Information Systems for Crisis Response and Management: The EU Data Protection Regulation, Privacy by Design and Certification

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

ABSTRACT

With technological development in crisis management reaching a point at which there is wide-scale aggregation of data, including social media, there is a need to focus strongly upon the position of end users in order to uphold data protection principles. Recent wide-ranging European Union legal reforms, finalized in 2016, have enshrined the concept of data protection by design and paved the way for certification schemes to validate compliance. There is a need for those involved with the practical development of information systems for crisis management to understand these new developments and determine their practical implications. This paper presents a critical analysis of the reforms, focusing on the interplay between the law and technological design and predicting their impact on crisis management system development.

Keywords

Data Protection, EU law, Privacy by Design, Certification, Crisis Management Technology

INTRODUCTION

It has been recognized that the development of information systems for crisis management raises a number of complex ethical and legal issues (Buscher et al, 2015). Of specific interest are the growing risks to end user privacy that come as new systems increasingly focus on supporting inter-agency data sharing, alongside an emphasis on harnessing social media in emergency situations. The EU's new data protection regime maintains the exceptions relating to the processing of data to protect vital interests and in relation to actions in the public interest. However, in an emergency situation there is need for responders to balance public interest considerations with the potential harm that may arise from not storing and sharing information. Empirical work (Ellebrecht and Kaufman, 2015) into the development of crisis management technologies highlights the complex socio-technical interplay of the approaches taken by users and the technology itself. These complexities are being recognized in recent initiatives and strategies aimed at bridging the gap between technological development, its use in practice and legal principles (SecInCoRe D2.4). For some time the need has been identified for privacy enhancing technologies to be developed and employed alongside "legal, organizational, ethical and educational tools" (Borking and Raab, 2001). An example of such a measure is the Privacy Impact Assessment (PIA), a tool that is being employed on large-scale disaster response projects (Easton and Buscher, 2015). Strongly related to this tool is the concept of privacy by design, an approach that seeks to embed privacy in the development of and throughout the implementation of a technology. The European Data Protection Regulation (EU, 2016) will enshrine this disputed concept within a legal regime, while also providing for a certification scheme to facilitate the practical uptake of key principles. This short paper raises questions about the concept of privacy by design and moves on to outline the approach the new law

takes to certification and the potential impact this could have on the development of disaster response technology.

PRIVACY BY DESIGN

The term "Privacy by Design" (PBD) refers to the practice of incorporating privacy-supporting specifications into the planning of technological design and throughout its on-going implementation. Its examination first appeared in a joint report of the Dutch Data Protection Authority and the Information and Privacy Commissioner for the Province of Ontario, Canada (1995). This highlighted the dual challenges of the zeal of both private and public organisations to collect an ever-increasing amount of data, set against a lack of user awareness of the benefits of anonymity-protecting technology. Over the subsequent twenty years the concept has been developed, with particular enthusiasm from Ann Cavoukian, the Information and Privacy Commission of Ontario, whose office created the Seven Foundational Principles of Privacy by Design (2001), which, when applied allow "*for greater privacy and personal control over one's information, while enabling organizations to gain a competitive advantage, that is sustainable over time*" (Cavoukian, 2014). While its multi-faceted, technology-focused approach has led to a welcome practical emphasis on the protection of users' privacy, the concept is not without criticism. These include: the difficulty of embedding true anonymity into technological design, the development of facial recognition and location-based technologies (O'Donoghue et al, 2011), the need to address issues of control when users voluntarily share information (Rubinstein and Good, 2012) and the potential for inequalities to persist in technological design. The socio-technical qualities of anonymity, control and inequality change according to context, location and situation; they are not absolute "states" of data. These factors are particularly prescient when responding to emergencies. However, despite these misgivings, we are approaching a situation where PBD, under the name "data protection by design" is now enshrined as a legal concept across the EU.

