Towards User Centric Regulation: Exploring the Interface Between Information Technology Law and Human Computer Interaction

By Lachlan David Urquhart

Thesis submitted to the University of Nottingham for the degree of Doctor of Philosophy

September 2016

Abstract

This thesis investigates the role of technology designers in regulation. Emerging information technologies are complex to regulate. They require new strategies to support traditional approaches. We focus on the use of technology design as a regulatory tool. Whilst this solution has significant conceptual traction, what it means in practice is not clear. Deeper investigation of the role of the design community in regulation is necessary to move these strategies from theory into practice. We structure our analysis by asking: how can we understand the role of designers in regulation of emerging technologies?

We answer this question from four primary perspectives: conceptual, legal, practical and design. We situate our investigation within the context of the domestic internet of things and information privacy by design. We adopt an overtly multidisciplinary approach, critically assessing how to bring together the human computer interaction and information technology law communities. To do this, we utilise a range of qualitative methods, including case studies, documental and legal analysis, semi structured expert interviews, questionnaires, focus groups, workshops, and development, testing and evaluation of a design tool. Our contributions are as follows:

Conceptually, we provide a critical investigation of the role of technology designers in regulation by consolidating, evaluating and aligning a range of theoretical perspectives from human computer interaction (HCI) and information technology (IT) law. We draw these together through the concept of user centric regulation. This concept advocates a user focused, interaction led approach to position the role of designers in regulation. It draws on the turn to human values and societal issues in HCI, and the increasing reliance in IT law on design for regulation of emerging technologies.

Legally, we present two detailed case studies of emerging technologies (domestic internet of things and smart metering) mapping the emerging legal landscape and challenges therein. We situate the role of designers, as regulators, within this space, and show how they can respond accordingly through their user centric focus.

Practically, we analyse experiences from leading experts in technology design and regulation to understand the challenges of doing information privacy by design (PbD) for the IoT. We present our findings within the framing of technological, business and regulatory perspectives.

Lastly, we present a design tool, 'information privacy by design cards', to support designers in doing PbD. This tool has been designed, tested and refined, providing us with a practical approach to doing user centric regulation. Based on our findings from using the cards, we provide the concept of regulatory literacy to clearly conceptualise the role of designers in regulation.

Keywords

User Centric Regulation; Information Technology Law; Human Computer Interaction; Privacy by Design; Internet of Things; Smart Metering

Acknowledgements

I offer my sincere thanks and gratitude to many great people who have supported me throughout my PhD.

Firstly, to my supervisors Professors Tom Rodden and Lilian Edwards for all your guidance, advice and kind support over the years, helping me to navigate the world of multidisciplinary research.

To Professor Andrew Adams for your mentorship and for kindly hosting me as a visiting researcher at the Centre for Business Information Ethics, Meiji University, Japan.

To those who have guided me over the years, especially Prof Derek McAuley; Prof Steve Benford; Dr Richard Mortier; Dr Ewa Luger; and Dr Stuart Moran.

To all my participants who kindly gave their time and effort.

To the Research Councils UK, Engineering and Physical Sciences Research Council, Mixed Reality Lab and Horizon Centre for Doctoral Training for funding this research.

To my fellow Horizon and Mixed Reality Lab colleagues whom I have worked with over the years, in particular, my friends Dimitri Darzentas, George Filip and Dr Gilad Rosner.

To my family and friends, especially my parents Anne & David and brother Struan for all your support and love.

To Diana for all your patience, love and companionship.

Lachlan David Urquhart

September 2016

Table of Contents

List of Figures and Tables

Figures

Tables

Abbreviations

A29 WP	=	*Article 29 Working Party*
ACM	=	*Association for Computing Machinery*
DAPF	=	*Data Access and Privacy Framework*
DCC	=	*Data Communications Company*
DP	=	*Data Protection*
DPD	=	*EU Data Protection Directive 1995*
GDPR	=	*EU General Data Protection Regulation 2016*
HCI	=	*Human Computer Interaction*
ICO	=	*UK Information Commissioner Office*
IEEE	=	*Institute of Electrical and Electronics Engineering*
iPbD	=	*information Privacy by Design*
IoT	=	*Internet of Things*
IT Law	=	*Information Technology Law*
NDA	=	*Non-Disclosure Agreement*
PIA	=	*Privacy Impact Assessment*
PbD	=	*Privacy by Design*
RTBF	=	*The Right to Be Forgotten*
SEC	=	*Smart Energy Code*
SME	=	*Small and Medium Sized Enterprise*
UCR	=	*User Centric Regulation*

Chapter 1. Introduction

This thesis investigates the role of technology designers in regulation**.** Emerging information technologies are complex to regulate requiring new strategies to support traditional approaches. We focus on one solution: the use of technology design as a regulatory tool. Privacy by design (PbD) is a key legal example of this, as it mandates information privacy risks to be addressed within the design process for new products and services. Whilst this solution has significant traction, as we shall show, what it means in practice is not clear. To move these strategies from theory into practice, we argue that deeper investigation of the role of the design community in regulation is necessary.

In responding to this, our overarching research question is: **how can we understand the role of designers in regulation of emerging technologies?**

To answer this, it is not sufficient to look purely from a technology regulation or design perspective. We require critical assessment of how to bring two communities together, the creators and the regulators of technology, to explore how concepts and knowledge can flow between them. Within this thesis, we do this through the proposed concept of 'user centric regulation', developed from a conceptual and practical investigation of the fields of human computer interaction and information technology law. We adopt an overtly multidisciplinary approach, utilising a mixture of qualitative methods and following four lines of inquiry: namely, conceptual, legal, practical and design. To situate our narrative, we now outline the aims, objectives, areas of focus and the structure for each of the four parts and ten chapters.

Part I - Conceptual Perspectives

The aim of **part one** is to provide the conceptual backbone of the thesis, by conducting a critical examination of prominent theories that sit at the boundaries of information technology (IT) law and human computer interaction (HCI). Our underlying objective in this part is to understand **how we can conceptually align IT law and HCI to situate the role of technology designers in regulation?** We

do this by interrogating the respective epistemological commitments of each community and to critically question the barriers, gaps and commonalities between their respective theoretical underpinnings.

The move towards greater interaction between the technology regulation and design communities means we need to understand how they can best work together. Before turning to practical perspectives in later parts, their role needs to be situated conceptually. The IT law community has long recognised technology can be a regulatory tool to shape behaviour. Regulation as a concept has broadened, both in motivations and the actors involved, hence we need deeper assessment of how design fits into regulation. This involves an explicit turn to those who create the technologies, where designers are now regulators. However, as technology designers are not conventionally involved in regulation, the nature of their role is not well defined. A significant strength of HCI, as a field of design, is the proximity of such designers to users. They focus on the contexts of technology use, reflecting the interests and environment of end users in order to design better systems.

We want to investigate what role HCI designers can play when focusing on regulatory dimensions of users interests too. Part 1 assesses how open HCI is to incorporating regulatory considerations. We do this by looking to dominant ideas in HCI and IT law to understand areas of crossover and alignment. We start the process of building a solid, shared conceptual basis between the fields, and to assist with clarity, we pull together our findings and present them within a new concept: 'user centric regulation' (UCR).

We briefly sketch the foundations of UCR as a concept here.

UCR builds on the respective turn in technology regulation to design, and the turn in design to societal implications of technology. UCR explicitly links and extends these shifts, arguing for increased incorporation of legal values into design by developing the existing focus on human values in HCI. UCR represents an express alignment of the two fields of HCI and IT law and it formalises the process of building a shared conceptual basis between them. This develops from our critical reflections conceptualising the role of designers in regulation. UCR recognises HCI

designers need legitimacy as regulators, and proposes this can emerge from their proximity to end users. HCI tools for understanding user relationships and interactions with technology can be extended to develop a richer picture of how regulation manifests in practice for users and allow designers to respond accordingly. This needs particular focus on end user legal rights, and related designer responsibilities. Through design, legal challenges can be considered earlier, making law more prospective than retrospective, offering scope for compliance with laws to be built into systems. However, UCR needs to go beyond just compliance, where ethical dimensions of designers are key too. Accordingly, structuring reflection and action by designers on the nature of their legal and ethical responsibilities to users is critical.

Doing UCR in practice requires deeper understanding of legal, practical and design perspectives. Accordingly, in the remainder of the thesis, we situate our analysis of the role of designers in regulation through the specific context of information privacy by design for the domestic internet of things. We turn to more detail on these below, briefly conclude with structure and approach for Part 1.

Our approach is a critique and analysis of a range of academic material from the boundaries of IT law and HCI. Accordingly, we consider a vast range of sources primarily from engineering and computer ethics, information technology law, regulation theory, human computer interaction, social systems theory, and science and technology studies (STS). The consolidation is a contribution, aligning otherwise disparate theories, often coming from distinct epistemological perspectives. Indeed, by adopting a critical position, we question and deconstruct established concepts within HCI and IT law, with the goal of understanding how they can be aligned. For example, our critique of technology regulation theories questions the dominant social systems theoretical approaches, arguing that to understand the role of design in regulation needs a turn to more interactionist, phenomenological perspectives of HCI. In chapter 2 we present and critique a number of theories from IT law, regulation theory and social systems theory. We look at the broadening of the concept of regulation, situating the role of designers as regulators therein and unpacking challenges they face, such as lack of authority and legitimacy. We then look at how design is currently understood in IT law and

argue it needs to move beyond its social systems theory roots by following shifts in the Scandinavian School of Participatory Design. In chapter 3 we focus on the broadening of human computer interaction and increased engagement with social implications of technology. We look to computer and engineering ethics to help understand responsibilities of designers to regulatory interests of end users and propose the focus on human values in HCI be extended to law. We conclude by proposing the concept of user centric regulation.

Part II - Legal Perspectives

The aim of Part 2 is to explore the regulatory challenges designers will face in doing user centric regulation and to understand how they can respond accordingly. Therefore, our aim in this part is to understand: **what are the regulatory challenges designers face in the context of doing PbD for domestic IoT and smart metering, and how can they respond?** We use two detailed case studies to contextualise our discussions: the domestic internet of things and smart metering. We focus on the regulatory backdrop of data protection law, specifically the requirement of information privacy by design. We consider how designers can respond to two legal challenges: ensuring user control and appropriate access around personal data for IoT and smart metering respectively.

To provide greater detail on the approach within our case studies, firstly we analyse the nature and development of these technologies, the underpinning regulatory landscape, issues users face living with these systems and the legal challenges that surround their use. For smart metering we analyse the **UK Government Smart Meter Implementation Programme (SMIP),** and for the domestic Internet of Things it is the **Works with Nest IoT device ecosystem.** These two case studies were chosen due to their differing regulatory backdrops, where smart meters are part of a government led programme and IoT is largely market led.

