacy by Desing. *IEEE Technology and Society Magazine*, 4, 18-19. 10.1109/MTS.2012.2225459

Cavoukian, A. (2012b). Privacy by design and the emerging personal data ecosystem. *Privacy By Design*. Canada: Ontario Information Commissioner. [Retrieved from].

Cavoukian, A., Taylor, S., & Abrams, M.E. (2010). Privacy by design: Essential for organizational accountability and strong business practices. *Identity in the Information Society*, 3(2), 405-413. doi. 10.1007/s12394-010-0053-z

Colesky, M., Hoepman, J.H., & Hillen, C. (2016). A critical analysis of privacy design strategies. In: *Security and Privacy Workshops (SPW), 2016 IEEE* (pp.33-40). IEEE.

Cronk, J. (2018). *Strategic Privacy by Design*. US: International Association of Privacy Professionals (IAPP).

D'Acquisto, G., Domingo-Ferrer, J., Kikiras, P., Torra, V., de Montjoye, Y.A., & Bourka, A. (2015). Privacy by design in big data: an overview of privacy enhancing technologies in the era of big data analytics. arXiv preprint arXiv:1512.06000. [Retrieved from].

de Casterle, B.D., Gastmans, C., Bryon, E. & Denier, Y., (2012). QUAGOL: A guide for qualitative data analysis. *International Journal of Nursing Studies*, 49(3), 360-371. 10.1016/j.ijnurstu.2011.09.012

Dennedy, M.F., Fox, J. & Finneran, T. (2014). *The Privacy Engineer's Manifesto: Getting from Policy to Code to QA to Value*. US: Apress Media LLC.

Denscombe, M. (2014). *The Good Research Guide: For Small-Scale Social Research Projects*. McGraw-Hill Education.

Di Iorio, C.T., Carinci, F., Brillante, M., Azzopardi, J., Beck, P., Bratina, N., ... & Jecht, M. (2012). Cross-border flow of health information: is 'privacy by design'enough? Privacy performance assessment in EUBIROD. *The European Journal of Public Health*, 23(2), 247-253. doi. 10.1093/eurpub/cks043

Ebrahim, Z., & Irani, Z. (2005). E-government adoption: architecture and barriers. *Business Process Management Journal*, 11(5), 589-611. 10.1108/14637150510619902

Etikan, I., Musa, S.A., & Alkassim, R. S. (2016). Comparison of convenience sampling and purposive sampling. *American Journal of Theoretical and Applied Statistics*, 5(1), 1-4.

Friginal, J., Gambs, S., Guiochet, J., & Killijian, M.O. (2014). Towards privacy-driven design of a dynamic carpooling system. *Pervasive and Mobile Computing*, 14(1), 71-82. 10.1016/j.pmcj.2014.05.009

Gill, P., Stewart, K., Treasure, E., & Chadwick, B. (2008). Methods of data collection in qualitative research: interviews and focus groups. *British Dental Journal*, 204(6), 291-295. 10.1038/bdj.2008.192

Harrison, M.I., Koppel, R., & Bar-Lev, S. (2007). Unintended consequences of information technologies in health care—an interactive sociotechnical analysis. *Journal of the American Medical Informatics Association*, 14(5), 542-549. doi. 10.1197/jamia.M2384

Hoel, T., & Chen, W. (2016). Privacy-driven design of learning analytics applications–exploring the design space of solutions for data sharing and interoperability. *Journal of Learning Analytics*, 3(1), 139-158. 10.18608/jla.2016.31.9

Hoepman, J.H. (2014). Privacy design strategies. In: *IFIP International Information Security Conference* (pp.446-459). Springer, Berlin, Heidelberg.

Hustinx, P. (2010). Privacy by design: Delivering the promises. *Identity in the Information Society*, 3(2), 253-255. 10.1007/s12394-010-0061-z

Ihmouda, R., & Alwi, N.H.M. (2014). E-government development models: Review of social-technical security aspects. *International conference on Intelligent Systems, Data Mining and Information Technology* (ICIDIT'2014), April 21-22, 2014 Bangkok, Thailand.

Islam, M.B., & Iannella, R. (2011). Privacy by design: Does it matter for social networks?. In: *IFIP PrimeLife International Summer School on Privacy and Identity Management for Life* (pp.207-220). Springer, Berlin, Heidelberg.

