Analysing the role of Privacy Impact Assessments in technological development for crisis management

Abstract

The ability to harness technology in crisis management has enabled an increase in wide-scale interagency collaboration. This development has occurred alongside a move to accumulate and analyse crowdsourced responses. Given the scale and the nature of the information harnessed, there is a pressing need to ensure that technology is developed in a way that protects the interests of end users and stakeholders. 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 implemented, the EU's Data Protection Regulation will, in certain circumstances, require the need for a PIA. This paper focuses upon the PIA process in an EU-funded project with the aim of developing cloud-based disaster response technology. It introduces the project and then gives a background to the PIA process. Insights and observations are then made relating to how the PIA operates, with the aim of drawing conclusions that can both improve the current project and be transferable to other crisis management focused projects.

Keywords: Privacy, ethics, PIA, disasters, technology

1. Introduction

The Disaster Relief 2.0 report, jointly authored by the Harvard Humanitarian Initiative, the United Nations Foundation, the UN Office for the Coordination of Humanitarian Affairs (OCHA), and The Vodafone Foundation, provides numerous examples of the use of a wide-range of technologies in disaster response (Harvard Humanitarian Initiative. 2011). In particular, the January 2010 Haiti earthquake saw emergency responders, such as health care professionals, and the population sharing information globally and locally at an unprecedented level. The new age of communication is both centred around and spurred on by people, general end users. It is this very democratisation of and access to technology that leads to a number of challenges, particularly the need to maintain privacy. The report puts forward as one of its recommendations the need to create:

> *An innovation space where new tools and practices can be explored as experiments, allowing for the failures that are a necessary component of learning new ways of working.*

It is within this developmental space that the techniques implemented in Privacy Impact Assessments (PIAs) are crucial in order to shape innovative, experimental development of disaster response communications technologies. PIAs are 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 is the potential for proactively and constructively addressing problematic issues (de Hert et al, 2012). An example of this is that any technology that relies fundamentally on location tracking will have important implications for individual privacy, even when operating within large-scale datasets (de Montjoye et al, 2013). Furthermore, the push towards further collaboration and interoperability between the information systems of a wide range of agencies involved in emergency response throws up numerous nuanced, and often problematic, ethical and legal issues (Buscher et al, 2013). These include reluctance to share data due to perceived risks and liability and the inequitable focusing of services. Added to this are policymakers' and emergency technology developers' moves towards harnessing social media and crowdsourced responses during emergencies. Given these shifts, there is a need for the systematic embedding within technological developments of a wider consideration of the legal and ethical issues particularly those relating to data processing and sharing. It was to address the gap between the realities of technological use and the developmental process that the PIA was created. It acts a shaping tool to aid in proactive strategic planning and, in turn, protect the rights of technology developers and users, and data subjects, while also aiming to support the development of better technological solutions. In this paper we bring practical insights into this area through a discussion of this potential and of some of the successes and difficulties based on first experiences of including PIAs in IT innovation in crisis response and management.

The observations are based on work undertaken on an EU FP7-funded project. 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.*

The project 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 to guide future development of similar initiatives and related policy.

Building on experiences in the SecInCoRe project, this paper makes some observations on the privacy impact assessment process with the aim of making recommendations that could be transferable to other similar projects whether or not based in the cloud.

2. Privacy and privacy by design

The notion of privacy is a fluid concept which can be described as a given state, or normative, in terms of a right to force or stop others dealing with your personal information in certain ways. Its definition and, indeed the nature of privacy itself, is impacted upon by a wide range of societal and cultural factors, with no true consensus. This is due to a number of factors, such as the evolving nature of technology and legal systems with differing focuses on, for example, reasonable expectations of privacy and the importance of place. One way of approaching privacy that has received wide-ranging support is to see it from both the normative and descriptive perspectives as predicated on control, as Moore (2008: 435) states, as: a "*right to control access to places, locations, and personal information along with use and control rights to these goods*". In the modern age, the strength of user control is diminished by the complexities of technology and the potential extent of data collection and aggregation. This has led to a situation in which the EU data protection regime has developed a bundle of rights and responsibilities, many of which aim to lead towards a clearer, more transparent relationship between data subjects and their data. A relevant example is the new focus on allowing data subjects more control over the erasure of their data. Writing in relation to this so-called "right to delete", Bernal (2011) holds: "*if the holder of data has to provide a means for a user to delete data, they must first provide fast and understandable access to that data, and to do this properly would mean taking data privacy into account right from the start*". He then links this approach to the concept of privacy by design (PBD), arguing that such a right would lead to designers having to engage from the beginning of any project with individuals' control of their data. PBD is a concept that has been developed and expanded upon by Ann Cavoukian (2001), the former Information and Privacy Commission of Ontario. It promotes on-going engagement with privacy from the first inception of a technology and then throughout its development and ultimate use. The approach relies upon strategies to embed privacy protections through technological solutions. It seeks to bridge the gap between developmental processes and end user rights. However, the concept of PBD is not without its critics due to, among a number of issues, the changing nature of data within certain scenarios, difficulties in achieving effective anonymity, and issues of control (Rubinstein and Good 2012). PBD is one of the concepts that shaped the move towards the development of PIAs in order to provide a flexible tool to support privacy-enhancing techniques throughout the design process. PIAs aim to focus developers on the wider impacts of technology, drawing together socio-technical solutions to operate effectively within organisational and legal frameworks.

