Playing the Legal Card: Using Ideation Cards to Raise Data Protection Issues within the Design Process

Ewa Luger
Microsoft Research
Cambridge, UK
a-ewluge@microsoft.com

Lachlan Urquhart, Tom Rodden & Michael Golembewski
University of Nottingham, UK
Firstname.Lastname@nottingham.ac.uk

ABSTRACT
The regulatory climate is in a process of change. Design, having been implicated for some time, is now explicitly linked to law. This paper recognises the heightened role of designers in the regulation of ambient interactive technologies. Taking account of incumbent legal requirements is difficult. Legal rules are convoluted, uncertain, and not geared towards operationalisable heuristics or development guidelines for system designers. Privacy and data protection are a particular moral, social and legal concern for technologies. This paper seeks to understand how to make emerging European data protection regulations more accessible to our community. Our approach develops and tests a series of data protection ideation cards with teams of designers. We find that, whilst wishing to protect users, regulation is viewed as a compliance issue. Subsequently we argue for the use of instruments, such as our cards, as a means to engage designers in leading a human-centered approach to regulation.

Author Keywords
Regulation, Data Protection, Ideation cards, Design

ACM Classification Keywords
H.5.m. Information interfaces and presentation (e.g., HCI): Miscellaneous

INTRODUCTION
We stand at the threshold of a major change in policy accountability around systems design. The 'designer', having played a background role in an ecosystem of products, requirements and users, is being called to the fore. International policy and transnational legal infrastructure are foregrounding the designer and highlighting a new set of legal conditions. Where once designers and systems architects were only subject to the influence of regulation at the point of product market entry, they are now being called to account from the minute pen hits paper. Privacy and security will soon be expected 'by design and by default' – and with this regulatory turn, comes a raft of responsibilities.

CHI 2015, April 18 - 23 2015, Seoul, Republic of Korea
Copyright 2015 ACM 978-1-4503-3145-6/15/04…$15.00
http://dx.doi.org/10.1145/2702123.2702142

The sphere of systems design is already clearly implicated within international policy discourse. The Organisation for Economic Cooperation and Development (OECD) privacy guidelines (2013) Part Five, call for national complementary measures. Under this section, member states have committed to consider "*the promotion of technical measures which help protect privacy*" [27]. At the same time, regulations proposed by the EU have foregrounded 'privacy by design' as the mechanism by which data protection (DP) might be assured. Whilst DP is already articulated through accepted mechanisms, such as Fair Information Practice Principles (FIPPs), these have focused solely upon the *rules* of data management and control rather than 'the system'.

The locus of responsibility, having previously rested with the user or data subject, is now being refocused. Whereas the user *was* predominately responsible for protecting their data, it is now broadly agreed that this undertaking is beyond the ability of the layperson. Instead, the weight of accountability is more firmly placed upon the data controller; in other words, those who control and are "*responsible for the keeping **and use** of personal information on a computer or in structured manual files*". Indeed, if you (a) keep/process *any* information about living people and (b) decide what personal information is to be kept, or (c) decide the purpose to which that information is to be put, you are already subject to 'serious legal responsibilities' [2]. With the advent of the coming EU General Data Protection Regulation (GDPR) however, these responsibilities are set to expand with international implications, but at what cost? As with any move to govern and control a market, so comes the fear that innovation will be stifled, lawyers will become necessary, and that subsequent costs will limit speculation, startups, and grassroots development.

However, this perspective misses a trick. If data protection is to be 'by design', surely this also presents a huge opportunity. Rather than bolting on onerous terms and conditions or parachuting in lawyers after the fact, consider the possibilities of taking a step back and asking; 'how can HCI as a community, make privacy and data protection a creative integral component of the systems we design?' What if, rather than outsourcing this knowledge and bowing to the glacial

pace of the legal machine, we seek to build it into our practice? What if we were to take our human-centered skills and approaches and methodologically ply them to advance the regulatory field? In this paper we ask - how and at what stage of the design process might we engage designers with data protection regulation? Drawing upon an approach to creative engagement recognised by the design community - ideation cards - we develop a deck of cards and test these with 4 groups of designers in a workshop setting. Our study surfaced the limited ways in which designers reasoned about regulation; as a practical matter for address within a system. This both raised questions around the orientation of designers to DP, and also the need to consider the use of instruments similar to our cards in the early stages of the design process.

REGULATION AND THE ROLE OF DESIGN

'Regulation' is traditionally defined as "the sustained and focused control exercised by a public authority over activities valued by the community" [5, p.12]. From this perspective, regulation is a mechanism of state systemic control. However, changing conditions have rendered this definition less relevant, particularly within the sphere of technology where regulation includes multiple non-state actors participating in creation of technical standards, e.g. the World Wide Web Consortium (W3C) [26]. As a field of study, regulation has broadened. Technology regulation in particular is unique in that the speed of development necessitates a mixed regulatory climate, including intergovernmental treaties such as the OECD Privacy Guidelines [26], international agreements amongst private sector organisations, co-regulatory and self-regulatory arrangements, which arise from the market and often take the form of technical solutions. In this way, Internet regulation is something of *"a patchwork of different regulatory approaches in continuous flux"*[12, p.542]. Reflective of this broader conception, our study proceeds from the position that *"regulation is the sustained and focused attempt to alter the behaviour of others to standards or goals with the intention of producing a broadly identified outcome or outcomes, which may involve mechanisms of standard-setting, information gathering and behavior modification"* [6, p103]. Unlike traditional definitions, this perspective does not stipulate the source of regulation, embracing non-sate actors such as designers, whilst retaining a clear focus upon the function and intentions of regulation and the processes by which these might be achieved.

