PREAMBLE

The information on this page is used to assign your paper to the right track. It will not be part of your final, camera-ready version of the paper.

Please answer the following.

Track. *Indicate the track to which you are submitting the paper, based on the list in the ISCRAM 2015 Call for Papers. If you do not have a specific track in mind, indicate "Open Track".*

Type of review. *Indicate which of the following*

X Insight Paper reviewed with respect to practical relevance and applicability

Type of paper. *Indicate which of the following*

X Short paper presenting work in earlier stages, outlining and discussing concepts and methods and presenting first results (2,000-3,500 words)
Target acceptance rate: > 60 %

Contribution of the paper. *This paper gives an overview of observations made while undertaking the Privacy Impact Assessment (PIA) on a large EU- funded project to develop cloud-based emergency response technology. It provides a wider overview of the PIA process itself, drawing this into practical insights, with the aim of presenting transferable conclusions.*

The role of the privacy impact assessment in IT Innovation in Crises: An Example

Catherine Easton
Lancaster University
c.easton@lancaster.ac.uk

Monika Buscher
Lancaster University
m.buscher@lancaster.ac.uk

ABSTRACT

Privacy Impact Assessments (PIA) are increasingly used and, in certain jurisdictions legally mandated, in projects to foresee risks to privacy and to plan strategies to avoid these. Once adopted and implemented, the EU's Data Protection Regulation will, in certain circumstances require the need for a PIA. This short paper focuses upon the PIA process in a large, EU-funded project to develop cloud-based disaster response technology. It introduces the project and then gives a background to the PIA process. Insights and observations are then made on how the PIA operates, with the aim of drawing conclusions that can both improve the current project and be transferable to others.

Keywords

Privacy, ethics, PIA, disasters, technology

INTRODUCTION

Privacy Impact Assessment is an important tool for understanding the implications of innovation for privacy. The earlier and the more intensively this concept is embedded in socio-technical innovation processes, the greater the potential for proactively and constructively addressing problematic issues. In this paper we discuss this potential and some successes and difficulties based on first experiences of including PIA in IT innovation in crisis response and management.

The observations are based on two projects:

SecInCoRe (Secure Dynamic Cloud for Information, Communication and Resource Interoperability based on Pan-European Disaster Inventory, 2014 - 2017) is an FP7-funded project with the overarching aim of identifying "data sets, processes, information systems and business models used by first responders and police authorities leading to a dynamic and secure cloud based common information space". This brings together public and private partners across the European Union (EU) to learn from past events and responses and to build upon this learning to develop and design a cloud-based communications system to support disaster response. Within these aims, there is a strong focus on probing ethical, legal and social issues (ELSI) to learn more about the regulatory framework surrounding the technology and guide future development.

The longer running BRIDGE project (Bridging resources and agencies in large-scale emergency management, 2011-2014) has developed prototype systems and middleware to support emergent interoperability (Mendonça et al, 2007) and the flexible assembly of a 'system of systems' for large-scale multi-agency response. It, too, relied on collaborative, public and private research and development with a diverse group of stakeholders.

Building on experiences in the BRIDGE project and related work, this short paper sets out observations on the privacy impact assessment process within the SecInCoRe project with the aim of making recommendations that could be transferable to other similar projects.

DEFINING PIA

There is a variety of definitions of a PIA; an early one was put forward by Stewart (1996) as "a process whereby a conscious and systematic effort is made to assess the privacy impacts of options that may be open in regard to a proposal". In general, a PIA is an assessment of any actual or potential effects that the activity or proposal may have on individual privacy and the ways in which any adverse effects may be mitigated. It is essentially a formalization of internal data protection and privacy processes and amalgamates existing organizational approaches. As such, it is a method of shaping practice and maintains a level of fluidity. Due to this it provides benefits to organizations and to project planning by delivering a framework to enable the improvement of systems and the meeting of external obligations.

