Privacy by Design and the Internet of Things: From Rhetoric to Practice using Information Privacy Cards

Lachlan Urquhart, University of Nottingham

This paper discusses a tool that has been developed to help move the principle of data protection by design from theory to practice. Article 23 of the General Data Protection Reform Package mandates data protection by design and default. This, in turn, increases the role of technology designers in regulation.[1] However, guidance on what that actually requires in practice is sparse. Different technical measures to ensure privacy by default exist, such as anonymisation or encryption. Equally, organisational approaches like privacy impact assessments[2] can be of assistance. However, the regulatory challenges posed by emerging technologies, like internet of things ecosystems,[3] require a more accessible means of holistically bringing information privacy law principles into system design.

By calling on design to be part of regulation, it is calling upon the system design community: a community that is not ordinarily trained or equipped to deal with regulatory issues. In order to implement Article 23 in practice will require far greater engagement with and support of the system design community.

Law is not intuitive or accessible to non-lawyers, yet by calling for privacy by design, the law is mandating non-lawyers be involved in regulatory practices. We argue that there is a need to engage, sensitise and guide designers on data protection issues on their own terms. Presenting a non-legal community with legislation, case law or principles framed in complex, inaccessible legalese is not a good starting point. Instead, a truly multidisciplinary approach is required[4] to translate legal principles from law to design. This is no easy task.

Technical and human centric approaches to engaging with the regulatory challenges of emerging technologies have emerged in the fields of usable privacy and security (eg P3P)[5], privacy engineering[6] or more recently, human data interaction (eg personal data containers).[7] By looking at the interface between privacy law and human computer interaction we've developed a new, practical tool to engage designers: information privacy cards.

Ideation cards[8] have an established lineage in design as a tool to help designers explore and engage with unfamiliar or challenging issues. They also are also sufficiently lightweight and can be deployed in a range of design contexts, for example at different stages within the agile software development process. We have developed a set that draw on European data protection law principles.

We have tested different iterations of them with designers and found a number of barriers between the two communities that need to be overcome.[9] For example, data protection knowledge of system designers (ranging from software architects to user interface specialists) is limited and needs driven. Meeting DP regulations is also often seen as a limitation on system functionality and is not really the job of designers**.** Our new iteration of the cards translates a range of user rights and designer responsibilities from the *whole* post trilogue General Data Protection Reform Package. Through workshops with teams of designers in *industry* and *education* contexts we are trying to understand the utility of the cards as a privacy by design tool.

In this paper we will discuss our findings so far, seeking feedback from the IT law community. We present a number of issues and lessons from this work on what privacy by design actually means in practice, and the challenges and barriers between the design and legal communities. We situate many of these discussions within the context of the internet of things.

[1] L Urquhart and E Luger "Smart Cities: Creative Compliance and the Rise of 'Designers as Regulators'" (2015) *Computers and Law* 26(2)
[2] D Wright and P De Hert *Privacy Impact Assessment (*2012 Springer)
[3] A29 WP "Opinion 8/2014 on the recent Developments on the Internet of Things" WP 233
[4]; We are conducting a project in the EU and US involving researchers from: University of Nottingham (Tom Rodden, Neha Gupta, Lachlan Urquhart), Microsoft Research Cambridge (Ewa Luger, Mike Golembewski), Intel (Jonathan Fox), Microsoft (Janice Tsai), University of California Irvine (Hadar Ziv) and New York University (Lesley Fosh and Sameer Patil). ***- EU project page and cards are available at designingforprivacy.co.uk***
[5] J Hong "Usable Privacy and Security: A Grand Challenge for HCI" (2009) *Human Computer Interaction Institute*
[6] Danezis et al "Privacy and Data Protection by Design – from policy to engineering*"* (2014) *ENISA;* M Dennedy, J Fox and T Finneran "Privacy Engineer's Manifesto" (2014) Apress; S Spiekermann and LF Cranor "Engineering Privacy" (2009) *IEEE Transactions on Software Engineering* 35 (1)
[7]H Haddadi et al "Personal Data: Thinking Inside the Box"(2015) *5th Decennial Aarhus Conferences;* R Mortier et al "Human-Data Interaction: The Human Face of the Data Driven Society"(2014) http://hdiresearch.org/
[8] IDEO https://www.ideo.com/work/method-cards; M Golembewski and M Selby "Ideation Decks: A Card Based Ideation Tool" (2010) Proceedings of *ACM DIS '10,* Aarhus, Denmark https://dl.acm.org/citation.cfm?id=1858189
[9] E Luger, L Urquhart, T Rodden, M Golembewski "Playing the Legal Card" (2015) Proceedings of *ACM CHI* '15, Seoul, S Korea