To assist with clarity and to further conceptualise our analysis, we develop diagrams that map the personal data ecosystem focusing on the interactions, relationships and personal information flows between users, designers, technologies and third parties. We use these to inform our legal analysis on ensuring user control and

appropriate access around personal data, to understand the types of legal challenges designers as regulators need to engage with in doing PbD, and UCR more generally.

We conclude by proposing responses designers can take to address these regulatory challenges and do UCR in practice. For the IoT this involves considering how to **redesign consent mechanisms using the 'trajectories framework'** (Benford et al, 2009), an approach normally used for designing user experiences within human computer interaction. For smart metering we focus on how HCI designers can use methods like **tracking provenance of data and personal data vaults to give users greater control over who accesses their consumption data.** This provides deeper insight into the nature of the role of designers as regulators.

Methodologically, the case studies and analysis develop from a number of approaches. Primarily it is **extensive documental analysis** of research papers, government, industry and third sector reports, technology installation guides, European and UK law and policy documents (eg DECC, European Commission etc), sales and service contracts, websites, standards etc. Other elements include **informal conversations** whilst being a legal researcher in a human computer interaction lab, **cross disciplinary academic networks and research visits** such as a two month trip to Meiji University in Japan to conduct research on security and privacy issues of smart metering; **presentations and discussions** at numerous international and domestic conferences, and **workshops, seminars and lectures** over the PhD in different disciplines and multi-stakeholder forums (eg small to medium enterprise/start-ups, multinational industries, government, regulators, academia, third sector).

The structure in Part II is as follows. In chapter 4, we critically assess the nature of PbD, considering challenges it faces generally as a concept and how it is legally formulated in Article 25 GDPR. In Chapter 5, we characterise the Internet of Things, situating the trend within predecessor technology visions and highlighting lessons therein. We look at regulatory challenges and user experiences of domestic IoT, particularly with home energy and security devices. We look at personal data flows in IoT ecosystems, reflecting on human rights vs ownership led approaches to increasing user control and mapping how designers can respond by redesigning

consent mechanisms within the IoT. In chapter 6 we map the nature of smart metering, regulatory challenges and user experiences, how access is regulated in the government led programme, and how designers can respond to increase user control over access to consumption data.

Part III - Practical Perspectives

The aim of this Part is to go beyond the conceptual and legal perspectives, to understand the practical challenges in doing UCR, by looking at **doing PbD for the IoT**. We do this by exploring the experience of **thirteen** leading UK experts in information technology law and design. We use semi structured interviews to give us much deeper insight into **how** to align these two communities, by considering perspectives of thought leaders from each.

Accordingly, our high level research objective is to consider: **What are the challenges to be addressed in order to realise PbD for IoT in practice?**

Design and regulation do not operate in vacuums, hence we turn to the actors and their practical experience. We speak to those with a range of different areas of expertise, from a variety of sectors, and levels of experience. The seven 'technologists' have an average of **32 years** of professional experience. We speak to a range of expert participants, some with decades of experience in the IT sector, and many who are now working at a strategic level. The six 'lawyers' have an average of **14 years** of experience, with many participants working across areas of technology law like contracts, data protection, intellectual property, procurement and outsourcing, dispute resolution, and litigation.

We focus on a wide range of issues including the roles and relationship between these communities and practicalities of compliance with privacy by design, the internet of things and smart metering in their professions. Following our case studies, we focus on privacy by design, and the Internet of Things (where smart metering emerged as a theme). The questions broadly revolve around:

- definitions and regulatory challenges of IoT;

- nature and understanding of PbD, including reception in their industry and practical challenges it will bring,
- solutions to regulatory challenges of IoT and role of designers in regulation and protection of end user rights therein;
- practical challenges engaging with law or design (respectively).

Part III is Chapter 7, where we consider our empirical findings in detail. We look at the nature of IoT in practice and the regulatory challenges therein, particularly for data protection and privacy, consent, managing flows of information and end user rights and system designer responsibilities in data handling. We look to realising privacy by design in practice, focusing on challenges in defining what it is, motivations for doing it and engaging with underlying business models. We focus on topics like differentiated resources between SMEs, start-ups and multinational firms to do PbD, how to ensure effective communication and engagement between designers and lawyers, and challenges to be overcome around legal language. We then look at compliance in practice, considering the changing relationship, roles and interaction between lawyers and designers therein. We conclude by assembling our findings under distinct business, regulatory and technology perspectives.

Part IV - Design Perspectives

Our aim is to understand how to support designers doing PbD, as a form of UCR, in practice. As we have explored, PbD explicitly involves technology designers in regulation. They need to consider information privacy risks of a technology as early as possible in the design process, ideally before anything is built or comes to market. However, doing PbD in practice is complex, as we see in Part III. One element is finding design tools to support designers' engagement with law and their role as regulators. This section unpacks one approach we have designed, tested and evaluated with designers: **information privacy by design cards**. These are based on the new EU General Data Protection Regulation (GDPR), and translate the law into a more accessible medium: physical playing cards. We use these cards to understand how to support PbD in practice.

Accordingly, our high level objective is to understand: **how can we support technology designers' engagement with data protection law in order to do PbD in practice?**

Our playing cards are developed to support designers' engagement with data protection in a structured manner, to move PbD from theory into practice. We have tested these cards in a series of **six** workshops with **twenty-four** technology designers from a large global media firm ("MOZ"); a small technology businesses trade association ("SBA"); and an innovation network centre for SMEs/start-ups ("INC")). We investigate the utility of the tool by asking those who will use it for feedback. They help us build understanding of how designers, as non-lawyers, respond to legal concepts, where strengths lie, where greater support is needed, and what is necessary to enable them to act effectively as regulators, and make PbD a reality. We contextualise the role of designers through the proposed concept of **regulatory literacy** which assesses how designers interact with **regulation, their sense-making strategies and how they manage complexity**.

A range of methods have been utilised in the development and testing of the different iterations of these cards. Questionnaires, focus groups, practical workshops, card sorting exercises and informal discussions have all played a part.

The structure of this part is as follows. In chapter 8 we present the development process for the cards, both for an original prototype deck and a newer, wider full GDPR deck. We also outline findings from workshops with the prototype deck, and how these informed the development of the newer deck. We outline the methodological approach for testing and evaluating the cards, discussing the development and approach for our data collection through questionnaires, focus groups, and workshops using the cards. In Chapter 9 we present findings from our questionnaires, workshops and focus groups. We document the motivations for participants' engagement with DP law, their reflections on the cards, their prior experience and strategies for engaging with DP. This chapter ties together our findings under the model of **regulatory literacy**. This builds on the three elements, documented above. With **regulatory interaction,** we look in more detail at how participants negotiate around legal concepts, particularly how they contend with

legal language and definitions, and how the cards support their interactions with law. With **managing complexity**, we look at the responses of participants to law, such as their pragmatic, user centric approaches to balancing compliance risk and technology utility. With **sense making strategies**, we look at the practical support mechanisms within SMEs, start-ups and large organisations for doing PbD in practice, what role the cards play in raising participant awareness, and where further support is necessary.

Publications and Conference Presentations

A range of publications and conferences have emerged from this PhD. Discussions at conferences, doctoral schools and workshops have shaped the narrative and approach of the PhD too. Accordingly, we present a list of relevant work below.

Publications

- (Forthcoming - Accepted) with T. Rodden (2016), New Directions in Technology Law: Learning from Human Computer Interaction, Special Edition of *International Review of Law, Computers and Technology: Justice in Algorithmic Robes*, 1-34.

- (Forthcoming) White Noise from the White Goods? Embedded Regulation for Ambient Domestic Computing, B Schafer, L Edwards, E Harbinja, (2016) *Future Law,* Edinburgh University Press

- (Forthcoming – Under Review) with T. Rodden (2016) A Legal Turn in HCI: Towards Regulation by Design for the Internet of Things, *Working Paper on SSRN*, 1-38.

- with D. Darzentas (2015) Interdisciplinary Reflections on Games and Human Values, *Proceedings of ACM CHI Play '15*, p805-810[1]

- with E. Luger (2015) Creative Compliance and the Rise of Designer as Regulator" *Computers and Law: Special Edition on Smart Cities*, 26(2) p9-11

- with E. Luger, T. Rodden, M. Golembewski (2015) Playing the Legal Card: Using Ideation Cards to Raise Data Protection Issues within the Design Process, *Proceedings of ACM SIGCHI '15*, p457-466

- (2014) Bridging the Gap Between Law and HCI: Designing for Effective Regulation in Everyday Ubicomp Systems, *Proceedings of ACM UbiComp'14 (Adjunct),* p355-360

[1] Associated Grant - EPSRC Digital Economy Network Grant with D. Darzentas for Workshop at CHI Play – 'Using Games as a Research Method to Explore Human Values, October London 2015 - EP/L011891/1

Selected Conference Presentations

- **20th May 2016 – Invited Speaker**, Doing Information Privacy by Design: Engaging Technology Designers with Regulation, *Data PSST! ESRC Seminar Series,* Bangor University, Bangor, UK - position paper on website

- **5-6th May 2016** - **Invited Speaker,** Multidisciplinary Reflections on Regulation and the Internet of Things, *Internet of Things and Cybersecurity Conference*, Royal Holloway University, London, UK

- **21-23rd April 2016**, Regulation by Design for Ambient Domestic Computing: Lessons from Human Computer Interaction, *7th Biannual Surveillance and Society Conference,* University of Barcelona, Barcelona, Spain (PhD studentship awarded)

- **11-12th April 2016**, Privacy by Design and the Internet of Things: From Rhetoric to Practice using Information Privacy Cards, *31st Annual BILETA Conference* 2016, Hatfield, University of Herefordshire, UK

- **25th Jan 2016 –** with E. Luger, Privacy by Design in Action, 2 Know How Sessions for *UK Information Commissioner Office*, Wilmslow, UK

- **10th Dec 2015 -** Privacy Ideation Cards, *BBC/Horizon Workshop*, University of Nottingham, UK

- **4th October 2015 – Workshop Organiser**, Interdisciplinary Reflections on Human Values and Games, *CHI Play 2015, University College London, UK*

- **18-23rd April 2015** - with E. Luger, Playing the Legal Card: Using Ideation Cards to Raise Data Protection Issues within the Design Process, *ACM SIG CHI 2015*, Seoul, South Korea

- **16th April 2015 - Invited Speaker**, Smart Meters, Home Automation and Regulation, *Centre for Business Information Ethics,* Meiji University, Tokyo, Japan

- **8th Dec 2014, Invited Speaker**, Smart Energy Infrastructure: Privacy and Security Concerns, *Scottish Privacy Forum* Smart Cities Symposium, University of Stirling, UK

- **11th - 17th September 2014**, Bridging the Gap Between Law and HCI: Designing for Effective Regulation in Everyday Ubicomp Systems, *UbiComp '14,* Seattle, WA, USA – (Poster; Published Extended Abstract in Adjunct Proceedings; Travel Scholarship)

- **10-11th July 2014**, The intersection of EU Data Protection Law Reform and everyday ambient computing design: challenges and opportunities, *Easy Privacy, 4th International Asian Privacy Scholars Conference*, Meiji University, Tokyo, Japan.