The UK Information Commissioner's Office 2014 report on PIA describes it as: "a tool which can help organizations identify the most effective way to comply with their data protection obligations and meet individuals' expectations of privacy" (UK ICO, 2014). A further aim is to better understand variations in the concepts and approaches to privacy protection across different jurisdictions. This is particularly prescient in relation to large pan-European projects such as BRIDGE and SecInCoRe which, while comprising partners from within the area in which EU law is harmonized, may operate in Member States which take differing approaches to the implementation of such provisions.

THE POSITION OF THE PIA

PIAs have been promoted and used across a number of jurisdictions and are mandatory in certain circumstances, such as in relation to Canadian health care projects and in relation to the operation of US' government agencies (Wright and Friedewald, 2013). The position in the EU is affected by an on-going data protection reform spurred by the need to update the 1995 Data Protection Directive in order to ensure that its protections are effective in the face of technological development and increasing global information flows. The proposed General Data Protection Regulation was published in January 2012. Since then it has undergone a series of amendments, had its timetable revised and as of January 2015, the Commission, Parliament and Council are negotiating with an aim of completing the legislative process later in 2015. A key focus of these discussions has been the need to minimize risk (Council of the European Union, 2014). Once the text has been finalized, the majority of the provisions will not come into force for a further two years.

This new wide-ranging piece of legislation will, in its Article 33, make what it terms data protection impact assessments mandatory "where processing operations present specific risks to the rights and freedoms of data subjects". It continues to give further details as to the requirements: "The assessment shall contain at least a general description of the envisaged processing operations, an assessment of the risks to the rights and freedoms of data subjects, the measures envisaged to address the risks, safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation, taking into account the rights and legitimate interests of data subjects and other persons concerned". Wright and Friedewald (2013, p758) suggest that these developments and the regulatory impetus of the EU could lead to the development of an international PIA standard. This, however, would need to be carefully implemented as a lack of strategic roll-out relating to an enforceable PIA standard could lead to its formative aspects being lost and it being considered as another level of constraining bureaucracy.

THE PIA PROCESS IN PRACTICE

There are a number of tools to help organizations carry out a PIA. Wadhwa and Rodrigues (2013) provide an in-depth overview of some of these. The development of such tools is essential to support organizations through this process, but there is a danger that if they are badly designed they can become "mere box-ticking exercises" (Wright and De Hert, 2012 p22). This would clash with the overarching ethos of the PIA as, although fulfilling legal requirements is one of its aims, the PIA process goes much further by focusing on stakeholders, processes, predictions, the changing environment, and mitigation. As a 2007 report states: "Many exercises which are called PIAs are, however, little more than legal compliance checks. To be meaningful, PIAs have to consider privacy risks in a wider framework which takes into account the broader set of community values and expectations about privacy" (Linden Consulting, 2007 pvi).

In this way the PIA is a method of carrying out a wide-ranging evaluation of organizational processes and contexts, attitudes to and awareness of privacy issues, with a particular focus on identifying the on-going needs of a wide range of stakeholders. Key issues need to be identified early in the stages of a project and transferable lessons learned with a focus on finding solutions, which did not necessarily have to be technical, and supporting on-going consultation. The process is, therefore, flexible, responding to the individual character of the organization or project and open to change. In relation to this dynamism, Gary T. Marx (Wright and De Hert, 2012 pxiv) states: "PIA faces the challenge of preventing a particular kind of future which involves new elements. It goes beyond routine audits of compliance with established rules and policies. Since the future has not yet happened, its assessment is forever vulnerable to challenges and doubts". This perceived vulnerability can also be a strength of the process as it guides individuals to revisit and reevaluate their actions and responses as a project or organization evolves.

RELATIONSHIP TO THE ETHICAL IMPACT ASSESSMENT (EIA)

Having set out the PIA as a process that goes beyond a simple compliance exercise there is the need to place it alongside another review methodology; the EIA. This is a newer form of review and was developed mainly in order to address the challenges posed by developing technologies (Harris et al, 2011). An EIA addresses the issue that while practices may comply with relevant laws, particularly in a fast-moving area such as information technology the wider impact of a project may have ethical implications that extend further than the static legal framework. This is especially relevant given the fluid concept of privacy and the potential danger of technology exacerbating existing socio-economic divisions, an observation that has been labelled the "digital divide".