EUROPEAN UNION LAW AND PRIVACY BY DESIGN

Any examination of the EU's provisions needs to be set against the backdrop of on-going data protection law reforms, 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 (EU Parliament, 2012). Since then it has undergone a series of amendments, with the Commission, Parliament and Council in December 2015 announcing that their negotiations were completed with the aim of approving the consolidated text in early 2016. Once this text has been finalized, the majority of the provisions will not come into force for a further two years. The 1995 Directive did not include PBD provisions but the new regulation includes a number of references, the most prominent being:

Article 23: Data protection by design and by default

> *(1) Having regard to the state of the art and the cost of implementation and taking account of the nature, scope, context and purposes of the processing as well as the risks of varying likelihood and severity for rights and freedoms of individuals posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data protection principles, such as data minimisation, in an effective way and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.*

This Article enshrines a focus on user rights as central to the measure itself and the specific reference to risk expands upon the required organisational, non-technical strategies. The final version does not, however, provide examples of the potential objectives of the relevant processing as suggested in earlier versions. This is a positive development as, given the need for flexibility, preference for certain objectives of processing should not be included as all of the principles of data protection should be given equal consideration within their relevant contexts. In negotiations these now-removed examples caused disagreement, with Germany arguing for the inclusion of the term "*data economy and avoidance*". Furthermore, the reference to "*minimisation*" also proved problematic; the data minimisation principle that personal data must be "*limited to the minimum necessary in relation to the purposes for which they are processed*" (Art 5(1c)) has survived to the final draft and was not

replaced with the Council's much less restrictive standard of personal data collection being "*not excessive*"(Council Reg Art 5 (c)).

In the final draft, Article 23(1) is followed by a further provision (Art 23 (2a)) which allows for delegated legislation to be made by the Commission to specify "*appropriate measures and mechanisms*" to comply with the Article's requirements. In allowing for on-going measures to be made, the Regulation acknowledges the manner in which the technology relating to PBD is constantly evolving and that further provisions and updates to the law may be required. Those developing crisis management technologies need to be aware of any changes and their implications; there is, therefore, a greater need for outreach from a body such as the European Data Protection Agency to provide easily accessible, affordable and clear guidance.

Despite the vague nature of the term PBD, the EU has already included the concept in soft law, such as the Recommendation on the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems, which ties it strongly back to the Data Protection Regulation's Article 33 data protection impact assessment requirement. Furthermore it is a concept that has been embraced by the current Data Protection Directive's Article 29 Working Group in, for example, its report into the Internet of Things (Article 29 Working Party, 2014). This states: "*privacy protections should be built-in from the very outset, in application of the "Privacy by Design" principle*" (p19) and later, "*Every stakeholder in the IoT should apply the principles of Privacy by Design*" (p21). The concept is now an important facet of data protection policy and proposed legislation but, as demonstrated by the negotiations around the EU's Data Protection Regulation, its nature is far from clear and regulatory measures required to support its application need tailoring to the realities of organisational management and technical development.

Crucially, there is a need to bridge the gap between the regulatory environment, with its focus on end-user protection, and the realities of technological design. Paul Ohm's "*Broken Promises of Privacy*" (2010) presents a comprehensive challenge to designers' responses to privacy concerns being a reliance upon the claim that the data is anonymised. He outlines how technology has now developed to the point where re-identification of individuals in purportedly anonymised data is becoming ever easier. These concerns have, to a limited extent, been addressed in the reforms with the inclusion of specific measures to address pseudoanonymity, a term which occurs at numerous points in the Regulation (eg Arts 23, 30, 38, 83). It is defined as "*the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information*" (Art 4(3b)). The data is deemed to be personal data if there is a reasonable likelihood of identifying the individual. To determine what is reasonable:

> *account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration both available technology at the time of the processing and technological development.(para 23 Preamble)*

These measures are in response to criticism that the legally-enshrined distinction between anonymised and non-anonymised data was becoming, in essence, redundant. The Regulation makes further attempts to address this issue with the expanded definition of anonymous data as: "*information which does not relate to an identified or identifiable natural person or to data rendered anonymous in such a way that the data subject is not or no longer identifiable*" (Preamble para 23). This clarification of a technical concept, however, will only be effective if regulators and end users are able to trust that true anonymity is achieved, even in the face of technological advancement.

The debate has continued with PBD originator and advocate, Cavoukian, writing a 2014 report (Cavoukian, and Castro, 2014) in support of de-identification, with the rather questionable concluding argument that it is a viable concept as it is achievable in the vast majority of instances, even though there may be a small number of cases when it is not. Her jointly written report uses the analogy of home security which helps reduce burglaries but may not do so in 100% of cases. This is a dangerous argument, as identified by Ohm, due to the need for legal clarity and the risk that a reliance on a technical concept that is accepted to be fallible will only lead to a confused application of the legal principles. Indeed, in a critical response to the Cavoukian paper, Narayanan and Felten (2014, p7) question its calculations of the possibilities of de-identification as being based "*on arbitrary and fragile assumptions about what auxiliary datasets and general knowledge are available*" to an "*adversary*" trying to identify an individual. This is particularly prescient in any developmental environment in which a focus on the realities of the end user experience is lacking; for example, criticisms have been raised in response to the use of integrated response systems introduced in the aftermath of some emergency situations

(Naphade et al 2011). The debate in this area demonstrates the inherent difficultly of legislating in a technologically-neutral manner for in-built flexibility while also acknowledging technological functions and capabilities. It also demonstrates the difficulty of including the nuanced socio-political practices that are part of the technological design, not just the technology or software itself.