- **14-16th April 2014** - Bridging the gap between law and technology design: the challenges of ubiquitous computing, *BILETA 2014*, University of East Anglia, UK

- **16-17th September 2013** – Presentation and Poster – The Persistence of Memory: Towards the Synchronic Society, *Gikii VIII*, University of Bournemouth, UK

- **Doctoral Schools**

  - **12 -15th July 2015** - The Digital Economy Web Science and Big Data Analytics Summer School 2015, University of Southampton, UK

  - **30th June - 5th July 2014** - Microsoft Research Summer School, Cambridge, UK

  - **11th September 2014** - ACM Ubicomp 2014 Doctoral School, Seattle, WA, USA

  - **3rd-8th February 2013** - Doctoral Training School, Centre for Research Information, Surveillance and Privacy (CRISP), University of Stirling, UK

  - **10-11th July 2013** - Digital Economy Summer School, RCUK Digital Revolutions, University of Oxford, UK

Part I Theoretical Perspectives: Questioning the Relationship Between Law and HCI

Part Overview

In this part, we theoretically explore how to bring law and HCI closer together. It culminates with the proposed concept of 'user centric regulation' (UCR). We argue that increased practical and conceptual support is needed to help designers participate in regulation. This part of the thesis focuses on the conceptual element, building understanding of how these two communities can work together.

Technology designers are increasingly being called upon to act in a regulatory capacity by the law. A key example is the GDPR provisions on information PbD. Due to the proximity of HCI designers to users in systems design, these regulatory commitments will increasingly fall to them. However, as designers are not conventionally involved in regulation, the nature of their role is not well defined, and traditional regulators may not fully appreciate their practice. A significant strength of HCI is the user centric focus and we want to investigate the role they can play when thinking about the regulatory dimensions of users.

The move towards greater interaction between the technology regulation and design communities means they need to understand how they can best work together. This requires linking together their respective epistemological commitments to increase common knowledge. This section does this by critically questioning the barriers, gaps and commonalities between the theoretical underpinnings of each community. We narrow our endeavour firstly by concentrating on relevant ideas from HCI and IT law, and secondly, on theories that are amenable to crossover and alignment between these communities.

The novelty of this section stems from the consolidation, critique and linking of otherwise disparate concepts. Bringing them together starts the process of building a solid, shared conceptual basis. To assist with clarity, the findings from our inquiry are pulled together and framed within a new concept: 'user centric regulation' (UCR). We develop the details of UCR in chapter 3, and in subsequent parts we

unpack the **practical** and regulatory challenges HCI designers will face in doing UCR. But first the **conceptual** work needs to be done.

Structure

In Chapter 2 we present and critique a number of theories from the domain of law and regulation, situating these in the context of privacy by design for the IoT. Generally, we argue that regulation as a concept has broadened, both in motivations and the actors involved, and now designers can be seen as regulators.

We need to unpack what this means theoretically, particularly the nature of this new role and the interaction with traditional state regulation. For user centric regulation to become a reality in practice, we need critical reflection on how to align the HCI and technology regulation communities. In part, this means moving past systems theoretical models that dominate in IT law to HCI models that focus on user interactions with technologies in context.

In Chapter 3 we turn our attention to approaches seen in design and human computer interaction that are amenable to crossover with law. HCI as a discipline has long interacted with other disciplines, and there is an increasing willingness from the community to engage with and reflect on the broader social and ethical aspects of technology. The nature of responsibility and role designers play is still being settled, but technology ethics assists understanding of the nature of the role. We identify the line of work on bringing human values into design as a key route for bringing legal and regulatory issues into HCI. We conclude by pulling together the critique from the prior two chapters in our proposed concept: user centric regulation.

Managing Definitions

We do not provide top down, absolute definitions of designers or regulators in this thesis. Instead, a process of reflection between the law and technology design communities needs to occur, mapping perceived borders between them, wherever these may lie (or not). Any definitions should emerge **from, within and most importantly, between** these two communities.

That being said, for purposes of navigating the thesis, descriptive handles help. Accordingly, by designer we mean those involved in the **creation** of technologies. Design is broad, encapsulating many different domains like product, service, fashion, web, graphic, or game design. We have HCI designers in mind, which we sweepingly frame as those **closest to and most focused on the end users**. This is more likely to be the requirements engineers or user experience (UE) specialists as opposed to the systems architects or algorithm designers in the design process. However, whilst we often use the label HCI designers in this work, there are a wider range of actors involved. Our privacy by design card workshop attendees, for example[2] show the breadth of actors involved in technology design, ranging from professionals in technology, creativity and design; business strategy and management; and researchers (see table 10). As we discuss in parts 3 and 4, the contexts of technology design vary greatly, as do the resources and actors involved. This underpins our reluctance for creating absolute definitions.

Equally, for regulators, as we see in Chapter 1, definitions are broad. Nevertheless, we have in mind those who **create, interpret and enforce** rules. They may be from the **state** like the various arms of government, i.e., legislator, executive and judiciary, law enforcement bodies, and the criminal justice system. Equally, **non-state** actors like multinational companies, corporate governance, policymakers, legal profession, lobbyists (industry, NGOs, charities etc.) also have their part to play, as we discuss below. In Chapter 1 we look briefly at why we focus on the term regulation, as opposed to governance.

To stress again, these are by no means absolute, and merely for descriptive purposes.

[2] Workshops targeted at those involved in design of technologies

Chapter 2. The Broadening Nature of Regulation

We present and critique a number of theories from the domain of technology law and regulation, drawing on the context of privacy by design for the IoT. We argue that regulation as a concept has broadened, both in motivations and the actors involved. There is an explicit turn to the role of design when regulating emerging technologies to the extent that those who build these technologies can now be seen as regulators.

We firstly need to consider **why technologies are regulated in the first place, and why the turn to designers.**

There are a vast number of reasons why regulation is needed, varying from ensuring competition and guarding consumers from monopolies in the market, ensuring adequate information about products or ensuring protection for human rights like privacy (Baldwin, Cave and Lodge, 2011, p16-24). With regulation **of** emerging technologies, like IoT, challenges often emerge for state regulators and law, partly because the regulatory subject is shifting and the pace of regulation, particularly legislation, is slower (Reed, 2010).[3] Innovative responses are needed to ensure effective regulation of these technologies, often balancing a range of dimensions such as the nature of technology,[4] stage of life cycle, whether fundamental science or product,[5] and the regulatory tools being used, by whom and how (Jaap Koops, 2010). Indeed, many stakeholders are involved in regulation of technologies, both state and non-state entities, and accordingly many different strategies have emerged such as state led technologically neutral legislation eg EU's Regulatory Framework for Electronic Communications or new GDPR[6], industry led self-regulatory codes

[3] For a good example of this see Reed (2010) discussing the EU eSignatures Act
[4] Everyday technologies or emerging NBIC's - nanotechnology-biotechnology-information technologies-cognitive technologies
[5] See the 'Collingridge Dilemma' i.e. regulating a technology in its early stages is hard as there are many unknowns, yet once it is better developed, regulation becomes more-costly and change more difficult.
[6] http://ec.europa.eu/justice/data-protection/document/factsheets_2016/factsheet_dp_reform_technological_developments_2016_en.pdf

eg IPSO[7] Editors Code of Practice or hybrid co-regulatory strategies where self-regulation is overseen by government eg NOMINET[8] (Marsden, 2012).

In particular, regulation **through** the technology itself is key option, as it enables regulatory norms to be reflected in the architecture. We delve into the challenges of this approach throughout this section, but importantly it calls upon the design community, as those who build these systems, to respond to regulatory challenges of technology. Below we briefly introduce privacy by design as an explicit example of this i.e. a regulation mechanism to protect the human right of privacy in personal data driven technologies. Following this, we look in more detail at the interaction between legal and design communities around regulation, particularly questioning the nature of the role of designers therein.

[7] Independent Press Standards Association
[8] .UK generic Top Level Domain Registry

Introducing Information Privacy by Design

We start by providing some context on information PbD. As this Part shows, our arguments about the closer alignment of law and HCI go far beyond PbD. **The proposal of user centric regulation is more holistic and could be used to focus on any number of areas of law and design, such as accessibility and disability laws or environmental laws.** However, focusing on one area of law helps us to really unpack what UCR might look like and privacy by design is a good starting point.

Broadly, it requires technology designers to consider privacy risks of their technology as early as possible, **before a system has been built**, in order to embed safeguards from the beginning. Adopting this approach means technologies have built in mechanisms that account for and address privacy risks before hitting the market. It also helps to regulate end user privacy rights and narrow the regulatory effectiveness gap created by slow legislative change and quick technological development.

Privacy by Design (PbD) is a policy tool that has been discussed in EU and UK regulatory circles for some time (Cavoukian, 2011; Spiekermann 2012). It has existed in various design led iterations like privacy enhancing technologies (PETS) (Camp and Osorio, 2003), privacy impact assessments (PIAs) (Wright and De Hert, 2012), especially for Radio Frequency Identification (Spiekermann, 2011), privacy engineering (Dennedy, Fox and Finneran, 2014; Oliver 2014; Spiekermann and Cranor, 2009) and usable privacy (Iachello and Hong, 2007). Legally speaking, privacy by design (PbD) is broader than information privacy/data protection by design (iPbD/DPbD), a distinction we return to in Part II. However, the terms PbD/iPbD/DPbD are sometimes used interchangeably in this thesis, and the core idea remains throughout: **designers needing to think about privacy risks of their technology as early as possible and embedding safeguards.**

We provide more legal detail in Chapter 4, but for now highlight that Article 25 (1) of the 2016 General Data Protection Regulation 2016[9] mandates data

[9] Formerly Article 23 of draft

protection/information privacy by design and default. This is an explicit legal grounding for iPbD, and the law will be enforced from 25 May 2018.[10] The law reads:

"Article 25: Data Protection by Design and Default:

1. Taking into account the ***state of the art, the cost of implementation and the nature, scope, context and purposes of processing*** *as well as the* ***risks of varying likelihood and severity for rights and freedoms of natural persons 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 manner 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…*** [11]"

Other state regulatory bodies like the UK Information Commissioner Office (ICO 2016), the European Data Protection Supervisor (EDPS) (EDPS, 2013; EDPS, 2014; EDPS, 2015), European Union Agency for Network and Information Security (ENISA), (Danezis et al., 2014) and EU Article 29 Working Party also recognise the importance of PbD approaches (Article 29 Working Party, 2014). For example, the EDPS has stated that "*systems and software engineers need to understand and better apply the principles of privacy by design in new products and services across design phases and technologies*" (EDPS 2015b). More specifically for the IoT, the Article 29 Working Party Opinion (2014) recommends "*Every stakeholder in the IoT should apply the principles of Privacy by Design and Privacy by Default*" (p21).