Whilst such conceptual framings are gaining ground amongst legal scholars, the extent to which HCI sees itself as part of this climate is questionable. So, if designers are currently incognisant within the regulatory machine, how can we begin the process of sensitising our community to the attending opportunities, limitations and responsibilities? One approach to encouraging thought, recognised by the design community, is that of ideation cards as a stimulus for creative endeavor.

USING IDEATION CARDS

The use of cards as a methodological design instrument is well established [15,13] as a means to "help define constrained design problems within a broader overall problem space" [15]. The use of cards as a creative stimulus has been applied to (a) the sphere of human values in the design process [13], (b) to support communication within and between families [24], (c) to encourage participants to think about security threats [30], (d) to stimulate creative methods within design practice by "representing diverse ways that design teams can understand the people they are designing for"[16], (e) to "help people explore and discuss issues around online privacy"[4], and (f) to support the exploration of design problems within a broader context [15]. Despite their different emphases, fundamental to all of these applications is the notion of cards as a mechanism to stimulate creative thought, often around subjects previously unfamiliar to the participants. Reflective of this tradition, the focus of our research was to design and test a creative method that raised awareness, amongst designers, of the intersection between their work and the proposed EU DP Legal framework. Law and policy instruments are often drafted in obtuse legalese, rendering them inaccessible to anyone other than lawyers and regulators. However, there is an increasing recognition within the legal community that, through their design decisions, technologists can play a key role in data protection. Our intention was to sensitise designers to this notion.

THE CHALLENGE OF DATA PROTECTION

Technologies already enforce regulatory norms through architecture and information management practices [20]. However, this raises important questions around the legitimacy and accountability [19,33] of such design decisions. Whilst technical solutions have been developed to protect personal data, e.g. through data anonymisation, pseudonomysation, or end-to-end data encryption, the extent to which privacy goals are considered within broader system design is less clear. The design of ambient systems that preserve privacy and respect data protection law is challenging. This is because;

(a) Ambient systems do not support established legal mechanisms such as obtaining informed user consent to data processing [8,18,21], **(b)** Human agency and control over human data processing is lessening, driven by increasingly autonomous systems with decreasing functional accountability to the user, i.e. the growth of so called 'black box' systems, **(c)** Law creates principles, rules, and sanctions, but not implementable design guidelines. Regulators advocate privacy by design approaches to data management (i.e. reflecting on and addressing privacy risks of a system during design) (EU Art 23) [9,17].

Despite these challenges, legal changes are already underway, with the 2012 proposed EU General Data Protection Regulation currently being scrutinised and altered by the legislative machinery of the European Union. If passed, the law will harmonise rights and responsibilities for data processors, controllers and subjects across 28 EU Member States, and extend to controllers outside the EU that (a) offer goods or services to EU data subjects or (b) monitoring them.

[GDPR Art 3(2)], thereby having widespread international implications.

METHODOLOGY

Our study, which brings together a multidisciplinary team, was developed in three phases:

Phase one: Consulting the legal community - We sought to identify aspects of the GDPR (EU General Data Protection Regulation 2012 Com Final 11) most likely to implicate the design community. This was achieved through deployment of a survey instrument to a small purposive sample of European data protection experts from the legal community. ***Phase two: Designing the cards*** - Having established the key principles, the second phase applied these principles to the development of a broader deck of ideation-style cards, and ***Phase three: Design workshops*** – The designed cards were tested with 21 designers through 4 structured workshops.

Phase 1- Consulting the Legal Community

In order to inform our ideation card approach, we investigated four specific areas of the GDPR. These were drawn, in part, from recommendations of the UK Information Commissioner Office, [29], on (1) *data breach notifications*; (2) *explicit informed consent*; the controversial (3) *right to be forgotten,* and (4) *privacy by design*. In order to establish the importance of these areas for systems design, we posed open questions to a highly targeted group of prominent UK data protection and privacy law experts. Seven legal academics were surveyed; primarily professors but also lecturers and doctoral researchers. The following section introduces each area and the challenges posed for designers, as highlighted by our experts.

Legal Area 1: Data Breach Notifications requirements are extended to all data processors in Article 31 GDPR. This builds on existing obligations that ISPs must notify data protection authorities, and data subjects, potentially within 24 hours when a data breach has occurred; i.e. data is accidentally or unlawfully destroyed, stolen, lost, altered, transmitted etc. [Article 2(h) PECD 2002]. Breach severity is key in determining what information should be conveyed, to whom, in what form, and how quickly [25].

The Challenge for Designers: Experts highlighted the importance of accuracy over speed of notification; i.e. proper time to investigate and inform the user of all facts in preference to frequent or incomplete warnings. Combatting 'notification fatigue' and helping users to differentiate between legitimate and fraudulent warnings were also noted challenges. The *post hoc* nature of breach notification concerned some experts. One stated: "*it's too late for autonomy after a breach has occurred*". Using reparation to coerce better security practices was also mentioned; "*the reputational harm of having to disclose a data breach should act as an incentive to improve data management*". However, relying on fines alone might result in these being seen as an acceptable 'business cost' rather than a punitive measure. Accordingly, we reflected these concerns in our card text; (a) reference to reputation damage, (b) the need for consideration of innovative approaches to notifications, and (c) ensuring breach information is accurate and within a short timeframe.

Legal area 2: Obtaining Informed Meaningful Consent is a significant challenge within Ubicomp systems [22,14]. Designing consent mechanisms that truly scaffold user understanding is a challenge which remains unaddressed by the dominant model of Terms and Conditions [21,22]. Article 4 (8) GDPR mandates a higher threshold of explicit, informed consent to data processing, requiring "any freely given specific, informed and explicit indication of… wishes … either by a statement or by a clear affirmative action". This raises questions as to how a system might remain ambient, yet still inform and obtain this higher threshold consent.