Wright and Friedewald (2013) advocate a fusing of the PIA and EIA processes as, they argue, in the development of new technologies legal and ethical issues are often intertwined and so should be addressed together at the earliest possible stage of a project. They continue to highlight the EU's strong and on-going focus on legal and ethical issues relating to research and development in new technologies, which, they argue will "become an inherent part of European research policy" (Wright and Friedewald, 2013 p764). The ethos of the BRIDGE and SecInCoRe projects is strongly grounded in this approach, with work packages (small sub-projects of the work as a whole) dedicated to monitoring the ethical, legal and social aspects (ESLI) of the research processes and innovations developed in the projects. This strategy goes beyond internal monitoring and, perhaps more usefully, in a wider sense, aims to disseminate findings and observations on these issues to a wider audience in a manner transferable to other projects; the underlying rationale for this short paper.

SECINCORE AND THE PIA PROCESS: DETAILS AND OBSERVATIONS

Within the SecInCore project the ELSI team is responsible for coordinating a work package that connects empirical studies of ethical, legal and social opportunities and challenges as they arise in practice with socio-technical design and innovation efforts. Work is undertaken to ensure that ELSI are addressed proactively across the project as a whole, particularly in relation to the development of technology. After attempts to fuse PIA and EIA in response to Wright and Friedewald's (2013) suggestion failed as this created too confusing a set of questions, the two assessments are being carried out separately, but in parallel within the SecInCore project. They are also embedded in a wider collaborative and value sensitive design approach that follows up periodic dedicated PIA and EIA with more experimental hands-on engagement with stakeholders (Submitted as ISCRAM short paper).

The origins of the PIA process lie, among other aims, in a desire to address the implications or unintended consequences of new technologies (Stewart, 1996). As the SecInCoRe project is developing innovative cloud-based disaster response technology it falls squarely within this remit. Cloud computing and middleware for emergent interoperability raise a range of ethical, legal and social risks and opportunities, ranging from enhanced surge capacity and capabilities for agile and disaster proof establishment of systems of systems for multi-agency response to an erosion of privacy (ISCRAM 2014, IJISCRAM 2015).

In SecInCoRe, a first PIA was undertaken as part of the production of a research ethics package for the initial funding application to the EU's FP7 call. This was developed by drawing upon the tools in the UK ICO's PIA Code of Practice, which was updated in 2014 (UK ICO, 2014). The project partners outlined their responses in the light of the questions posed and these were amalgamated and submitted with the grant application. Throughout the literature on PIA, a strong theme is the need to avoid risk and take early steps to avoid infringing upon fundamental rights (Wright and De Hert, 2012, p10). This process was, therefore essential, both as it was mandated by the funding body but also in a wider sense because it was important, from an ethical and legal perspective, to predict potential risks within the project and address them at the earliest stage possible. One key practical observation here is the importance of timing and co-ordination. The initial PIA was carried out as part of the speculative grant application process. This involved speedy input from diverse partners, who did not know each other and who were working within tight workload constraints. While the review was carried out thoroughly, its timing in relation to the project as a whole underscores the importance of on-going review of the PIA process as the work develops.

One of the key aims of the PIA process is that it leads to transparency in relation to the operation of organizations and projects, which can increase end user confidence (UK ICO, 2014). This can be enhanced by the publication of the PIA on the organization's website (Wright and Wright, 2013). A challenge for SecInCoRe, which by its very nature, includes treatment of sensitive data, is to determine the extent to which the PIA and related reporting can be made public. It has been suggested that this could significantly change the PIA process, making participants far more guarded, obstructing self-criticism and vision. This aspect of the review is subject to on-going negotiation within the project with the aim of achieving the highest level of transparency possible. The SecInCore website (2015) contains a regularly updated section on research ethics, outlining the approach taken within the project and giving information on key ethical principles and protocols.