---

[10] UK Information Commissioner Office
https://iconewsblog.wordpress.com/2016/07/07/gdpr-still-relevant-for-the-uk/

[11] Art 25(*2.) The controller shall implement appropriate technical and organisational measures for ensuring that,* ***by default, only personal data which are necessary for each specific purpose of the processing are processed****. That obligation applies to the* ***amount of personal data collected, the extent of their processing, the period of their storage and their accessibility****. In particular, such measures shall ensure that* ***by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.***

3. ***An approved certification mechanism pursuant to Article 42[11]*** *may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article.*

As this shows, there are obligations on controllers to consider what technical and organisational safeguards will be needed in light of factors like state of art, cost of implementation and risks to fundamental rights, to ensure the rights of data subjects are protected and there is general compliance with the GDPR during processing of personal data. Legally, data controllers are "*the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data*" (GDPR, 2016, Article 4(5)), a drafting that is sufficiently broad to encapsulate a range of system designers from manufacturers to third party services. Furthermore, data processing is very broad, including "*any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction*" (Article 4(2), GDPR, 2016).

Consequently, **we assert Article 25 puts those creating the technologies at the forefront of compliance with information privacy laws during the design of new personal data driven technologies.** We return to challenges and further detail around implementing privacy by design in law and design in Part II. For now, we return to unpacking how regulation as a concept has been changing, with a view to understanding how design (ers) may fit in the regulation process.

Designers as Regulators

We want to understand the nature of regulation, to understand how HCI designers may fit into established models. We suggest that regulation has broadened to the extent that HCI designers can be viewed as regulators. However, whilst this brings responsibility, we need to understand how the standards regulators are traditionally held to translate to HCI designers.

Traditionally, regulation is seen as the purview of the state, where laws are used to control behaviour, for example of markets, companies or individuals. As Selznick's (1985) classic definition captures, it is the "*sustained and focused control exercised by a*

public agency, on the basis of a legislative mandate over activities that are generally regarded as desirable to society" (p363) State regulation for consumer in competitive markets in energy (Ofgem) or telecoms (Ofcom) or public interests like the environment (Scottish Environmental Protection Agency) capture this kind of regulation. **These continue to exist,** but we build on the recognition that the **purposes of and institutions involved in** regulation have broadened significantly. Selznick's (1985) more traditional, state centric view of regulation looks decidedly outdated alongside recent versions that reflect both the role of **non-state actors**, and **unintended purposes of regulation**.

Newer definitions accommodate factors such as type of control, specific methods, actors and purposes involved in regulation.

- **Control:** as Baldwin and Cave (1999) assert regulation is "*all forms of social control, state and non-state, intended and non-intended*" (p91)

- **Specific methods and purposes:** as Jaap Koops (2006) argues "*controlling human or societal behaviour by rules or restrictions*" (p81); or

- **Actors:** as Leenes (2011) considers "*because the state and other (non-state) actors affect the behaviour of individuals by means of intentional control and because those interventions need to be justified, I would regard any entity engaging in social control within the scope of regulation*" (p149).

However, Black's (2002) definition of regulation offers the most scope for framing the role of HCI designers in regulation. She terms it as: "*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 behaviour-modification*". (Black, 2002, p26). This definition clearly widens the practice of regulation to non-state actors, like designers, but also to the methods they use in order to produce outcomes.

The background of this definition is relevant. Black's work more generally asserts that we have moved to a 'post regulatory state' which involves a *'hollowing out of the state'* through the growth of 'decentred regulation' (Black 2001, p106-122).[12]

This means that **many non-state organisations are now involved in the practice of regulation such as NGOs, charities, auditors and professional advisers** (Black, 2007, p61-62). In the context of information technology regulation, this could include standard setting organisations like the World Wide Web Consortium (W3C) and Internet Engineering Task Force (IETF) or multi-stakeholder bodies like the Internet Governance Forum or Internet Society.

Concurrently there is a '*thickening at the centre*' of government where they centrally expand to improve their powers to control these decentralised institutions (Black, 2007, p58).[13] Government encourages hybrid regulation where there are arrangements between state and non-state actors in both self-regulatory (Black, 2001) and co-regulatory formats (Marsden, 2011; Marsden and Brown, 2013). Hence, increasingly we see '*regulation in many rooms*' (Black, 2007, p63), not just traditional forums of the state.

Alongside Black, Braithwaite (2000) argues that traditional top down command and control governance[14] is being coupled with "*strategies for regulating already private institutions through compliance systems, codes of practice and other self-regulatory strategies*" (p225) and Scott (2004) asserts control increasingly exists beyond hierarchy of the

---

[12] Decentred regulation is "*at its simplest a counterpoint to the notion that regulation is something delivered by the state through the use of legal rules backed by (often criminal) sanctions: 'command and control or CAC regulation*" Black (2007), p61;

See also Black (2001) p106-122 on the rise of decentred regulation being driven by factors such as complexity of interactions between systems and actors; fragmentation of knowledge; fragmentation of power and control; autonomy of social actors; interactions and interdependencies; and collapse of private public distinction.

[13] Black (2007) p58 "*The rise of the meta-regulatory agency is also being accompanied by a 'thickening at the centre': an expansion and enhancement of the role of the core executive, notably the Treasury and the Cabinet Office, in monitoring and attempting to direct the activities of regulators to whom it nonetheless wants to give a reasonable degree of operational autonomy*"

[14]See Black (2001) p105 with command and control regulation, rightly or wrongly, "*the term is used to denote all that can be bad about regulation: poorly targeted rules, rigidity, ossification, under or over enforcement, unintended consequences*"

law and the state (p167). This expansion of regulation brings many sources, activities, aims and methods to the fore, including the explicit, legal involvement of designers in data protection regulation.

However, the state still has key oversight over regulation. As Black (2001) notes, governments now 'steer but do not row' as they latently set regulatory agendas (p126). They mandate action, but do not stipulate how this is implemented, as we see with IPbD. They have a paternalistic role to play in protecting civic values, correcting and regulating markets, and defending consumer and fundamental rights, to name a few. The powerful position of the state is linked to their hierarchy and law (Scott 2003). Law prompts action, particularly through **fear** of sanctions and repercussions, as Ayres and Braithwaite's (1992) model of 'responsive regulation' captures. It shows the hierarchical utility of law, whether or not it is actually used or effective (Scott, 2003, p12).

They frame regulation as existing in a pyramid structure, where self-regulation and more autonomous social ordering occurs at the bottom of the pyramid. Following failures, regulatory responses can be escalated up the pyramid to stricter legal oversight and sanctions like criminal or civil penalties (Ayers & Braithwaite, 1992, pp 35 & 39). This model can persist despite weak, underfunded or fragmented regulatory agencies. State regulators should normally be in the bottom of the pyramid, '*speaking softly while carrying a big stick*', (Braithwaite, 1997) warning and advising, but threatening to prosecute, fine, or revoke licenses if necessary (Scott, 2003, p13).

This picture fits for the UK data regulator, the ICO, where despite limited resources, the big stick is pursuit of high profile prosecutions against councils, hospital trusts and telemarketing firms for breaches of the Data Protection Act 1998 (ICO 2016b). Speaking softly involves interpretative technical guidance and support on data protection compliance for organisations and the public (ICO 2016c).

At this point it is worth mentioning why **we are interested rules and social norms, as instantiated in laws**. Laws are just one tool for regulation, backed by

sanctions and hierarchical power of the state for enforcement, but other instruments for rules and standard setting exist, many beyond the realm of the state. For example, if we consider information privacy regulation (Raab and Bennett, 2006), whilst there are enforced legal norms in formal legal provisions like international, EU and domestic laws (as interpreted in case law), there are many unenforced quasi-legal tools like opinions or guidelines from advisory agencies, industry wide policies or codes of practice, auditing tools like privacy impact assessments or technological approaches like privacy enhancing technologies. Our interest in rules, control, and shaping behaviour is more aligned with regulation as opposed to governance, which is a broader term focused on governing processes by different organisations, including government (Braithwaite, Coglianese and Levi Faur, 2007, p3).

Overcoming Lack of Authority and Legitimacy

If we accept that, HCI designers can be viewed as regulators, an issue is their lack of authority to regulate (Hood and Margetts, 2007, 126-127). Traditional governments have **detectors** (means to pull in information) and **effectors** (means to change the outside world) (Hood and Margetts, 2007, p3-5).[15] As Hood and Margetts (2007) highlight, the nodal, central authoritative position of government to oversee, accumulate and control information and their **authority** to "*officially … demand, forbid, guarantee, and adjudicate*"(p5) are key regulatory powers. Indeed, such authority defines and differentiates government from other regulatory actors, like designers.

However, this authority is not without bounds, and needs to be **legitimate**. Traditionally, legitimate authority is derived from factors like democratic process (e.g. elections, consultations, judicial review) or public accountability (e.g. holding public officials to account) for different arms of government like the legislature, executive and judiciary.

[15] Hood and Margetts (2007) p5 "*it is not enough simply to know what is going on. No control system is worthy of the name unless it is capable of taking some action on the basis of that knowledge…it must have some means of trying to adjust the state of the system to which it relates. Here we come to the 'business end' of government - a range of tools which vary from the gentlest of blandishments to extremely blunt instruments*"

For non-state actors like HCI designers, this does not exist. Yeung (2014), for example, questions the political responsibility of designers (p12) where opaque rulemaking and limited stakeholder input can undermine accountability (p15) and the non-state regulatory agenda may be in conflict with state *values* like valuing profit over human rights of the citizens. As she argues, accountability for designers is not the same as the state where "*accountability usually involves not just the provision of information about performance but also the possibility of debate, of questions by the forum and answers by the actor, and eventually of judgment of the actor by the forum*"(Yeung, 2014, p12). Indeed, as Reidenberg (1998) noted nearly 20 years ago '*the technical community, willingly or not, now has become a policy community, and with policy influence comes public responsibility.*'(p584). However, the nature of that public responsibility has yet to become settled.