The Challenge for Designers: Our legal experts emphasised themes (a) how to obtain meaningful informed consent, (b) how to outline risks to users properly, and (c) how to allow them to withdraw their data. Designing mechanisms to truly give choice and inform, when users may not care, was perceived to be a challenge. One expert stated: "*Consent is an important part of the matrix of protections for autonomy and dignity but it must be informed … it is not informed consent to tick a box on a webpage or to agree to a privacy policy which you have not read.*" Many experts were critical of the nature and definition of informed legal consent as a concept, terming it 'illusory' and too 'fixed' in light of the complexity and dynamism of both the data processing landscape and human attitudes and control. It was felt that current approaches do "*not account for partial consent or revoked consent over a period of time. Often consent is not the issue, rather the lack of control re data collection is the issue.*"

Reflective of this, our cards hinted at the opportunities for creativity in addressing these requirements and stated that the form of information or delivery was not fixed, and that consent was a fluid concept requiring negotiation.

Legal area 3: The 'Right to be Forgotten'/ Right to Erasure (Article 17 GDPR) would grant a data subject rights to request the data controller stop further dissemination of data, and erase personal data relating to them, in certain conditions; e.g. when data is no longer necessary or consent is withdrawn. Here, US and EU perspectives have differed greatly. The US has voiced concerns over stifling free speech and creating censorship, whilst the EU has highlighted the importance of privacy rights [1,5]. For example, the recent European Court of Justice Google Spain Case [31] discussed balancing privacy interests of one individual against freedom of expression. In this case, Google was requested to remove website links in search results that related to an individual [23]. Other discussions focus on practical difficulties in implementation where copies may exist across different platforms and devices [11].

The Challenge for Designers: Our experts highlighted the challenge of balancing competing rights against the granularity of enforcement; e.g. the interests of archiving memories or complete and accurate records of one individual,

versus the right to be forgotten of another. One expert stated *"there are approaches that make it comparatively easy to forget but they tend to overreach, causing problems for other rights. …the worry is that over simplistic design solutions to the RTBF will overreach and harm social and political discourse."* Another expert prioritised privacy interests*; "the individual should be able to rip their data trail right off any Ubicomp system when consent is withdrawn"*. Overall, it was thought to be a valuable tool for empowering individuals. Practically however, whilst a few thought it was achievable, many wondered how it might work in reality. Reflective of this, our card text hinted at issues around balancing interests, difficulties in implementation and the technical decisions that shape this.

Legal area 4: Privacy by design (PbD) seeks to create information systems that embed privacy-enhancing solutions into the architecture. Article 23 GDPR defines this regulatory tool as the need to regard 'the *state of the art* and the *cost of implementation*...' to implement '*appropriate technical and organisational* measures and procedures in such a way that the processing will meet the requirements of *this Regulation* and *ensure the protection of the rights of the data subject*'.

The Challenge for Designers: Key design challenges from this include questions of (a) what the state of the art might be for these purposes (commercially available vs lab based technologies), (b) what an unreasonable cost of implementation (e.g. how high a percentage of overall costs) might be, and (c) what aspects of data protection/privacy should be prioritised (e.g. should there be greater focus on certain provisions depending on the context of the system, with deployment home vs public space?) Grounding such considerations through the design process is important. We sought the most detailed feedback on PbD and all experts agreed that it was an important sphere of investigation, despite a level of sematic uncertainty. Experts questioned whom the obligations are incumbent on (e.g. the designer, the manufacturer, etc.), and whilst bridging the gap between law and design is critical, one cautioned "*there is a danger to search for solely technical solutions at the expense of other measures, and to turn substantial debates about ethics and law into mere software design issues*" Experts prioritised; fair and lawful processing, purpose limitation for data use, proportionate data collection, and data subject access rights as key focus areas for ubicomp systems. These aspects were reflected within our text and divided across 2 cards. Having explained the design of our legal cards, the following section describes design of the wider deck.

Phase 2: Designing the Cards

Design of the card deck drew directly from previous work with ideation cards. As in the case of Freidman & Hendry [13] and Golembewski & Selby [15], we employed four sets of criteria, described 'suits' [15]. Taking the regulatory principles previously described, we developed a 5 card suite entitled 'Regulation'. In order to construct a deck, we added 3 factors regularly considered within the design process. These were (a) a specific system to focus group activity [30], (b) a series of user groups [30], drawn from groups from the 'edges' [10], and (c) a series of potential constraints for each system. The content of the 'constraints' and 'system' cards were generated during structured conversations with developers. The former were selected by participants to represent factors that, in their experience, typically constrained the design of data-driven systems. The latter describe systems that are, on the basis of participant input, either already in development or under discussion. Each suite featured 10 cards, making a total deck of 35. In-keeping with other card studies [13, 15] we also sought 'evocative' images, featured alongside the descriptive text.

Establishing the rules of the game

Friedman & Hendry found that a 'focused design activity' was instrumental in supporting participants to consider values. In light of this, our activity was constructed within strict parameters (temporal and systemic) to focus group attention.

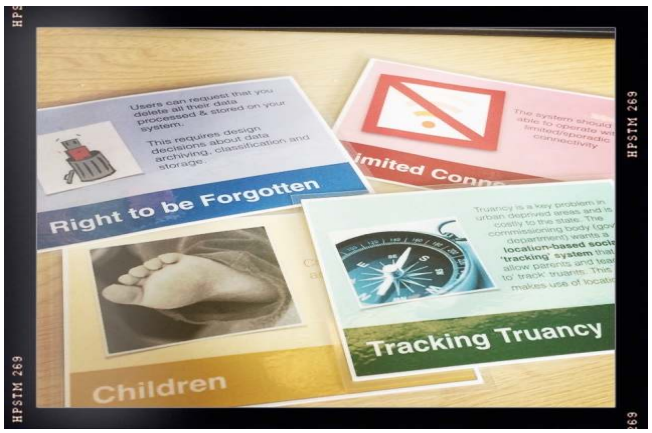

Figure 1. Examples from the four 'suits'

Creating Focus: This was established at the start of the activity with our 'System' cards. Suggesting a pre-defined system allowed us to frame and focus discussion. These cards described (a) the system function (b) the type of data to be collected, and (c) the type of organisation commissioning the work, For example: **Tracking Truancy:** *Truancy is a key problem in urban deprived areas and is costly to the state. The commissioning body (govt department) wants a location-based social 'tracking' system that will allow parents and teachers to' track' truants. This system makes use of location data.* Beyond those listed in Fig. 3, other systems included (a) a smart energy system, (b) a live biometric system for use in cinemas (c) a community-level energy monitoring system (d) a platform that allows users to sell the data generated at home, and (e) a live marketing system that provides targeted advertising on the street.