Furthermore, Paul Swartz (1999) highlights that lobbying from the online industry has led to a bottom-up approach to the creation of ineffective standards that may even weaken privacy protections. He argues strongly for a State intervention both in what he terms the market of privacy and in the creation of norms. The EU has taken a lead by embedding the concept into its reforms but there is a need for further critical work to define the concept and to determine the limits of its practical application to avoid it becoming a worthless notion that ultimately acts as a smokescreen for bad practice.

CERTIFICATION

The Regulation tasks the Member States, the supervisory authorities and the European Data Protection Board (Art 39) with encouraging the establishment and monitoring certification schemes to demonstrate compliance with key principles. It goes on to reference expressly (Art 23 (2a)) the adherence to a certification mechanism as a manner of upholding the duties of a controller in relation to data protection by design. Legally-mandated certification schemes have long been in place in sectors such as the environment and medicine. Such an approach demonstrates the importance attached to the enforcement of the law, as regulator-mandated certification schemes have often been found to produce quicker and more effective results and protections than post hoc legal sanctions. While the details have yet to emerge about any Data Protection Regulation scheme, care should be taken in the methods employed to put the measures in place. Certification schemes backed up with the sanction of the law can harness industry expertise while providing higher levels of compliance than self-regulation (Lookabaugh, 2006). However, the acquisition of any certificate should not lead to a situation in which those collecting data feel complacent and do not then respond to on-going risks and unforeseen events. There is a need to ensure that those providing the validation have a firm grasp of the continuing socio-technical and organisational realities of protecting data. As Lookabaugh et al (2006, p13) state:

> *an organization may find it infeasible to maintain adequate criteria to certify products that change rapidly in function and capability. In such cases, certification may be practical only if it is restricted to aspects of the system that undergo fewer changes and that can be reasonably isolated.*

This raises key questions for the development of technology for emergency response, relating to whether there is a need for tailored or nuanced certification schemes focusing specifically on disaster response technology. In this area the EU has supported the development of "sector-specific coalitions" (Boin et al, 2014; Kuipers et al., 2015) and guidelines based on approaches taken in the USA (U.S. Dept. of Health and Human Services, 2006) are being developed to embed key ethical, legal and social issues into disaster response technologies (SecInCoRe D2.4). A point is being approached at which it is important for those working in the emergency response sector to engage in a dialogue with regulators regarding what an effective certification mechanism would look like, who would provide it and whether it would be nuanced enough to address and support key issues relating specifically to emergency response technologies.

CONCLUSION

Measures to address the wider legal and ethical environment within which technology operates have become embedded in the development of information systems for crisis response and management. The EU's Data Protection Regulation marks an important milestone in the pursuit of practical privacy-enhancing legal provisions in the face of ever-encroaching technological development. However, its acceptance of a term such as data protection by design without full and thorough appreciation of its potential failings could dilute the impact of the regulation itself. Furthermore, while certification schemes are a useful tool in regulation, they need to be carefully established and maintained in order not to reach a point at which they increase bureaucracy while reducing engagement with complex socio-technical environments to a mere box-ticking exercise. Those working in the creation of disaster response technologies need to engage critically with these legal and regulatory developments to ensure that the best possible systems are produced, employed and maintained, in order to support an environment in which end user rights are placed at the centre of the design process.

ACKNOWLEDGMENTS

The research is part of research funded by the European Union 7th Framework Programme in the SecInCoRe project (Grant no: 261817) and the BRIDGE project (Grant no.: 261817).