Technology designers are not currently held to the same principles of public accountability, oversight or adherence to the 'rule of law'(Hildebrandt, 2011)[16] **as governments institutions are**. Whilst responsible innovation frameworks and codes of ethics have a role to play in identifying responsibilities of designers, the nature of this responsibility not yet crystallised (IEEE, 1963, s1; ACM, 1999, s1.01; Stilgoe et al, 2013). We return to this point in Chapter 2.

The **source** of the mandate for action may play a role in determining legitimacy. With more self or co-regulatory approaches, such as those involving non-state actors, the state has varying levels of input. For HCI designers, the **legitimacy** of their role may stem from explicit steering by the state, in line with democratically negotiated, publicly debated norms and values (as instantiated in laws). Leenes (2011) argues state use of regulation through design approaches *'is legitimate if there is respect for human rights, choice, transparency and accountability'* (p159). The long legislative process around the GDPR is a good example, as whilst it legally mandates privacy by design, it develops from extensive input from a range of stakeholders from the general public to industries and academia.

However, as Leenes (2011) continues, for non-state actors, the picture is more complex (p143) if a legal obligation to follow rules is lacking, then different

[16] 'Rule of law' is requirement of adherence to set standards, to prevent arbitrary decision making

standards of legitimacy are required (p168). Contracts are often used to mediate legal interactions with a technology, yet these terms need to be communicated and sufficiently transparent to the user because "*the norms may be legally null and void and hence not legally bind individuals, yet as long as the norms remain embedded in the technology they in fact do regulate behaviour*" (p168). There needs to be better standards of legitimacy than contracts for non-state actors involved in regulation. We return to legal challenges of contracts as a route for regulation of user interests, like informed consent, in Part 2.

To understand the need for legitimacy, **we consider why regulation using design approaches can be problematic**. As Leenes (2011) states, where norms are embedded into technology, sanctions do not exist, instead "*enforcement and sanction coincide*" (p147 and p168). This is in contrast to traditional legal approaches to regulation where enforcement often involves costly civil litigation or criminal prosecutions. More critically, Brownsword (2004; 2005; 2006; 2008) argues that it is because they impact users' empowerment and their ability to make *choices.* (Brownsword, 2008b, p247; Brownsword 2004, p211).[17] If the system only ever lets users do the 'right' thing it could remove the notion of good and bad. (Brownsword, 2006). When regulation is embedded into a technology, rules can be perfectly enforced and non-compliance may not even be possible. User choice is key.

For Yeung (2011), regulation using design in this way means individuals are no longer "*being called upon to offer an explanation of [their] reasons for action*" (p5) and technologies are enforcing behaviours without relying on moral reflection (p12). [18] This is in contrast to traditional regulation because as Leenes (2011) has noted, citizens "*have to know that their behaviour is regulated and how it is regulated*" (p159) but "*unless the regulators purposes are transparent, there can be no meaningful debate about the acceptability of the measures taken*" "(p159). At a minimum then, system designers have

[17] Brownsword (2004) p211 frames empowerment in terms of human dignity i.e. "*one's capacity for making one's own choices should be recognised; that the choices one makes should be respected; and that the need for a supportive context for autonomous decision making (and action) should be appreciated and acted upon*"

[18] Yeung (2011) p12 "*the importance of moral responsibility derives from that of basic responsibility and to this extent, it can be understood as a mark of basic responsibility…a morally responsible agent is one who acts on the basis of moral reasons, that is, reasons for action that pertain to the interest of others*"

a responsibility to provide some **transparency to users on how their systems are regulating their behaviours**. This lets them at least know they are being regulated in some capacity. Yeung (2011) argues for allowing individuals to make choices and exercise their judgement and agency.[19] By showing individuals how they are being regulated and letting them choose if they accept this, it goes some way towards legitimising the role of designers.

Building on this, **there are routes for designers to obtain legitimacy as regulators**. They can improve the quality of regulation as they have the capacity to understand how users interact with technologies in context, providing them an opportunity to design interactions that understand user needs. This may require prompting user **reflection, increasing transparency** and enabling greater **choice around how technology mediates their behaviour**. Whilst legitimacy can stem from steering by the state via legislative mandate, as we see with IPbD, broader sensitisation and response to human **values** in design offers a wider route for understanding how designers fit into regulation. We return to this in chapter 2.

We conclude this section by reasserting regulation is becoming broader, with a shift away from state centricity, towards incorporation of more actors (including non-state actors), broader goals (including non-public policy) and loosely defined approaches (including but not limited to standard setting or information gathering). By situating the role of designers within this view of regulation we can start to unpack where they may fit. Rules and government are still key. The state retains authority, often through laws and this ensures their power to steer non-state actors. The state also retains legitimacy through their public accountability.

Designers, as new regulators, lack such authority and the standards of legitimacy they are held to are yet to be settled. However, we'd argue their proximity and sensitivity to interests of users, as we explore in detail in chapter 2 and 3, are a channel to increasing their legitimacy. **We argue designers require support to**

[19] Yeung (2011) gives interesting example of the 'Drachten Experiment', a town without traffic lights, where change of design, agents were still required to exercise their judgment see - http://www.telegraph.co.uk/news/uknews/1533248/Is-this-the-end-of-the-road-for-traffic-lights.html

understand their new regulatory role, and this firstly requires understanding how they fit into established models of technology regulation. Accordingly, we now look at how technology design, and its role in regulation, is currently understood within the IT law community.

Embedding Regulation in Technology

Beyond the regulatory field, other domains have long recognised the **normative and regulatory dimension of technology**. Historian Kranzberg (1986) and political theorist Winner (1978; 1980) stated respectively, "*technology is neither good nor bad, nor is it neutral*" (p544), and "*technology in a true sense is legislation. It recognizes that technical forms do, to a large extent, shape the basic pattern and content of human activity in our time"* (1978, p323). Designers have long been involved in regulation, from architects building housing estates using situational crime prevention approaches (Von Hirsch, Garland and Wakefield, 2004), or software engineers building enforcement of copyright laws through digital rights management (Jondet, 2006).

IT legal scholars agree on the **importance of technology in shaping behaviour and more broadly as a regulation tool** (Brownsword, 2008 p247; Leenes, 2012; Jaap Koops et al 2006 p158; Van den Berg, 2011, p319). Reidenberg's (1998) pioneering work started this trend with the recognition "*technological capabilities and system design choices impose rules on participants. The creation and implementation of policy are embedded in network designs and standards as well as in system configurations*" (p555). Following Reidenberg was Lessig's famous aphorism 'code is law' (Lessig 1999, p6)[20] which captured the field and has been an enduring tenet in the history of IT law[21] (Johnson and Post, 1995; Perry Barlow, 1996; Reidenberg 1998; Post, 2002, Zittrain, 2006; Goldsmith and Wu, 2008).

For Lessig (2006) there are four interdependent modalities (p123) involved in regulating the liberty and behaviour of individuals (as he terms them, 'pathetic dots'), and they mix and interact in different ways. Those are **market forces, social norms, law and architecture** (p72-74). The novel inclusion of architecture, or

[20] From Lessig (1999) "*In real space we recognize how laws regulate through constitutions, statutes, and other legal codes. In cyberspace we must understand how code regulates how software and hardware that make cyberspace what it is regulate cyberspace as it is. As William Mitchell puts it, this code is cyberspace's law. Code is Law.*" Reference to Mitchell (1995)

[21] There is a broader debate as the Internet emerged in the mid 1990s between the cyber-libertarians who argued the internet is a new domain beyond the realm of traditional regulation, and the cyber paternalists who argued it is still subject to same jurisdictional rules and laws. The former are typified by the position of Perry Barlow (1996), Post (2002), Johnson and Post (1995), and the latter by Lessig (2006), along with Reidenberg, (1998) Goldsmith and Wu (2008) and others.

'code', is the manmade system of hardware and software, which has no inherent or immutable values/features and thus can be redesigned to different ends. As Lessig (2006) says, "*technology is plastic. It can be remade to do things differently*" (p32-37). The longstanding traction of Lessig's model is its succinct expression of the importance of how technology is built and how code can be functionally comparable to law as a regulatory mechanism, hence 'code is law' (Lessig, 2006, p5).

How these modalities interact is of great importance and relate to some themes discussed above, particularly legitimacy. With law acting on code, Lessig is concerned about the scope of creating 'perfect regulation', where control and state power over individuals can be realised through code enforcing legal norms (Lessig, 2006, p74). He argues, "*Code is an efficient means of regulation. But its perfection makes it something different. One obeys these laws as code not because one should; one obeys these laws as code because one can do nothing else*" (Lessig, 1996, p1408).

Similarly, he is wary of the **values being embedded into code by industry, and the disconnection in purpose between industry and democratic values** (Lessig, 2006, p40-60). As Lessig said, "*if code is a lawmaker, then it should embrace the values of a particular kind of lawmaking*" (Lessig, 1999, p224) or more poetically, "*as the world is now, code writers are increasingly lawmakers…how the code regulates, who the code writers are, and who controls the code writers—these are questions on which any practice of justice must focus in the age of cyberspace. The answers reveal how cyberspace is regulated…its regulation is its code, and its code is changing*" (Lessig, 2006, p79).

Despite the influence of his work, many others have built on Lessig. Zittrain, for example, focused on the impact of code on 'generativity' (Zittrain, 2006 and 2009), which he defined as "*a system's capacity to produce unanticipated change through unfiltered contributions from broad and varied audiences*" (Zittrain, 2009, p70). His argument is that the original Internet architecture (PC's and end-to-end infrastructure) has been highly generative in allowing users to tinker and create new positive innovations. (Zittrain, 2009, p30). However, the counter issue is that generativity enables negative innovations such as malware. (p54-57). Accordingly, the response from designers can be to change the 'code' to reduce functionality, control what users

can do and ultimately create less generative spaces of 'tethered appliances' and 'walled gardens' to order and retain control over the end user's behaviour (p59-60).

These controlled environments protect users, but reduce their freedoms; hence his work highlights a trade-off manifested by regulating through code.[22] The need to question the values underpinning design are increasingly important. How might Zittrain's concerns play out in the domain of data-driven domestic IoT, where the new walled gardens and tethered appliances that mediate human interactions are not just our laptops, mobile devices or set top boxes, but devices to manage temperature or home security embedded in our daily routines?