Phase 3: The Design Workshops

A series of four design workshops where held to trial the cards. The term 'designer' was used with little supporting clarification in recruitment in order to attract a broad range of participants. There were 21 participants in total, (16

Male/ 5 female). Participant specialisms included classifications of HCI, systems architects, a programmer and an engineer; years of experience ranged from a designer in the first year of his training to 16 years and system types included lab-based experiment systems to broadcast, online shopping, robotics, mobile apps, customer support, games, tracking systems, persuasive systems and databases. Participants were arranged into 4 groups.
Group 1 (G1): Most experienced, mixed specialism (predominately HCI)
Group 2 (G2): Mixed experience, mixed specialism
Group 3 (G3): Mixed experience, (predominately systems architects)
Group 4 (G4): Least experienced, mixed specialism

Groups 1 to 3 were each made up of 5 participants and group 4 including 6. Figure 2 shows the gender, years of experience of systems design, their specialism and knowledge of DP.

Ref	Gender	Yrs	Specialism	DP knowledge
G1_1	M	12	HCI	At university
G1_2	F	10	HCI	Through practice
G1_3	M	5-6	Sys Arc / HCI	At school
G1_4	F	4	HCI	Through practice
G1_5	M	16	HCI/ Sys Arc	Through practice
G2_1	M	1	HCI	Training at work
G2_2	M	9	Sys Arc /HCI	Through media
G2_3	M	10	Sys Arc	At university
G2_4	M	2-3	HCI	Through media
G2_5	M	11	Privacy expert	Expert
G3_1	M	10	Sys Arc	Training at work
G3_2	M	7	Sys Arc	At university
G3_3	M	4	Sys Arc	At university
G3_4	M	14	Sys Arc	Through practice
G3_5	M	2	Eng	Only aware
G4_1	F	4	HCI	At university
G4_2	F	2	HCI	At university
G4_3	M	5-6	Programmer	Through media
G4_4	M	2	Database	At university
G4_5	F	2	HCI	Only aware
G4_6	M	4.5	Sys Arc	Training at work

Figure 2. Participant profile

Experience of DP: Prior to the workshop, participants were asked about their DP knowledge (fig.2). We found that the majority of our participants had received only perfunctory training; 11 had experienced what they described as 'basic' awareness training at university, school, or at work. Three designers were only aware of stories in the media and 2 had only passing knowledge. Only 5 designers had a working knowledge; one participant was a DP specialist and 4 designers had developed knowledge of DP law through professional practice. Based on descriptions, DP knowledge was not systematically acquired, but rather *ad hoc*, limited or need-driven.

Cards	Group 1	Group 2	Group 3	Group 4
Syst'	Always on live wearable health device	Wearable cameras for shopping in store and home	Car that 'takes over' when sensing bad driving	Health device tied to medical records and store card
User	Everyone	Older People (65+)	Ex-offenders or those on probation	Women of all cultures and faiths
Const'	High level of user control	Limited connectivity	Low energy	Low cost
Const'	N/A	Low cost	Maximum Data	Minimal distraction
Reg	Right to be Forgotten	Data Processing	Explicit Consent	Privacy and Processing
Reg	Explicit Consent	Data Collection	Breach Notification	Breach Notification

Figure 3. Cards drawn by each group

Figure 4. Card Sorting Exercise (group 4)

Workshop Schedule: The workshops began with each group drawing 6 cards, blind, from the deck (see Fig.3). Friedman & Hendry and Mackay *et al*, both emphasise the importance of time in the ideation process; e.g. authors used a 3 minute sand *timer "to both symbolise and facilitate the possibility for meaningful use in a brief amount of time"* [13 p.1146]. In order to focus participant attention, our activity was strictly timed to 30 mins and participants were told when to turn each card. Upon the start of the game, designers drew 1 System card, 1 User card, 2 Constraints cards and 2 Regulation cards, laying them face down. They were asked not to turn the cards until instructed. Timing of the game began once the system card was turned. The User card, both Constraints cards, and finally both Regulation cards were turned, each after 5 minute intervals. After the turn of the Regulation cards, participants continued their discussions for the remaining 15 minutes. With the turn of each suite, designers were asked to consider the system they were designing in light of the newly turned cards. The principle function of the cards was to prompt and encourage reflection on aspects of DP law. By turning the regulation card last ('playing the legal card') we were able to infer whether the cards stimulated DP/privacy

concerns, or whether they were pre-existent. Thinking about the cards last, and therefore potentially having to rethink the nascent systems under design, primed the participants for the card-ordering task.

Card-ordering exercise: Having completed the structured activity, participants were asked to reflect upon the game overall, and the regulation cards in particular. This was catalyzed by a card-sorting activity. Participants were asked to collectively sort the cards they had worked with, in order of importance, for (a) concept, and (b) technical design. Feedback at the end of the activity for the first group suggested that it would be more realistic to have a greater number of constraints imposed upon designers. Subsequently, two cards were drawn by each remaining group.