REFERENCES

1. Article 29 Working Party (2014) Opinion 8/2014 on the on Recent Developments on the Internet of Things Adopted on 16 September http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf [Accessed 01/12/15]
2. Boin, A., Rhinard, M. and Ekengren, M. (2014). 'Managing Transboundary Crisis: The Emergence of European Union Capacity'. Journal of Contingencies and Crisis Management, 22(3): 131-142
3. Borking J and Raab C, Laws, PETs and Other Technologies for Privacy Protection 2001 (1) The Journal of Information, Law and Technology (JILT). https://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2001_1/borking/ [Accessed 09/01/16]
4. Büscher, M., Perng, S.-Y., and Liegl, M. (2015). Privacy, Security, Liberty: ICT in Crises. International Journal of Information Systems for Crisis Response and Management (IJISCRAM)
5. 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 11/11/15]
6. Cavoukian, A. (2014) Privacy by Design: From Rhetoric to Reality January https://www.privacybydesign.ca/index.php/paper/privacy-design-rhetoric-reality/ [Accessed 11/12/15]
7. Cavoukian, A. and Castro, D. (2014) Big Data and Innovation, Setting the Record Straight: Deidentification Does Work, 2014 http://www2.itif.org/2014-big-data-deidentification.pdf [Accessed 09/01/16]
8. Committee on Civil Liberties, Justice and Home Affairs (2012) Draft Report on the proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)) http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/pr/922/922387/922387en.pdf [Accessed 09/11/16]
9. Easton, C. and Buscher, M. The role of the privacy impact assessment in IT innovation in crises: an example The 12th International Conference on Information Systems for Crisis Response and Management. ISCRAM
10. Ellebrecht, N., and Kaufmann, S. (2015). Boosting efficiency through the use of IT? Reconfiguring the management of mass casualty incidents in Germany. In IJISCRAM, 7
11. EU Regulation (2011) No 182/2011 of the European Parliament and of the Council of 16 February 2011 laying down the rules and general principles concerning mechanisms for control by the Member States of the Commission's exercise of implementing powers http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32011R0182 [Accessed 09/01/16]
12. EU (2014) Recommendation on the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems (2014/724/EU) 10th October http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014H0724&from=EN [Accessed 09/12/15]
13. EU (2016) Regulation (EU) of the European Parliament and of the Council (EU) No XXX/2016 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://static.ow.ly/docs/Regulation_consolidated_text_EN_47uW.pdf [Accessed 09/01/16]
14. EU Directive 95/46/EC 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 http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:31995L0046 [Accessed 09/12/15]

15. EU Parliament (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) Brussels, 25.1.2012 COM(2012) 11 final 2012/0011 (COD) http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf [Accessed 09/10/15]
16. EU Parliament (2014) 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) Council of the European Union Brussels, 19th December 2014 http://data.consilium.europa.eu/doc/document/ST-15395-2014-INIT/en/pdf [Accessed 09/11/15]
17. Kuipers, S., Boin, A., Bossong, R. and Hegemann, H. (2015). Building Joint Crisis Management Capacity? Comparing Civil Security Systems in 22 European Countries, Risk, Hazards and Crisis in Public Policy, Vol 6, No. 1
18. Lookabaugh, T., Ryan, P. and Sicker, D. (2006) A Model for Emergency Service of VoIP Through Certification and Labeling 58 Federal Communications Law Journal 115 http://www.colorado.edu/policylab/Papers/E911Certification.pdf [Accessed 12/01/16]
19. Naphade, M. et al (2011) Smarter Cities and Their Innovation Challenges *Computer* Issue No.06 - June (vol.44) pp: 32-39
20. Narayanan, A. and Felten, E. (2014) No silver bullet: De-identification still doesn't work July 9 http://randomwalker.info/publications/no-silver-bullet-de-identification.pdf [Accessed 09/01/16]
21. O'Donoghue, C., Tyler, N. and Chin, K. (2011) Meeting Report: Privacy by Design – 'Grand Design' or 'Pipe Dream' http://www.scl.org/site.aspx?i=ne19845 [Accessed 11/11/15]
22. Office of the Information & Privacy Commissioner of Ontario and Registratiekamer (1995) Privacy-Enhancing Technologies: The Path to Anonymity (Volume I) Aug 01, 1995 https://www.ipc.on.ca/english/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=329 [Accessed 11/05/15]
23. Ohm P. (2010) Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization UCLA Law Review, Vol. 57, p. 1701, 2010 http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006## [Accessed 09/01/16]
24. 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 11/10/15]
25. Schwartz, P. (1999) Internet Privacy and the State, 32 Conn. L. Rev. 815 http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1765&context=facpubs [Accessed 09/01/16]
26. SecInCoRe D2.04. (2015) Domain Analysis: Baseline and emergent future practices, 10/31/2015