3. Definitions of Privacy Impact Assessments

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 data processing 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 both organisational and technology-development practices, with the aim of supporting a level of flexibility. Due to this, it provides benefits to organizations and to project planners and executors by delivering a framework to enable the improvement of systems and the meeting of external, for example, legal 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 of the PIA process 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 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.

4. Privacy Impact Assessments: The Legal Position

PIAs have been promoted and used in many countries and are mandatory in certain circumstances, e.g. in relation to all Canadian public health care projects and in relation to US' government agencies' information processing activities (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 General Data Protection Regulation (GDPR) was first published in January 2012. Since then it has undergone a series of amendments, had its timetable revised and, finally in December 2015, the European Commission (2015) and the Parliament (2015) announced that they had been able to compromise on an agreed text. A key focus of the discussions leading up to this point has been the need to minimize risk (Council of the European Union, 2014). The text was finalized in December 2015 and adopted in April 2016 (European Union, 2016). The majority of the provisions are set to come into force two years after this point.

This new wide-ranging piece of legislation will, in, make what it terms 'Data Protection Impact Assessments' (DPIA) mandatory "*where processing operations present specific risks to the rights and freedoms of data subjects*". While the term used in the legislation differs from PIA, the approach taken follows closely that of the development and implementation of what has been termed to this point PIAs. In recital 84 there is a need for data processors to carry out an assessment where the processing could result in a "high risk" to rights and freedoms. The results of the assessment should then be examined to determine whether or not the processing complies with the regime set out in the Regulation. It continues to give further details as to the required inclusions in an assessment:

> 35 (7): a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller; (b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes; (c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and (d) the measures envisaged to address the risks, including 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 provide a template that could lead to the development of an international standard. This, however, would need to be carefully implemented by relevant policymakers and regulators, 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.

5. Privacy Impact Assessments 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. The development of such tools is essential to support organizations through this process, but there is a danger that if these tools are badly designed the PIA itself can become a "mere box-ticking exercise" (Wright and De Hert, 2012: 22). Without a true engagement with process certain risks could be overlooked and there is a danger that the examination of design issues only occurs once and is not revisited on an evolving basis. The results of such an approach 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: vi).

PIA is a method of carrying out a wide-ranging evaluation of organizational processes and contexts, and 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 by the organisational and technology design team, with an emphasis on finding solutions. These do not necessarily have to be technical, and supporting on-going consultation. The process is, therefore, flexible, responding to the individual characteristics of the organization or project and open to change. In relation to this dynamism, Gary T. Marx (Wright and De Hert, 2012: xiv) 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 leads individuals to revisit and re-evaluate their actions and responses as a project or organization evolves. However, a steady process of evolution is required to support the implementation of a PIA. A lack of knowledge or engagement with key legal, technical or analytical issues can lead to difficulties when an organisation or project first attempts to implement the PIA. If these obstacles are not addressed at an early stage and supported by effective resources then the PIA process itself may either have negligible impact or, more worryingly, be damaging to any existing procedures put in place to support embedding privacy-preserving techniques into technological development. Sometimes, an organisation may request external advice from data protection consultants, which can be costly and not specifically tailored to the sphere in which the work is being undertaken. The EU Data Protection Regulation states that a "controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment". The Regulation mandates the need for a data protection officer to be appointed by the majority of public authorities and in private authorities where data processing requires regular and systematic monitoring of data subjects on a large scale. It was recognised during the negotiations leading up to the new legal regime that this would cause increased financial burdens, but its inclusion recognises that there is a need for knowledge and competence in data protection to be embedded within many organisations. The requirement to employ personnel with an overarching remit for monitoring data protection may seem onerous at the outset but increased easily-accessible, tailored expertise should lead ultimately to the development of more efficient, cohesive internal privacy protecting strategies. Under Article 39 of the GDPR a data protection officer has the duty of advising on the implementation of the DPIA and, in this way, could serve as a facilitator throughout the on-going process.