RESULTS

Each workshop was video recorded and analysed within NVivo, using a thematic network analysis, which organised the coded text into three types of theme; (i) basic (lowest order, coded statements or beliefs that related to organising themes), (ii) organising (that cluster basic themes into organising issues) and (iii) global themes (super-ordinate themes that organise all codes into meta-groups or metaphor) [3]. Each workshop was coded separately and the resulting codes were compared to identify global themes. We give an overview of these themes in the following sections.

Not all designers are created equal

The strongest repeating theme throughout the workshops was the divide between those who classified themselves as systems architects, or programmers, and those who more closely aligned to HCI or research. The former group saw the responsibility for DP, and awareness of regulation, as unrelated to their role. From their perspective, the role of designer was to create a system aligned to its proposed function, unencumbered by external limitations such as regulation: *"When you're designing a system, at least for me, you always think of regulation as an afterthought. So, if I get what I want then I see how do I protect the user afterwards"* (G4_6).

Protection of whose interests

When engaging in the design activity, the theme of protecting interests was key. This subdivided into two categories; the interests of the user (data subject) and of whoever was responsible for the data (data controller). Groups 1, 2 and 4 began considering the protection of user data from the start of the activity – on the turn of the system card. In contrast, group 3 did not consider DP from the perspective of user protection until the turn of the regulation cards. They did, however, collectively opt to store user data locally on the system in order to protect *themselves* from any legal responsibility: *"If you know where an ex-offender is, you are in for a world of bureaucratic pain if the police come looking for that information. Whereas, if you can plausibly prove that you've no idea where they are…suddenly you are very much off the hook."* (G3_4). In this way, the turn of the regulation cards had most impact upon group 3. For example, user consent was not considered by this group until the turn of that card. Even after that point, their discussions were limited to forms of consent with which they were familiar; i.e. whilst designing a smart car they suggested that consent could occur at the point when the user sat in the driver's seat. Here, the information could be projected on the windscreen, and agreement occurring when the driver started the car. However, once the discussion developed, they became aware of the limitations of their proposed approach and began to see the need to think more creatively *"We've just designed the Ubicomp equivalent of terms and conditions haven't we?"**all laugh* (G3_3).

Where to keep the data

Designers across all groups consistently used the location of data as a mechanism for minimising risk. Equally, the role local storage as a means of augmenting user control over the data they generated was commonly employed. The rationale for this, however, varied. Again, group 3 tended towards the position that local storage enabled developers to protect themselves from liability and minimise the risk of physical harm befalling the user; e.g. if the system was allowed too much agency. Their concern did not initially extend to protection of the user from a DP perspective, though their discussions *after* the turn of the regulation cards led them to agree that such a model could also support the DP principles of breach notification and explicit consent: *"Anything to do with the command and control of the car is decided locally. But the data that it collects could be processed remotely"*. (G3_02)

Conversely, groups 1 and 2 tended towards the position that local storage would (a) allow the user a greater level of control, (b) would enable them time/space to review the data, and (c) make measured decisions about exposure in order and protection. *"That sounds really nice actually. There's not enough holding on to stuff...keeping it physically near you* (G1_02)…*"so, switching the roles of the whole kind of web cloud-based bit so that your server is the thing you carry around"* (G1_05). In this way, their tendency to focus on user requirements necessarily invoked the notion of protection. Group 4, having initially conceived an ambitious system that could collect highly sensitive biometric data and update live to the cloud, were limited by the turn of the constraints cards ('low cost' and 'minimal distraction'). This drew them to review their ideas and take a more modest approach. Their redesign, again favouring local data storage, made the turn of the regulation cards ('privacy & processing' and 'breach notification') much less problematic: *"Low cost made me think of less ambitious designs. In the beginning it was going to be in your bloodstream, monitoring everything and doing stuff and sending everything to satellites and then it was oh, this just means fitbits really"* (G4_06). Group reflections at the end of the process highlighted that it was only a lack of awareness of the breadth of regulation that

limited their desire or ability to incorporate such considerations at an early stage: *"That made it a bit more specific, the breach notification, the 24hr thing* (G4_1)….*Yeah, I suppose the one that would have freaked me out most would be the breach notification. I wasn't expecting it. Suddenly you'd have to design that in. That's quite scary."* (G4_2) Equally, considering DP as part of the design process, with specific users in mind, forced the groups to think in a more focused and creative way about possible solutions. For example, group 2 suggested supporting older people by automatically limiting data collection, linking it to location; so, when users entered a shop, data collection would be automatically turned on but would turn off as soon as they got home.

Revealing the user

Revealing the user card fundamentally altered the form of the system under discussion. Group 2 moved away from a permanently wearable solution to one that was wearable only during key points (such as in the store or at home) to reduce the cognitive burden and responsibility on the older user. Group 3 extended their system to include clearly defined data upload points in order to limit the liability of the company and enhance the privacy of ex-offenders and those on probation, and Group 4 sought design solutions that would enhance the ability of women of all faiths and cultures to control the flow of their data and limit access to those outside of the UK.

Group 1 was charged with designing an always on 'live' wearable health device for 'everyone'. In this case, revealing the user card elicited concerns over the possibility of designing a catchall product: *"well, you've got a failed product right there"* (G1_2)…"*designing for everyone you can't do"* (G1_5). Despite these concerns, the solution (to conceive a system that transmitted live biometric data to the cloud) elicited the most creative and complete design of all 4 groups. By having to design of everyone, Group 1 sought to envision a product that was highly customisable; a charm bracelet. This product would allow certain types of data to be transmitted, within user-defined contexts, through the physical act of clipping on components (beads). Individual beads being related to distinct data types. Their design choices were reinforced through the 'user control' constraints card and those two features (customisability and control) were applied to allow the user to indicate their explicit consent through the clipping on/off of the charms.