Another extension is Murray and Scott's four modalities of control. Their modalities are broader than Lessig's, opting for hierarchy (law), competition (market), community (norms) and design (code) (Murray and Scott, 2002, p493; see also Hood, 1996). *Hierarchy*, as opposed to *law*, reflects the broader bases providing authority for control; *community*, instead of *norms*[23] reflects group based, socially driven control mechanisms (e.g. fear of 'ostracisation or disapproval' as a behavioural stimulus); (Murray and Scott, 2002, p503); *competition,* not *market*, reflects how '*rivalry and competition provide a form of control in environments where there is no identifiable market*' (p503); for *code*, they prefer *design*, as it captures more forms of design based controls than just software/hardware. Their broadening is useful, but do not address a key critique, and limitation of Lessig's model: its view of subjects of regulation, as passive entities or so called 'pathetic dots'. Users do not possess agency within his model, instead being mere subjects of the interactions of the various modalities. As we argue below, the neglect of user agency is a key shortcoming of legal models of design based regulation. Seeking to overcome Lessig's limitation is Murray's (2008b) concept of 'network communitarianism'. To understand this, we need to briefly discuss social systems theory in law, as it has been a significant influence on Murray.

---

[22] Zittrain's has not been actively extended to an IoT context but the implications of locked down functionality for embedded, networked technology is even greater than in the web based world, where a combination of the technology design and sales/service contracts mediate our interactions.

[23] Which they advocate as being "the generic term for standards, guidelines and legal and non-legal rules" following Drahos and Braithwaite (2000)

Social systems theory classifies the world as being composed of numerous, autonomous social subsystems like politics, religion, art, economics or law (Luhmann, 1992). These subsystems are 'cognitively open but normatively and operatively closed' (Luhmann, 1992, p145), meaning how they communicate with other systems is shaped by their underpinning normative structure. With law there is a binary focus on whether actions are either legal or illegal, and it will interact with other systems, like politics, on that basis (Luhmann, 1992, p145; Scott, 2004). Furthermore, law, as a subsystem, may be deemed irrelevant to other sub systems, change them or itself be diluted by them (Tuebner, 1998, p406-414).

One of many risks of a social systems approach is, as Black (2001) highlights, that these sub-systems create a vision of other sub systems based on their own understanding where "*the information which systems possess about other systems is simply that which they have themselves constructed in accordance with their own criteria*" (p107). Furthermore, how sub-systems communicate is abstracted to such a level that 'subjectivities' of individuals involved in these systems are deemed transient to the underlying character of the systems. As Mingers argues, within a subsystem "*the people will come and go, and their individual subjective motivations will disappear, but the communicative dynamic will remain*." (Mingers, 1995, p144).

Against this backdrop, in Murray's model, citizens are so called 'nodes', existing in a networked environment system where actions to and by them affect others (Murray, 2008, p301). Top down, state-centric models of regulation are not sufficient in this environment. Instead, for Murray, the nodes form a community and this "*determines whether or not a regulatory intervention is successful or if it fails*" (Murray 2008, p302). This requires looking at how the nodes of the community (p311)[24] communicate (at an abstract level) with other sub-systems.[25] Successful regulation

[24] Murray (2008) p311 "*Communication in autopoietic systems is not a process directed by the actions of individuals but is rather a system in which they act as the nodes temporarily located within the communication. People are unable to alter the course of communications as they have formed a self-referential loop within which actors play their part rather than write it. In this way, social systems effectively have a life of their own that gives direction to the thought and activity of individuals*"

[25]Murray (2008) p311 - The system maintains its form by only incorporating information from communications of other sub-structures that pertain to itself "*Through self-reference, and the memory of previous selections a subsystem focuses on only specific communications as among the possible social connections there are only a few that are relevant or compatible with its identity. Functionally differentiated subsystems within the social*

must understand and symbiotically mimic changes in the community (Murray 2006; 2008, p309). [26]

This requires looking at information about communications between nodes and it can be used by regulators for designing and targeting regulatory interventions; for monitoring the response of nodes (positive or not); and, for altering the intervention based on feedback from nodes (Murray, 2008, p309-315; Luhmann, 1996; Mingers, 1995; Forrester, 1961).

A strength of Murray's model is that the nodes are now given a degree of agency, where they can respond to regulation and this will shape their environment. However, our primary criticism is this still sits within a highly abstracted, social systems led model. The technology users are no longer just 'pathetic dots' (Lessig, 2006) but they are still reduced to mere nodes in a networked system. The lack of engagement with the *actual users* of technologies in these models is a fundamental limitation. To understand why that is an issue, we briefly consider the shifts away from social systems theory and formalism[27] that occurred in system design, particularly in the Scandinavian School of participatory design (SSPD). We focus on the SSPD as it is a useful example of an area of design driven by interplay

---

systems are thereby concerned and can only be concerned with communications that are relevant to their functioning, autonomous of one another. Thereby communicative acts effectively say nothing about the world that is not classified by the communication itself."

[26] Murray (2008) p309 "*Use contemporary modelling techniques to predict where tensions will arise within the regulatory matrix and to design a regulatory intervention to avoid such tensions and to instead harness the natural communications flows within the matrix: in other words to mimic organic regulatory developments*"; See Murray, A. (2006) Chapter 8

[27] We tacitly refer to Suchman's concept of situated action throughout the thesis. Situation Action is an *ethnomethodologically* driven approach that "*underscores the view that every course of action depends in essential ways on its material and social circumstance. Rather than attempt to abstract action away from its circumstances and represent it as a rational plan, the approach is to study how people use their circumstances to achieve intelligent action.*" (Suchman, 2007, p70)[27]

Basically it requires looking at specificities of a setting and the practices, as opposed to making assumptions and *formalising* those into the system as representative of real practice.[27]. For source of discussion see Suchman (1994; 1995; 2007) debate with Winograd's (1986), Flores et al (1988) about a system (The Coordinator) that was used for holding people accountable to tasks in the workplace, by formalising what they said as being indicative of anticipated later action (Suchman, 1994, p180).

A key part of her view is that "*although the course of action can always be projected or reconstructed in terms of prior intentions and typical situations, the prescriptive significance of intentions for situated action is* ***vague****. The coherence of situated action is tied in essential ways not to individual predispositions or conventional rules but to* ***local interactions contingent on the actor's particular circumstances*** (p52)".

between of user legal rights, politics and regulation. However, it also highlights the move away from more systems led models of design of (workplace) IT systems. We use this as an example **why system led approaches for addressing needs and interests of users are no longer sufficient**. As this shift already occurred in IT system design, we argue IT law regulation needs to do the same. Our concept of user centric regulation builds on this basis. We delve into HCI perspectives in more detail below, but it is important to reflect this point briefly here as the parallels are strong.

Moving Beyond Social Systems Theory: The Scandinavian School of Participatory Design

We firstly need to set the scene and roots of the Scandinavian School of Participatory Design (SSPD). It focuses on the goal of creating industrial democracy in the workplace, reflecting worker labour rights and improving overall quality of working lives (Kraft and Bansler, 1992; Ehn and Kyng, 1987). **Accordingly, workers need to be involved in development of IT systems that are incorporated into their jobs, of which they are end users.** Law was a key driver, for example with Norway's Working Environment Act, requiring workers to be informed and educated about work systems, and given more control and responsibility for their work (Bjerknes and Bratteteig, 1995, p76; Kraft and Bansler, 1992). As Bansler (1989) argues workplace democracy is no easy goal, and "*a truly democratic working life will only become a reality after a prolonged struggle by the unions against the dominance of capital over labour*" (Bansler, 1989, p16).

Critical for us is the transition to SSPD is a response to earlier models of design that neglected end user interests. Bansler (1985) charted the chronology, starting with the initial 'systems school' of design looked to "*rationalise work processes by using computer based information systems to eliminate waste in labour, time and materials*" (Bansler, 1989, p5). Langefors (1966) systems theory was influential here, framing organisations as machines consisting of components that should behave in an orderly way, according to prescribed rules. Humans, being the less controllable components, are given minimal influence and agency overall, instead being programmatically factored into the overall functions of the 'machine' (Bansler, 1989, p8-9). High profile cases of worker rejection and hostility to new

payroll/accounting systems in the 1960s (Bansler, 1989, p10) drove awareness that worker job satisfaction is a meaningful part of the system, leading to a shift away from more systems led approaches (Mumford, 2006). However, the resulting 'socio-technical' approaches (Mumford, 2006) assumed common interests in the organisation between workers and employers, like the predecessor systems model. In contrast, SSPD is conflict driven, where employees and employers have broadly opposing interests, bringing political interests to the fore (Bansler, 1989, p5; Kraft and Bansler, 1992; Ehn and Kyng, 1987). The SSPD approach "*is built on the assumption of inherent and pervasive conflict, struggle and unequal power relations*" (Törpel et al, 2006, p17) where workers' rights need to be supported to seek industrial democracy, improve quality of workplace life (Floyd et al, 1989) and "*enable them to push their agendas forward against exploitative capital endowed with far greater power and resources*" (Torpel, 2006, p17).

Whilst SSPD clearly owes much to its specific legal and cultural context, it may not be limited to just Scandinavia or work settings, hence why it is useful for this analogy**.** Its wider traction outside Scandinavia has long been questioned (Muller et al, 1991; Bjerknes and Bratteteig 1995; Muller, Wildman and White (1993) reflecting on factors like weak trade unions in the US (Kraft and Bansler, 1992, p132), more military, as opposed to trade union, driven US computing research agenda (Floyd et al, 1989, p264).

Nevertheless, Floyd et al (1989) note that whilst the trade union element is important to consider, it does not limit the approach as "…*the theoretical and methodological approaches, the system development models, and the concepts encouraging user participation with a view toward humanising technology and work design*…" have broader appeal (p340-341). Similarly, Muller at al (1991) argued that by focusing on the goals of PD (e.g. improving work life, involving users in design, iterating designs) as opposed to procedural intricacies, its appeal could have spread beyond Scandinavia (p390).

Contemporary participatory design (PD) has shifted away from the overtly political focus, trade union roots and emphasis on workers and workplaces (Kyng, 2010, p57, Törpel et al, 2009). As Kyng (2010) states, values like democracy are less

prominent, with focus on society in general, not just workers, and elements like user involvement and prototyping dominate. For Halskov and Hansen (2015), contemporary PD is typified by looking at people generally, not just users; looking beyond traditional workplace contexts of PD to healthcare settings, hackerspaces, etc; continued heavy focus on methods; and lastly, a shift towards PD improving quality of life generally, not just through products/technologies. Despite these shifts, some feel the political roots are key to remember. Beck (2002) calls for increased political focus in PD again, engaging with ethical, social, cultural implications of computer design, and moving away from PD as just a method, and looking to its roots of challenging power asymmetries or dominance.