The SecInCoRe project as a multi-disciplinary project includes a team with expertise in the ethical, legal and social issues related to the development of disaster response technology to facilitate sharing. In this way there is always an "in-house" team available to provide guidance alongside a continuing focus on end user rights as the project developed. However, challenges arose in relation to the extent to which embedded practices can evolve to address privacy protections from the outset. The potential for technical teams to develop work in isolation was recognised and this was addressed through greater interaction between the partners, both using virtual communications and through face-to-face meetings. While this led to a stronger focus on and on-going engagement with end users in technological development, there was still a risk that the technology could be created in a way that deals with legal issues in a more post hoc rather than evolutionary manner.

6. The Relationship to the Ethical Impact Assessment

The EIA is a newer form of review and has developed, drawing upon a body of work on technology and ethics (Marx, 1998; Nissenbaum, 2004) 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 legal obligations. It takes a holistic approach to the development of technology as Wright (2010) states:

> an ethical impact assessment must not only focus on the ethics of a technology, but on the technology itself, its values, how it is perceived and how it is used or might be used in the future, not only by itself but as a component in a larger technological framework.

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 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 SecInCoRe project is strongly grounded in this approach, with a full work package (small sub-projects of the work as a whole) in each project being dedicated to monitoring the ethical, legal and social aspects (ESLI) of the research processes and innovations developed. This strategy ensures on-going internal monitoring and, perhaps more usefully, in a wider sense, also supports the dissemination of findings and observations on these issues to a wider audience in a manner transferable to other projects; the underlying rationale for this paper.

7. SecInCoRe and the PIA Process: Details and Observations

Within the SecInCore project, the ELSI team based at Lancaster University is responsible for coordinating a work package that connects empirical studies of ethical, legal and social opportunities and challenges as they arise in practice related to socio-technical design and innovation efforts. The ELSI team is also responsible for implementing and monitoring the PIA. The work undertaken ensures 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 the periodic dedicated annual PIAs and EIAs with more experimental hands-on engagement with stakeholders.

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 firmly within this remit. Cloud computing and middleware for emergent interoperability raise key ethical, legal and social risks and opportunities, such as enhanced surge capacity and capabilities for agile and disaster proof establishment of systems of systems for multi-agency response, to erosion of privacy (Buscher et al 2014).

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 to the assessment questions 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, not only 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 as thoroughly as possible, 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. Given that it is essential to employ a PIA in the planning phase, a strong recommendation to draw from this is to ensure that enough importance is given to its implementation in the face of the need to address other pressing and time consuming issues.

One of the key aims of the PIA process is to increase 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, included treatment of sensitive data, was to determine the extent to which the PIA and related reporting can be made public. It felt within the project that making the process public could significantly change the PIA, making participants far more guarded, obstructing self-criticism. 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. A potential solution could be to make a shorter version of the PIA available to the public, with sensitive information redacted. 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 in the project. A key aim was to avoid it being seen as the "box-ticking" exercise as criticized in literature on the subject. Furthermore, there was the need to ensure that partners did not see the PIA as a constraining exercise which just needed to be completed to placate the legal team. 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 throughout the project. Another basic observation is that, in the opinion of the Lancaster team, 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. The remit for carrying out the PIA and EIA falls within Work Package Two, which has a wider overarching focus on monitoring ELSI issues across the project as a whole. Work Package Two was allocated approximately 25% of the project's person months over its 36-month duration.

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 the specific 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 (see Appendix One) was developed by the ELSI team 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 analysed, 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 analysed 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.

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: 5). 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. The project Advisory Board includes a range of people drawn from across the European Union from sectors such as fire services, ambulance services, public emergency response planning and the Red Cross. A two-day Advisory Board meeting in September 2015, brought ELSI issues to the fore and, while the data is currently being analysed, the results of this stakeholder consultation will be built into the on-going PIA and EIA review process.

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 between the partners surrounding whether, once the data has been analysed, some of the responses to the PIA exercises will be made publicly available.

8. 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 in the project, 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. Lessons learned from this can be translated into any development of disaster and emergency response technology in order to focus attention on predicting change, while minimizing risk and prioritizing end users.

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 to the rights of end users; the need for co-ordination both within a technology development team and between the team itself and stakeholders; the need to ensure the sharing of information about how the work is progressing; the need to carry out an assessment of transparency in the light of potentially sensitive data; and the need to respond to changes during the project's development. Indeed, it is the evolutionary development of innovative technology that is the most challenging, yet rewarding, aspect of the PIA process.