Everything starts from the (stereotypical) user

The default orientation of all of the HCI specialists, though not of the (single-specialism) system architects, was that user requirements should come first. All groups, except for group 3, asked whether they could turn the user card before they were asked to do so. Group 1 repeatedly stated that it made no sense to start designing a system without knowing 'who the user was'. During the card sorting exercise, groups 1 and 4 both clearly indicated that the user was as important in the conceptual design of the systems as the specification of the system itself. This was further raised during the card-sorting exercise. However, the orientation of Group 2 was somewhat different. Led by the privacy specialist, this group leaned towards the role of regulation as being to protect the user from themselves. This position was also reflected within Group 4: *"Regulations are there to protect the user from their own bad decisions. So even if the user wants something it doesn't mean they should get it just because they want it…like, you're not allowed to drive without a seatbelt even if it makes you're uncomfortable and you're an idiot. So, the government prevents you making that stupid decision through regulation."* (G4_6).

With the exception of Group 1 (who had drawn the 'everyone' user card), user requirements were seen to come first. However, when discussions of user characteristic began, highly stereotyped profiles of user traits, needs or behaviours emerged. For example, Group 2 both implied and explicated that their users (aged 65+) were frail, had poor cognitive and memory skills, were incapable of making reasoned decisions and were easily confused. *"In terms of having to turn it on and off …They might forget and then they turn it on and they're recording their whole day and everything else."* (G2_04). Upon turning their user card (ex-offenders and those on probation), Group 3 made the assumption that such users would want to conceal their activities, would be careless of others, and that they would reoffend. In contrast, Group 4 (women of all cultures and faiths) began by focusing their system (wearable monitoring health device) on specific cultural issues. One designer drew on their own cultural experience to describe how such a device might be used as a mechanism of control, by husbands, within more repressive societies. Therefore, if the system was worn abroad, there may be grey areas in terms of DP: *"Woman…have less control over their lives. Suddenly I see this tool as a tool for controlling their lives even more so that their husband can now have access to this information"* (G4_6)

Whereas the other groups reported a natural progression of their system design with the turning of the cards, Group 1 found designing their system incredibly difficult; both self-reported and through observation. However, the key characteristic of the system they created was that it was highly individualised and customisable. By not knowing who 'the user' was, they were forced to keep their design sufficiently flexible and adaptable to suit all needs. Equally, Group 1 was the only group not to fall back upon describing existing systems. Group 1 spent far longer discussing form than any of the other groups, and expressed greater concern over whether all potential users would accept their design; leading them to seek forms with high levels of customisability. In contrast, groups 2, 3 and 4 all made assumptions as to what would be acceptable: *"If your users are going to be everyone, you've got to think about the social acceptability of it"* (G1_1)

Exhibiting regulatory behaviour

When considering the Regulation cards, four key tensions arose. These were (a) meeting DP requirements was seen as

limiting to system functionality, (b) protection of the user through design was seen as distinct from conforming to regulation e.g. protection of the user was generally foregrounded, whilst DP regulation was set in the background and the relationship between the two was rarely identified, (c) securing meaningful and explicit consent was seen as incompatible with the desire for systems to remain seamless/unobtrusive from the user perspective, and (d) concerns over the necessary/required threshold of knowledge/understanding (DP competence) was repeatedly raised. It was clear that designers felt insufficiently empowered/equipped to reflect DP within their practice. However, despite this, their emergent design ideas automatically brought to bear elements of regulation though a *limiting or managing of the flow of data*. When reflecting on the commissioning body (detailed in the System cards), the majority of designers felt the need to build in control mechanisms to protect the user from external interests. The theme of control through design, as central to articulation of DP, was a dominant strand across all groups, particularly within groups 2 and 3. The concept arose in a range of contexts, such as the need (a) to design systems that directed, limited or focused user engagement or attention in particular ways, (b) for systems to enable users to be able to manage, delay and direct the flow of data from their local devices to the cloud or central system, (c) for a system to control unfettered access a company/organisation or central system might have to user data, and (d) the need to build in access control so that companies/organisations were not able to use data beyond the purposes expressly allowed by the user.

The Designer as regulator

The regulation of user behaviour was cast as a given or implicit function of design. However, when reflecting upon the role of the 'designer as regulator', the dominant feeling was that designers were currently ill-equipped to undertake that responsibility. This was attributed to low levels of awareness, skills, competence and confidence. Despite this, when ranking the importance of the cards to the design of systems, the regulation cards were positioned second in importance only to the system and user cards. This was true across all groups. The system and user cards were seen as both indivisible from each other, and of principle importance for consideration in the design process. The only group to rank the user as less important (in practice) was group 3.

Reflecting on regulation in the design process

Having completed both the 30-minute design activity, and the card sorting exercise, participants were asked to reflect upon the process. It was put to them that proposed changes in the law would locate the designer as more central to the wider regulatory landscape in the future. Groups were asked to consider their individual orientation to this statement and discuss it collectively. Overall, those groups with a more diverse spread of specialisms, and with more experienced participants (Groups 1 and 2), were more positively oriented to this proposition. They were also the groups who believed there to be a need to train/develop multidisciplinary or 'hybrid' designers who could perform the role of both concept design and systems architecture.

Discussions also raised a series of design factors that would become increasingly important for DP through design. Overall, the following suggestions were raised (a) designing for transparency of data flows but not necessarily transparency of systems, (b) a focus on data breach *detection* rather than breach notification - the focus on breach notification was seen as a weak work-around, given that the more complex and expensive issue was breach detection, (c) designing systems that meet user expectations in terms of data – e.g. not violating the context within which users expected their data to be used, (d) exploring different approaches to when and how data was released/exposed (e.g. linking DRM to personal data), (e) considering where 'windows for consent' might be designed into a system, (f) revisiting notice and how that might be redesigned for more pervasive systems, (g) designing for local data storage as default, and sharing/exposure as an exception, and (h) moving beyond the 'data dump' – e.g. beyond the simple narrative of making all data visible/accessible to the user, and instead considering how design might support individuals to make meaningful decisions about data sharing.