To reiterate, we highlight SSPD, to show the shift away from social systems led and formalist models of understanding how users interact with technology. This grew from the inadequacies of those previous models for accounting for legal and political interests of users being reflected in design. This type of PD foregrounds legal rights of users, using them to inform the design of systems. **SSPD is a useful example, as it recognises the users of technology as individuals with legal rights and responds accordingly.**

As an aside, despite PD's growth in different directions, remembering the political roots and how PD as a method incorporates users' rights and values into technology design is useful. Designing methods for doing PD go beyond the scope of this thesis. However, as this is exploratory work, we highlight that there is future work for **user centric regulation** in understanding how designers, as regulators, can use PD as a tool to build situated understanding of legal values of users, their interests around regulation and how the technology can address these. This is an approach for increasing their legitimacy, but in this thesis, we focus on more value led approaches, as we see in Chapters 2 and 3.

The importance of technology in regulation has prompted a turn to design. However, currently, this views design from a very abstract perspective, where relations between users, technology and regulation are distilled down to code, norms, market, regulation. They lack focus on the real subject of regulation and this is no longer sustainable. Accordingly, like with SSPD, the top down, systems

led approaches that dominate IT law are not sustainable for regulation of user interests or rights. IT law needs a turn to developing rich understanding of the relationship between user and technology in context, and learning how regulatory interventions manifest in these settings.

The new role of system designers as regulators offers an opportunity to move in a new direction and obtain a deeper understanding of the subject of regulation: the user. As we uncover in Chapter 2, HCI focuses on understanding complexities of users and their environments in order to design better systems. This involves focusing on how users **really** interact with technologies, unpacking the detail through more contextual, interactional levels of inquiry. If we take the example of domestic IoT, designers can expose daily routines, values of occupants, politics in the home, the nature of domestic social dynamics, family conflict management and how technology may disrupt established order in the home.

As we have argued in this chapter, the technology design community are directly being involved in regulation, to the extent they can now be viewed as regulators. The nature of that new role, particularly in terms of legitimacy, needs further investigation. Given the lack of focus in regulatory theory and IT law on specificities of users, this seems a good place to start thinking about how designers fit into regulation. In chapter 2 we consider to what extent HCI is already engaging with law and regulation, and proposing theories that can deepen our understanding of what designers can bring to their role as regulators.

Chapter 3. A Legal Turn in Human Computer Interaction

In understanding the new role of system designer as regulators, we turn our attention to HCI. The field has broadened to incorporate a wider range of social concerns around technology. In particular, there is keen awareness of the importance of human values in design. However, HCI has yet to turn to regulation, to look at the explicit role of designers therein. One way of doing this is to extend the focus on human values to include legal values. Again, we focus on HCI as it is the closest area of system design to the end user. As laws and regulations pertain to the legal rights of citizens, those same citizens are also users of technology. Understanding how to incorporate their rights into the design process is a key consideration.

The Broadening of HCI

Over its growth as a discipline, HCI has long borrowed and integrated perspectives from other fields (Rogers, 2005, p88). These have varied from cognitive sciences (Gibson 1979; Hutchins, 1995) and activity theory (Bødker, 1989) to ethnomethodology from sociology and anthropology (Crabtree, Rouncefield and Tolmie (2012); Garfinkel, (1967)). Harrison, Sengers and Tatar (2011) argue more epistemologically diverse perspectives are increasingly being integrated into HCI particularly from critical design, participatory design, and values sensitive design (p385).

HCI has been going beyond utilitarian concerns like interface efficiency and performance or optimisation towards more experiential, cultural and ethical aspects of computing. This shift has been termed as a move from the second to **third wave** of HCI by Bødker (2006, 2016), where the third wave sees "*the use, context and application types [of computing] are broadened, and intermixed. Computers are increasingly being used in the private and public spheres. Technology spreads from the workplace to our homes and everyday lives and culture. New elements of human life are included in the human computer interaction such as culture, emotion and experience, and the focus of the third wave, to some extent,*

seems to be defined in terms of what the second wave is not: non-work, non-purposeful, non-rational..." (Bødker, 2006, p1-2). Whilst law is not explicitly mentioned in the third wave, the turn to broader social implications of computing is an opening to consider legal aspects around HCI.

Similarly, **critical reflection** is now a central part of HCI, with designers thinking about the broader social implications of their work during design (Sengers et al, 2005, p50). Critical reflection requires "*bringing unconscious aspects of experience to conscious awareness, thereby making them available for conscious choice*" (p50). Thus, there is a role for highlighting and questioning assumptions, ideologies, and beliefs of design (Sengers et al, 2005, p53-55; Pierce et al, 2015). Reflexivity of designers can foster notions of responsibility during technology design, through the ongoing process of reflection on their position, knowledge and impact (Grimpe et al, 2014). Accordingly, where critical reflection by designers is part of their practice, this should extend to considering the regulatory implications of their work too. Reflection on legal issues is challenged by levels of knowledge held by non-lawyers, hence support mechanisms are needed to sensitise designers to this aspect of their role. However, as we argue below, they are already sensitive to human values and societal concerns in design so this should be extended to legal values.

Engagement with Social Implications of Technology

HCI as a field is increasing engagement with social implications of technology, driven by many factors like responding to calls from leading figures or design requirements. However, there is limited reference to law explicitly [28] and in parts 3 and 4 of the thesis we look to our participants to understand their rationales for engaging with law and regulation specifically. In any case, designers bring fresh perspectives to societal concerns, but they need to come to terms with their role in this domain.

In the early 1990s, Shneiderman (1990) called on '*researchers, system designers, managers, implementers, testers and trainers of user interfaces and information systems*' to exert influence, moral leadership and responsibility to find "*ways to enable users to accomplish their*

[28] although many of these areas like privacy, accessibility or development have legal underpinnings

personal and organisational goals whilst pursuing higher societal goals and serving human needs" (Shneiderman, 1990, p2).[29] As we can see, the HCI community has actively engaged with broader societal concerns over the years, including:

- Development (Dray, 2012),
- Activism (Busse et al, 2013)
- Universal usability (Shneiderman, 2012)
- World peace (Hourcade et al, 2012)
- Accessibility (Lazar et al, 2012)
- Privacy (Belotti and Sellen, 1993)

Hochheiser and Lazar (2010) summarise the field as engaging with social issues due to *influences* prompting *responses*. Influences may be requirements, such as *accessibility requirements* to evaluate and design interfaces for a spectrum of disabilities, both physical and cognitive. Similarly, the goal of *universal usability* means designing for diverse users, technologies, levels of understanding, cultural contexts (p342). They map responses in HCI as falling into categories (p348), such as:

- *design and development* to build solutions
- *evaluation* particularly looking to different domains to learn lessons eg usable privacy and security
- *models and theories* like participatory design, value sensitive design, and participatory action research
- *reports, testimony and related public policy* activities like working with policymakers and institutions
- *calls to action* prompting the community to make change

We concur with their argument that "*the HCI community can play a constructive role in responding to concerns and questions raised by policymakers, citizens and other stakeholders. However, proactive engagement aimed at addressing concerns before technologies are widely*

[29] Shneiderman (1990) p2 "*My concern is on how users are empowered by new technologies, how they apply their growing power, and the choices that researchers and developers can make to influence user interfaces. I believe that we can choose to build a future in which computer users experience competence, clarity, control and comfort and feelings of mastery and accomplishment*"

developed and implemented will arguably have greater impact" (p340). Indeed, this is the premise of PbD approaches. However, like with PbD, implementation does not follow an easy path. Despite willingness, the HCI community may encounter difficulties engaging with these challenges (Lazar, 2012; Johnson et al, 1999).

Three particular challenges are dealing with unfamiliar terminology, engaging with normative debates and preserving interest.

Firstly, Flanagan, Howe and Nissenbaum (2008) highlight the epistemic challenges of unfamiliar terms, approaches and theories, meaning "*even conscientious designers, by which we mean those who support the principle of integrating values into systems and devices, will not find it easy to apply standard design methodologies, honed for the purpose of meeting functional requirements, to the unfamiliar turf of values*" (p323). We return to these concerns around values below.

Secondly, engaging in normative discussions and evidence-based policymaking can court political controversy which designers may not be used to. Flanagan, Howe and Nissenbaum (2008) argue: "*anyone can be political: the question is whether it is in one's capacity as a designer that one is or is not. We hold not only that system designers are system designers but that it is their duty as good system designers to embrace this dimension of their work, even if they are not able to prevail against the tide of countervailing forces"* (p350). Nissenbaum (2001) has gone as far as arguing for 'engineering activism'. Simply put, ignorance of the social implications of design is no longer tenable because "*systems and devices will embody values whether or not we intend or want them to. Ignoring values risks surrendering the determination of this important dimension to chance or some other force*" (p119). There are significant benefits from engagement by designers with public policy. As Shneiderman (1990) argues, "*in short, expanding our philosophical horizon can lead to better science*" (p4) and Hocheiser and Lazar (2010) argue, "*more contentious issues might involve wading into charged debates, but appropriate empirical studies and innovative designs can play a constructive role in providing guidance to policymakers*"(p354)[30]

[30] Hocheiser and Lazar (2010) argue at (Section 6) "*unpopular stands on controversial topics may involve risks to research funding and career advancement. Professional standards and conduct can help in these circumstances, as analyses grounded in successful research frameworks, experience in design and implementation and empirical analyses can provide a solid scientific basis for participating in policy discussions*."

Thirdly, Shneiderman (1990) argues that maintaining designer's interest in these issues is complex as "*hard-core computing professionals often have little patience with grand social visions. To capture their hearts and minds requires practical and realisable steps. This expectation is legitimate and even helpful*" (p5). Our proposal of privacy by design cards in Part 4 goes some way to engaging designers with intricacies of data protection law in a structured manner. It aims to maintain interest in such issues by offering a simpler entry point into a complex area of law. Sustained interest is important because if the HCI community can come to terms with these issues, they have much to offer to regulation. As Lazar et al, (2012) argue "…*our research, our data and our design expertise to help drive public policy – those things should drive policy, not politics or public opinion*" (p81).

Ethics and Responsibility

Ethical motivations and responsibilities are another basis for the widening attentions of HCI designers. In parts 3 and 4 we present empirical findings on why designers engage with regulation and the law specifically. We now turn to technology ethics to help us obtain a deeper understanding of both the responsibility and ethical nature of the designers' role in user centric regulation.