The PIA process undertaken is specific to SecInCore and, while some of the partners may have experience of the process within their own organizations, there was a need to introduce the project-specific use of the methodology. At the kick-off meeting at the University of Paderborn a presentation was given to the partners of the nature of PIA and how it was going to be implemented. A key aim was to avoid it being seen as the "box-ticking" exercise as criticized in the literature. Furthermore, there was the need to ensure that partners did not see the PIA as a

constraining exercise which just needed to be completed and forgotten about to "keep the lawyers happy". To achieve this, the presentation focused on the wider benefits of the PIA in relation to transparency, confidence and the streamlining of processes which could be beneficial to the project itself and to the partner organizations. It also highlighted the need for co-operation and integration in relation to the PIA and ELSI issues, rather than regarding them as an add-on which were only a matter for the Lancaster University ELSI team to address. Practical observations at this stage include that there was a positive reception to this approach and an interest in the issues raised by the PIA. It is accepted, however, that there is a need to translate this into action at a later stage. Another basic observation is that appropriate weight was given to the PIA process with the coordinator allowing for time to be spent on these issues in an otherwise time-pressured schedule.

A factor somewhat overlooked at this stage was the fact that the project pursues innovation and that this creates shifting ground for the PIA in the sense that it is not clear what kinds of technologies and what kinds of uses will be developed, or even exactly the goals the innovation aims to achieve. To address potential changes, the nature of PIA dictates on-going review of a project as it develops. As Beaumont (2014) helpfully summarizes: "By asking the right questions to the right people at the right stage in the development cycle…an organization can quickly distinguish between different levels of risk – and then use that information to decide where more effort is justified." In order to achieve this in SecInCore, time was given over for discussion at a subsequent project plenary meeting which took place in November 2014. To increase partner ownership of the process, a self-evaluation questionnaire was developed to prompt self-reflection and questioning of the on-going work undertaken. This was distributed to the partners before the meeting and the preliminary results were collated and presented for discussion. The questions related to, among other things, aspects of the partners' work, data sets collected, data sets analyzed, personal information collected and the sharing of data. There was also a section on sharing best practice, managing risk and the potential to improve processes. When presented in this collated manner it was useful to see the work of other partners, and the responses spurred intense discussion in relation to ELSI matters such as: inclusion of personal data in an inventory, the nature of a common information space, the capability to produce safe and secure information sharing infrastructures and the difficulty of knowing who was a legal entity. At this early stage in the project, the datasets analyzed were mainly publicly available and included planning documents relating to incident command systems. Partners with a strong technical focus reported accessing datasets that would not include personal information, such as lists of architectural security mechanisms and of markup languages used for information exchange between heterogeneous organizations. The small amount of personal information collected at this stage mainly related to activities undertaken to gain feedback on the developing technological solutions. A number of responses related to the collection of personal data to facilitate project meetings and publicity. The responses will be used to shape future practice and to identify ways in which approaches to privacy could be streamlined. It is expected that similar exercises will be carried out periodically in conjunction with project meetings.

Linking back to the need for transparency as outlined above, it is important that aspects of the PIA review process are made as accessible as possible. A 2013 report (Trilateral Research and Consulting, 2013) which examined 26 publicly available PIA reports in the UK found that, despite some stating that reports would be updated on the Internet, only one such update was found. Given the importance of the SecInCoRe on-going reviews, there are negotiations surrounding whether, once the data has been analyzed, some of the responses to the PIA exercises will be made publicly available.

A strong theme in the literature on PIA is the need to consult relevant stakeholders within the process in order to minimize any potential risks (De Hert et al, 2012, p5). In December 2014 the Lancaster University team organized a two day co-design workshop in the UK which brought together key stakeholders in emergency response to discuss the work of the SecInCoRe project. A number of activities were undertaken which brought ELSI issues to the fore and, while the

data is currently being analyzed, the results of this stakeholder consultation will be built into the on-going PIA and EIA review process.

.

CONCLUSION

In a reflection of Wright and Wadhwa's (2013) findings, the PIA process in the SecInCoRe project has had a positive impact on the shaping of the work undertaken, placing privacy at the heart of design and planning. The literature outlined above on approaching the PIA as a holistic, evolutionary process has been invaluable to enable a tailoring of the methodology to the work of SecInCoRe.