Engaging designers with regulation

When considering how designers might be engaged within the regulatory frame, a primary enabling theme was the need for the concept designer to have greater flexibility and control in the design process; particularly where system architecture was separated from conceptual design. It was also felt to be insufficient for DP to be a last consideration, or cast as something 'imposed upon design'. Rather, participants highlighted the need for it to be embedded in 'the institutional fabric' of the field. It was suggested that privacy and DP was currently 'under designed' due available 'off the shelf' fixes, leading designers to simply 'plug in' existing solutions rather than seeking creative alternatives. Despite recognised the value of DP through design, the idea of engaging designers in such practice was considered 'lovely in theory', but not realistic. Overall, there was felt to be a divide between the legal and design 'worlds', exacerbated by the absence of a common lexicon from which to draw. Group three was the only group not to feel the need for a closer drawing together of the fields. Instead, they preferred the model of working closely with an external legal expert, to ensure no laws were contravened. Others suggested the need for a new role - that of the 'regulation designer' who could be brought into a design team or called upon, much like an HCI specialist.

Reflecting on the cards: Overall, participants reflected positively on the cards and all felt they had been made aware of new aspects of DP. Discussions highlighted that they would be most effectively used as either an educational tool for those training to be designers, or as an ideation instrument for use within design meetings at the early, conceptual stages of the design process. Even Group 3 agreed that a greater

awareness of DP at an early stage would help with the overall design process. It was noted, however, that in order to be useful as design instruments, the cards would need to include a greater level of detail. For example, groups 3 and 4 both asked the facilitator for more explicit detail about the conditions of breach notification.

DISCUSSION

Legal scholars Brownsword and Yeung describe technology as a 'regulatory tool'. From this perspective, designers not only create systems to meet explicit regulatory purposes, such as criminal justice, but also implicitly regulate by affecting users through systems which "seek to, or have the effect of, shaping behavior" [7]. As designers, our job is to direct, nudge and channel user actions through the form and function of the systems we design. By incorporating knowledge of DP law from the start of the design process, the systems we release into the world can better ensure user protection. This position is not only increasingly recognised by legal scholars, but is reflected in the way regulation is being designed; e.g through the emergent PbD agenda. Whilst our participants recognised the need for DP, they did not necessarily see themselves as instrumental within the wider regulatory system. Instead, they cast regulation as an external force, which necessitated a level of *post hoc* compliance or compromise. Regulation, and more broadly law, was seen as something to be respected through systems design but its practical implementation was cast as the province of legal professionals and DP specialists. The ideation cards allowed us to challenge the nature of this discourse. Rather than seeing regulation as external and distant, it was placed within the initial framing of design. This was well-received by designers as an awareness raising exercise, and discussions highlighted a clear need for such an instrument; both as an educational aid and means to stimulate creative thought around DP at an early stage of the design process. Despite this, key themes arising from our analysis highlight some areas that require attention.

Engagement - Designing cards for multiple interests

'Design' is a catchall term that encompasses aspects such as conceptual, aesthetic, technical and functional design. As such, when we speak of 'designers' we are in fact invoking multiple, and often hybrid, tribes. Even where system design goals are the same, each tribe brings with it a distinct perspective and, as such, any ideation card approach will need to be highly customisable to context. The approach we took worked well for HCI and creative designers, where there was some familiarity with the function of cards in the design process. However, system architects were less convinced, requiring much more detail before they could comfortably engage. Equally, early career designers exhibited very low awareness of DP regulation, suggesting that there may be a need to engage them at an earlier stage in their training. Our next steps, therefore, will be (a) to develop a more detailed educational deck, aligned to undergraduate studies, in order to create awareness and begin stimulating creative thought around designing for DP, and (b) support the development of these cards into a more dynamic instrument to be used and further developed within multiple contexts.

Promoting Human-Centered Regulation

There are currently three 'modalities of design' in support of regulation [7]. These are those that (a) encourage behavioral change, (b) ameliorate the effects of harm-generating behaviour, or (c) totally prevent harmful behaviour. Whilst such approaches regulate human behaviour, they can result in a reduction of human agency, having a negative effect on accountability, transparency and participation [7]. These modalities, however, are drawn from existing practice based upon a narrow view of regulation. If designers were to be actively engaged in the regulatory frame, and explicitly promote a human centered perspective, we are likely to see a much broader range of creative solutions such as the charm-based and location-triggered data exposure solutions beginning to emerge during our study. There is a danger that, unless designers actively and knowingly participate, their work may ultimately be coopted. Upon reflection, our participants felt there was indeed a need for closer alignment between regulation and design, though they failed to see a natural connection between user experience/requirements and DP. We would argue that, given our designers' clear focus on the user, one solution would be to embed DP within user experience heuristics. For example, designers automatically sought to enhance user control over their data by privileging local storage over the cloud and focusing on mechanisms to limit upload unless it was user-controlled. It is reasonable to imagine that traction could be gained by linking aspects of DP to existing heuristics, such as 'enhancing user control'.

Addressing the skills gap

In the same way as Lessig argued that code could be law [20], so the form that technology takes can have an effect (intentional or otherwise) on human endeavor. Currently, such regulation is limited and somewhat binary; for example what can, or cannot, be done with a product or service through DRM. However, by drawing all designers into the DP field, more nuanced and aesthetic solutions can be achieved, such as the charm bracelet suggested by Group 1. Before this can become a reality, however, there is a pressing need to raise the skills, confidence and competence of designers in respect of DP regulation. Whilst the cards were intended to sensitise participants to DP issues, it was clear that in the case of less familiar aspects, such as breach notification, what was needed was further information, guidance and support. This could be achieved through the development of guidance notes to augment the cards, or through the emergence of hybrid specialists, as suggested by participants.