Kim, G.H., Trimi, S., & Chung, J.H. (2014). Big-data applications in the government sector. *Communications of the ACM*, 57(3), 78-85. 10.1145/2500873

Klitou, D. (2014). Privacy-invading technologies and privacy by design. *Safeguarding Privacy, Liberty and Security in the 21st Century*, *25*. Springer.

Koops, B.J., Hoepman, J.H., & Leenes, R. (2013). Open-source intelligence and privacy by design. *Computer Law & Security Review*, 29(6), 676-688. 10.1016/j.clsr.2013.09.005

Kowalski, S. (1994). *IT Insecurity: A Multi-Discipline Inquiry*. Department of Computer and System Sciences, University of Stockholm and Royal Institute of Technology, Sweden.

Kum, H.C., & Ahalt, S. (2013). Privacy-by-design: Understanding data access models for secondary data. *AMIA Summits on Translational Science Proceedings*, *2013*, pp.126-130.

Kum, H.C., Ragan, E.D., Ilangovan, G., Ramezani, M., Li, Q., & Schmit, C. (2019). Enhancing privacy through an interactive on-demand incremental information disclosure interface: applying privacy-by-design to record linkage. In *Fifteenth Symposium on Usable Privacy and Security {SOUPS}* 2019. [Retrieved from].

Langheinrich, M. (2001). Privacy by design—principles of privacy-aware ubiquitous systems. In: *International conference on Ubiquitous Computing* (pp.273-291). Springer, Berlin, Heidelberg.

Ma, Q., Johnston, A.C., & Pearson, J.M. (2008). Information security management objectives and practices: a parsimonious framework. *Information Management & Computer Security*, 16(3), 251-270. 10.1108/09685220810893207

Magableh, A.A., & Al Sobeh, A.M. (2018). Securing Software Development Stages Using Aspect-Orientation Concepts. *International Journal of Software Engineering & Applications (IJSEA)*, 9(6), 57-71.

McAfee, A., Brynjolfsson, E., & Davenport, T.H. (2012). Big data: the management revolution. *Harvard Business Review*, 90(10), 60-68.

Monreale, A., Rinzivillo, S., Pratesi, F., Giannotti, F., & Pedreschi, D. (2014). Privacy-by-design in big data analytics and social mining. *EPJ Data Science*, 3(1), 10. doi. 10.1140/epjds/s13688-014-0010-4

Pencarrick Hertzman, C., Meagher, N., & McGrail, K.M. (2013). Privacy by Design at Population Data BC: a case study describing the technical, administrative, and physical controls for privacy-sensitive secondary use of personal information for research in the public interest. *Journal of the American Medical Informatics Association*, 20(1), 25-28. doi. 10.1136/amiajnl-2012-001011

Rajamäki, J., & Simola, J. (2019). How to apply privacy by design in OSINT and big data analytics?. In *ECCWS 2019 18th European Conference on Cyber Warfare and Security* (p.364). Academic Conferences and publishing limited.

Rost, M., & Bock, K. (2011). Privacy by design and the new protection goals. *DuD, January*.

Rubinstein, I.S., & Good, N. (2013). Privacy by design: A counterfactual analysis of Google and Facebook privacy incidents. *Berkeley Tech. LJ*, 28, 1333-1413.

Sahama, T., Simpson, L., & Lane, B. (2013, October). Security and Privacy in eHealth: Is it possible?. In: *e-Health Networking, Applications & Services (Healthcom), 2013 IEEE 15th International Conference on* (pp.249-253). IEEE.

Saldaña, J. (2015). *The Coding Manual for Qualitative Researchers*. Sage.

Schaar, P. (2010). Privacy by design. *Identity in the Information Society*, 3(2), 267-274. 10.1007/s12394-010-0055-x

Spiekermann-Hoff, S. (2012). The Challenges of Privacy by Design. *Communications of the ACM (CACM)*, 55(7). 34-37. 10.1145/2209249.2209263

Tarimo, C. N. (2006). *ICT Security Readiness Checklist for Developing Countries: A Social-Technical Approach*. Department of Computer and System Sciences, University of Stockholm and Royal Institute of Technology, Sweden.

van Zoonen, L. (2016). Privacy concerns in smart cities. *Government Information Quarterly*, 33(3), 472-480. 10.1016/j.giq.2016.06.004

Veit, D., & Huntgeburth, J. (2014). Foundations of digital government. *Leading and Managing in the Digital Era*, *158*.

Williams, M.A. (2009). Privacy management, the law & business strategies: A case for privacy driven design. In: *Computational Science and Engineering, 2009. CSE'09. International Conference on*. Vol. 3, pp.60-67. IEEE.