References:

- Beaumont, R. (2014) '*Privacy Impact Assessments and the DPR'* http://www.eudataprotectionlaw.com/privacy-impact-assessments-and-the-dpr/ (accessed 20 September 2015)
- Bernal, P., (2011) 'A Right to Delete?', *European Journal of Law and Technology*, Vol. 2, No.2 http://ejlt.org/article/view/75/144
- Büscher, M., Bylund, M., Sanches, P., Ramirez, L., & Wood, L. (2013). 'A New Manhattan Project? Interoperability and Ethics in Emergency Response Systems of Systems'. In T. Comes, F. Fiedrich, S. Fortier, F. Geldermann, & L. Yang (Eds.), *Proceedings of the 10th International ISCRAM Conference*. http://eprints.lancs.ac.uk/62390/1/269_ManhattanProject_Final.pdf (accessed 08 September 2015)
- Buscher, M., Easton, C., Kuhnert, M., Wietfeld, C., Ahlsén, M., Pottebaum, J. and Van Veelen, B. Cloud ethics for disaster response ISCRAM Proceedings 2014 http://www.iscramlive.org/ISCRAM2014/papers/p137.pdf (accessed 20 September 2016)

- Cavoukian, A. (2011) Office of the Information & Privacy Commissioner of Ontario '*The Seven Foundational Principles'* January https://www.privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples.pdf (accessed 10 February 2016)
- 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 October 2015)
- 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 November 2015)
- 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
- 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 November 2015)
- European Commission (2015) *Press release Agreement on Commission's EU data protection reform will boost Digital Single Market* http://europa.eu/rapid/press-release_IP-15-6321_en.htm (accessed 18 December 2015)
- European Parliament (2015) News: Data protection package: Parliament and Council now close to a deal *EuroParl* http://www.europarl.europa.eu/news/en/news-room/20151215IPR07597/Data-protection-package-Parliament-and-Council-now-close-to-a-deal (accessed 18 December 2015)
- European Union (2016) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) OJ L 119, 4.5.2016, p. 1–88 http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC# (accessed 28 July 2016)
- 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, pp49-64
- Harvard Humanitarian Initiative (2011) '*Disaster Relief 2.0: The Future of Information Sharing in Humanitarian Emergencies'*. Washington, D.C. and Berkshire, UK: UN Foundation & Vodafone Foundation Technology Partnership
- Linden Consulting Inc (2007) '*Privacy Impact Assessments: International Study of their Application and Effects'* http://www.rogerclarke.com/DV/ICOStudy-2007.pdf (accessed 20 November 2015)
- Marx, G. (1998) Ethics for the new surveillance. *The Information Society* 14 171-185
- de Montjoye, Y, Hidalgo, C., Verleysen, . and Blondel, V. (2013) 'Unique in the Crowd: The privacy bounds of human mobility' *Nature Scientific Reports* 3, Article number: 1376 doi:10.1038/srep01376 http://www.nature.com/articles/srep01376

- Moore, A. (2008) 'Defining Privacy' *Journal of Social Philosophy*, Vol. 39, No. 3, pp. 411-428
- Nissenbaum, H. (2004) Privacy as contextual integrity. Washington Law Review, 79 (1), 101-139
- Rubinstein, I. and Good, N. (2012) 'Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents' *Berkeley Technology Law Journal* NYU School of Law, Public Law Research Paper No. 12-43, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2128146 (accessed 02 February 2016)
- SecInCoRe (2014-2017) http://www.secincore.eu/ (accessed 25 September 2015)
- SecInCoRe Research Ethics (2015) http://www.secincore.eu/open-research-ethics-protocol/ [Accessed 29/11/15]
- 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 November 2015)
- 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 October 2015)
- 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 October 2015)
- Wadhwa, K. and Rodrigues, R. (2013) Evaluating privacy impact assessments, Innovation: *The European Journal of Social Science Research*, 26, 1-2, pp161-180
- Wright, D. (2011) A framework for the ethical impact assessment of information technology *Ethics and Information Technology* 13, 199-226
- Wright, D. and De Hert, P (eds) (2012) '*Privacy Impact Assessment'* Springer, Dordrecht
- Wright, D. and Friedewald, M. (2013) Integrating privacy and ethical impact assessments '*Science and Public Policy'*, 40, 755–766
- 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

Appendix One:

Privacy Impact Assessment Self-evaluation Questionnaire

Please outline:

- The datasets you have already collected
- The datasets you plan to collect in the next 6 months
- The datasets you have analysed
- The datasets you plan to analyse in the next 6 months
- Given your current and planned work, should any new categories be added to the list above?

Please outline:

- The nature of any personal information you have already collected
- The nature of any personal information you plan to collect in the next 6 months
- Given your current and planned work, should any new categories be added to the list above?

- Please outline the categories with whom you are currently sharing information or with whom you plan to share information.
- Please outline the processes you have in place (or plan to put in place) to ensure data accuracy and completeness?
- Do you have any examples of best practice to share with project partners in relation to how you achieve data accuracy and completeness?
- Please outline the processes by which you manage access to any data collected. Could these processes be improved?
- In general, to what extent do you believe you are operating in a risk-averse manner? Please give brief details.
- Ideally, we would like to improve on the state of the art in relation to developing effective ethical and legal practices. In the light of this what would you see as:

❖ Challenges

❖ Opportunities