This paper has presented a snap shot of on-going work with the aim of continuously evaluating the strategies undertaken to shape and evaluate best practice. In the light of this, it is important to be candid about the challenges faced, these include: the need for sufficient time to plan for and address risks; the need for co-ordination and information about how the work is progressing; an assessment of transparency in the light of potentially sensitive data; and the need to respond to changes in project development in the light of the work undertaken. Indeed, it is the evolutionary development of innovative technology that is the most challenging yet rewarding aspect of the PIA process. In-keeping with the 2015 conference theme, while a project cannot fully be ready for the unexpected, the PIA process is essential for focusing attention on predicting change while minimizing risk and prioritizing end users.

ACKNOWLEDGMENTS

The research presented here is part of the BRIDGE and SecInCoRe projects, funded by the European Union 7th Framework Programme under (BRIDGE) FP7-SEC-2010-1 Theme: SEC-2010.4.2-1: Interoperability of data, systems, tools and equipment, Grant agreement no.: 261817 and (SecInCoRe) Topic SEC-2012.5.1-1 Analysis and identification of security systems and data sets used by first responders and police authorities, Grant agreement number 261817. We are grateful to our colleagues in these projects for our many inspiring conversations and their insightful comments.

REFERENCES

1. Beaumont, R. (2014) Privacy Impact Assessments and the DPR http://www.eudataprotectionlaw.com/privacy-impact-assessments-and-the-dpr/ [Accessed 20/01/15]
2. Bridge Projects (2011-2014) http://www.bridgeproject.eu/en [Accessed 25/01/15]
3. Council of the European Union (2014) General Data Protection Regulation [First reading] Interinstitutional File: 2012/0011 Brussels, 3 October 2014 http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2013772%202014%20INIT [Accessed 19/01/15]
4. De Hert, P., Kloza, D. and Wright, D. (eds) (2012) Recommendations For a privacy impact assessment framework for the European Union http://www.piafproject.eu/ref/PIAF_D3_final.pdf [Accessed 19/01/15]
5. 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 Official Journal L 281 , 23/11/1995 P. 0031-0050
6. European Commission (2012) Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data

(General Data Protection Regulation) http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf [Accessed 20/01/15]

7. Harris, I., Jennings, R. C., Pullinger, D., Rogerson, S. and Duquenoy, P. (2011) Assessment of new technologies: A meta-methodology, *Journal of Information, Communication and Ethics in Society*, 9, 49-64
8. Linden Consulting Inc (2007) Privacy Impact Assessments: International Study of their Application and Effects http://www.rogerclarke.com/DV/ICOStudy-2007.pdf [Accessed 20/01/15]
9. Mendonça, D., Jefferson, T. and Harrald, J. (2007) Emergent Interoperability : Collaborative Adhocracies and Mix and Match Technologies in Emergency Management. *Communications of the ACM*, 50, 3, 44–49
10. SecInCoRe (2014-2017) http://www.secincore.eu/ [Accessed 25/01/15]
11. SecInCoRe Research Ethics (2015) http://www.secincore.eu/open-research-ethics-protocol/ [Accessed 29/01/15]
12. Stewart, B. (1996) Privacy Impact Assessments, *Privacy Law and Policy Reporter*, 39 at: www.austlii.edu.au/au/journals/PLPR/1996/39.html [Accessed 22/01/15]
13. Trilateral Research and Consulting (2013) Privacy impact assessment and risk management https://ico.org.uk/media/for-organisations/documents/1042196/trilateral-full-report.pdf [Accessed 19/01/15]
14. UK ICO (2014) Conducting privacy impact assessments: code of practice https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf [Accessed 21/01/15]
15. Wadhwa, K. and Rodrigues, R. (2013) Evaluating privacy impact assessments, *Innovation: The European Journal of Social Science Research*, 26, 1-2, 161-180
16. Wright, D. and De Hert, P (eds) (2012) *Privacy Impact Assessment* Springer, Dordrecht
17. Wright, D. and Friedewald, M. (2013) Integrating privacy and ethical impact assessments *Science and Public Policy*, 40, 755–766
18. Wright, D. and Wadhwa, K. (2013) Introducing a privacy impact assessment policy in the EU member states International Data Privacy Law, 2013, 3, 1, 13-28