CONCLUSIONS

It is clear that, as things currently stand, designers struggle to engage with regulation. There is a pressing need to draw designers into the coproduction of meaningful DP heuristics. By taking a participatory approach it is likely that, not only will translation be more effective, but it could also result in greater likelihood of ownership and buy-in from the design community. Finally, we recognise that this study privileges a

European perspective on DP. It is our intention that this research be replicated within a US context, with further international studies planned in the future. However, keeping our cards close to our chest is not the way to proceed. We hope that by making our instrument available under the Creative Commons license (see designingforprivacy.co.uk), others will develop further the work we have started.

AKNOWLEDGEMENTS

This research has been supported by the following RCUK Grant No. EP/G037574/1, EP/G065802/1 and EP/M000877/1

REFERENCES

1. Ambrose, M., Ausloos, J. The Right to be Forgotten Across the Pond. *J Inform Pol, 3*, 1-23. (2013)
2. Are you a Data Controller? At http://www.dataprotection.ie/docs/Are-you-a-Data-Controller-/43.htm
3. Attride-Stirling, J. Thematic networks: an analytic tool for qualitative research. *Qual Res*. *1*, 3 (2001) 385-405
4. Barnard-Wills, D. Privacy Game. http://surveillantidentity.blogspot.co.uk/p/privacy-card-game.html
5. Bernal, P. The EU, the US and the Right to be Forgotten *In Gutwirth, S. Leenes, R. and De Hert, P. [Eds*] *Reloading Data Protection Multidisciplinary Insights and Contemporary Challenges*' Springer, 2014
6. Black J 'Decentring Regulation: Understanding the Role of Regulation and Self-regulation in a 'Post- Regulatory' World' (2001) 54 *Current Legal Problems* 103
7. Brownsword, R., Yeung, K. (eds), Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes. Hart Publishing, 2008
8. Camp, J. and Connelly, K. Beyond Consent: Privacy in Ubicomp Systems in Digital Privacy: Theory, Technologies and Practices (2007)
9. Cavoukian, A, Privacy by Design: The 7 Foundational Principles, IPCO, 2011
10. Dourish, P., Bell, G. *Divining a Digital Future: Mess and Mythology in Ubiquitous Computing*. MIT Press, 2011
11. Druschel, P. The Right to Be Forgotten - Between Expectations and Promise, ENISA 2012
12. Feick, R. & Werle, R. Regulation of Cyberspace. In Baldwin, R., Cave, M., & Lodge, M. [eds] *The Oxford Handbook of Regulation*. OUP, 2010, 523-547
13. Friedman, B. & Hendry, D. The envisioning cards: a toolkit for catalyzing humanistic and technical imaginations. In *Proc. CHI'12* ACM (2012)
14. Friedman, B. Lin, P. Miller, J.K. Informed Consent by Design in Cranor, L.F. and Garfinkel, S. (Eds) Security and Usability. O'Reilly Media Inc (2005) 503-529
15. Golembewski, M. Selby, M. Ideation decks: a card-based design ideation tool. *Proc. DIS'10.* ACM Press
16. IDEO. Method Cards for IDEO: 51 Card Deck to Inspire Design. At http://www.ideo.com/work/method-cards
17. ICO on Privacy by Design, 2014 http://ico.org.uk/for_organisations/data_protection/topic_guides/privacy_by_design
18. Langheinrich, M. A Privacy Awareness System for Ubiquitous Computing Environments. In *Lecture Notes in Computer Science 2498*, Springer 237–245 (2002)
19. Leenes, R "Framing Techno-Regulation: An Exploration of State and Non-State Regulation By Technology" *Legisprudence,* 2011, Vol. 5 No. 2, 143-169
20. Lessig, L. *Code V2.0*. Basic Books, 2006
21. Luger, E. & Rodden, T. An informed view on consent for UbiComp. In *Proc. UbiComp '13*. ACM (2013), 529-538
22. Luger, E. Rodden, T. Terms of Agreement: Rethinking Consent for Pervasive Computing *Interact Comput* 25.2 (2013)
23. Lynskey, O. Rising Like a Phoenix: The Right to Be Forgotten Before the ECJ *European Law Blog (*2014)
24. Mackay, W. The Interactive Thread: Exploring Methods for Multi-disciplinary Design *In Proc. DIS'04*. ACM (2004)
25. Manson, C G. and Gorniak, S. Recommendations for a methodology of the assessment of severity of personal data breaches, ENISA, 2013
26. Mayntz, R. The Changing Governance of Large Technical Infrastructure Systems in: Mayntz, R. (ed.): Über Governance. In Stitutionen und Prozesse politischer Regelung, Schriften aus dem Max-Planck-Institut für Gesellschaftsfor-schung, Campus (2009), 121-150
27. OECD. *The OECD Privacy Framework*. OECD Publishing (2013)
28. Stahl, B.C. Responsible research and innovation: The role of privacy in an emerging framework. *Science and Public Policy*, 2013, 40 (6), pp. 708-716
29. Smith, D. One small step for EU Parliament could prove one giant leap for data protection. ICO. At. http://ico.org.uk/news/blog/2013/one-small-step-for-eu-parliament (accessed 13.03.14)
30. The Security Cards. At http://securitycards.cs.washington.edu/index.html
31. C-131/12 Google Spain v AEPD and Mario Costeja Gonzalez
32. US Federal Trade Commission, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers, 2012 pp. 22-32
33. Yeung K. Design for Regulation in J van Den Hoven et al (Eds) *Handbook of Ethics, Values and Technological Design*, Springer, 2014