Importance of Technology Ethics

Computer ethics (CE) has long been responding to new ethical questions posed by ICT (Maner, 1980; Johnson, 1985) and the resulting "*policy and conceptual vacuums about how to use computer technology*" (Moor, 1985, p266). For Moor (1985), the field itself is defined by "*the analysis of the nature and social impact of computer technology and the corresponding formulation and justification of policies for the ethical use of such technology*" (p266). Indeed, CE is often broad, considering issues like computer crime, privacy, intellectual property, globalisation (Bynum, 2008).[31] Like law and regulation, both respond to social challenges of computing, albeit within their own frames of reference (legality vs morality). The combination of both is important, because whilst regulators may respond to emerging technologies with new rules, mere

[31] See also ETHICOMP, ACM Computers and Society, and IEEE ISTAS conferences/special interest groups for more detail on the field

compliance with these may fall short of ethical standards. In particular, the mechanisms of law, like legislation and case law, often struggle to keep pace with technological and societal change. Ethics fills a gap there, as Moor (1985) argues, ethics are not static, they adapt with human values, and are thus more organically responsive to new questions posed by computing.

In addition to CE, we obtain valuable insight by turning to the related field of engineering ethics, around topics of design, morality and human values in technology. Broader than just IT, authors like Verbeek (2006), Van Gorp and van de Poel (2001), Van Den Hoven (2011), Vermaas et al (2010)[32] and Millar (2014) help navigate differences between design and use of technology, and the moral role of designers therein.

Any notion of user centric regulation needs awareness that how a technology is built and how it is used may differ. For Verbeek (2006) engineering decisions on how users can act when using a technology are moral judgments, ultimately 'inscribed' into the technology (Akrich, 1992; Latour, 1992). Latour (1992) highlights that non-human artefacts are often delegated human functions, thus allowing them to prescribe human behaviour (Latour, 1992 p157). Beyond speed bumps or automatic door closing springs, his key/lock example shows how artefacts can work in this way. Berlin residents were not closing doors in flat stairwells, leading to security issues. In response, locks were installed where keys had to be pushed through the door and retrieved from the other side, forcing residents to lock the door. As Latour (1992) states "*this is a clever translation of a possible program relying on morality into a program relying on dire necessity: you might not want to relock the key, but you cannot do otherwise. The distance between morality and force is not as wide as moralists expect, or more exactly, clever engineers have made it smaller*" (p174).

For Verbeek, "*technological artefacts are not neutral intermediaries but actively co-shape people's being in the world: their perceptions and actions, experience and existence*" (Verbeek, 2006, p364). The technologies 'mediate' a users' understanding of the world, and building on Ihde's (1990) concept of 'multistability',[33] whilst they might have 'inscribed'

[32] See discussion of VSD at p497-498

[33] Verbeek, 2006, p365 "*A technology can have several stabilities, depending on the way it is embedded in a use context. Technological intentionalities, therefore, are always dependent on the specific stabilities that come about*"

intentions of use/function into a technology,[34] in reality the meaning is determined by use. For Ihde (2011) "*no technology ever remains limited to designer intent*", as we see with examples like claw hammers being used for removing nails, violence and art (p24). Technology and humans relate, interact and co-construct, with the relationship between them mediating the purpose and meaning of technology, as he says, "*left on a shelf, the Swiss army knife or the cell phone 'does' nothing*" (Ihde, 2011, p24).

Taking this back to a designer perspective, Verbeek (2006) concludes "*Ethics is about the question how to act, and technologies appear to be able to give material answers to this question by inviting or even exacting specific forms of action when they are used. This implies that technological mediation should play an important role in the ethics of engineering design. Designers should not only focus on the functionality of technologies but also on their mediating roles* (p377)." Likewise, Millar (2014) argues technologies act as 'moral proxies' shaping the relationship between users, artefacts and designers through design decisions.

Accordingly, engineers have a duty to look beyond function and consider these mediating impacts as "*engineering design is an inherently moral activity*" (Verbeek, 2006, p368) and as Millar puts it, *"in effect, engineers ought to be considered de facto policymakers, a role that carries implicit ethical duties"* (Millar, 2008, p4). Engineers have a moral responsibility and thus must find ways to "*bridge the gap between the context of use and the context of design*" (Verbeek, 2006, p378). That being said, the unpredictable differences between what they intend through design and how technology is used makes such reflection hard.

Indeed, conceptualising design in terms of responsibility, and moral decisions may put designers in tricky ethical situations. As Van den Hoven et al (2011) argue, engineers can suffer from 'moral overload' of making difficult, practical moral decisions involving value trade-offs and balancing competing interests during design. This leads to 'moral residue' which is the "*moral emotions and psychological tensions that are associated with the things that were not done, the road not travelled, the moral option foregone*" (p143). This can be useful insofar as it motivates a response to these

[34] "*Like the script of a movie or a theatre play, artefacts prescribe their users how to act when they use them. A speed bump, for instance, has the script "slow down when you approach me" and a plastic coffee cup "throw me away after use*" (p362)

issues as early as possible, as engineers seek to avoid such overload in the future. Value sensitive design is a useful tool for responding, one we return to below (Van den Hoven et al, 2011).

However, a key challenge of any design project is how to create and balance design requirements. Van Gorp and Van de Poel (2001) show that ethical decisions are made during technology design when engineers decide to prioritise certain requirements, with some trade-offs being acceptable and others unacceptable (eg safety against sustainability), (p16). Engineers normally use 'satisficing' where 'a *designer is satisfied with any solution that is good enough given the design requirements and will not look for optimal solutions'* (p19*).* This might not create the most ethical decision, but equally on a practical level the questions to be engaged with are not simple eg "*how should one decide for example, on the relative importance of safety versus costs? Who is to make this decision? The engineers, the manager or principle of the project, the portrayed users, the public possibly affected, the general public? And how is this decision to be made in an ethically acceptable way*" (p19).

Returning to the interplay between law and ethics again, whilst legislation defines bottom level thresholds for requirements such as safety guidelines (mere legal compliance), engineers can still make choices, for example exceeding those minimums (higher ethical standard). Fundamentally, the bottom line remains that engineers are not neutral and by participating in design processes, they are making ethical decisions (Van Gorp and Van de Poel, 2001, p21).

Lastly, requirements engineering is useful if we adapt it to thinking about how abstract legal requirements are given meaning during design of new systems. Goguen (1994) states information can be 'wet' and 'dry' where the latter information is very situated (Suchman, 2007) and can only be understood by specific social groups in specific contexts, and the former is information that can be understood in a wide variety of contexts (p173). Even with 'dry' information, local interpretation is necessary and thus "*information is always emergent, contingent, local, embodied, open and vague*" (p174). Importantly, design requirements are built on information which in itself is contingent, local, embodied, open and vague – abstract, formal requirements will not work hence situated knowledge is key to

formulating design requirements (Goguen, 1994, p181-182). This involves observing the social context of design, formulating requirements from understanding how values manifest locally within the context of technology use (Jirotka et al, 2005, p392-393).[35]

This is useful for understanding how law and ethics are factored into design. Abstract ethical or legal standards perhaps developed at broad ideological or normative levels need to be understood in context. For legal standards, that means taking legal requirements, and understanding how they manifest in the dynamic between designer, user and technological artefact. That is to say, how 'dry' legal requirements become 'wet'. The law may be abstractly defined at a broad level, but it obtains meaning when it is interpreted and situated. Compliance is local, and work between the legal and design communities can move forward on this basis. Indeed, user centric regulation must reflect this. For ethics that means designers considering how a technology mediates the actions of end users and responding accordingly. This may mean going beyond mere compliance.

With ethics, we advance the argument that ethics is a process of reflection, not necessarily tied to normative absolutes (e.g. privacy is good or bad) but instead reflecting on the mediating effects of a technology on the user. The difference between use and design needs to be factored into this too. In this section we have established the willingness of HCI designers to engage with social and ethical implications of technology. We have also considered what this might mean in ethical terms. However, if system designers *themselves* are now regulators, we want to understand how they can engage with their role as regulators.

Accordingly, we look to the approaches for bringing human values into HCI and design. There needs to be extension of these concepts to reflect values underpinning law and regulation. We unpack the kind of values at play in more detail through case studies in part 2, but for now we lay the groundwork for how human values are considered in design currently. In part 4 we propose our system for bringing legal values into design: privacy by design cards.

[35] p386-388

The Nature of Responsibility

In terms of thinking about practical tools for ethical conduct, codes of ethics through membership of specialist bodies are one manifestation of professional responsibility (Gotterbarn, 1991). For ICT, Association of Computing Machinery (ACM), Institute of Electrical and Electronic Engineers (IEEE) and British Computing Society (BCS)[36] have been providing guidance for members in codes of ethics and conduct for decades (IEEE, 1963, ACM, 1992). The IEEE Code of Ethics, for example, asks members to consider how their work impacts quality of life of others, and introduces broader notions of responsibility to public welfare, safety and health. However, early codes were viewed as focusing on acting in the best and public interest, exercising professional judgement, or protecting reputation but were not particularly aspirational (Gotterbarn, 1999; Berleur and Brunstein, 1997; Friedman and Kahn, 2006, p1193).

Similarly, the concept of responsible research and innovation has emerged as a process for creating a stronger relationship between innovation (broadly conceived) and the social consequences therein. Broadly RRI is practically orientated, seeking to be "*a transparent, interactive process by which societal actors and innovators become mutually responsive to each other with a view to the (ethical) acceptability, sustainability, and societal desirability of the innovation process and its marketable products (in order to allow a proper embedding of scientific and technological advances in our society)*" (Von Schomberg, 2011, p9).

The process for doing RRI has been unpacked in detail by Stilgoe et al (2013) propose who view its purpose as "*taking care of the future through collective stewardship of science and innovation in the present.*"(p1570) Stilgoe et al's (2013) framework draws on four elements namely *anticipation, reflexivity, inclusion, and responsiveness* as methods of reflecting on questions of "*uncertainty (in its multiple forms), purposes, motivations, social and political constitutions, trajectories and directions of innovation*"(p1570). Particularly relevant for our discussion are the first two, anticipation and reflexivity.

[36] http://www.bcs.org/upload/pdf/conduct.pdf ; IEEE Code http://www.ieee.org/about/corporate/governance/p7-8.html ; ACM Code https://www.acm.org/about/code-of-ethics (original from 1992 still stands)

- *Anticipation* is systematic consideration of risks posed by new technologies, with special precaution around unforeseen issues, to enable improved foresight. (p1570)

- *Reflexivity* on an institutional level, where scientists in public will "*blur the boundary between their role responsibilities and wider, moral responsibilitie*s" by reflecting on their "*own activities, commitments and assumptions, being aware of the limits of knowledge and being mindful that a particular framing of an issue may not be universally held.*"(p1571)

- *Inclusion* focuses on broadening the stakeholders represented in innovation governance, fostering legitimacy through greater public and wider stakeholder engagement for example through better dialogue.

The RRI framework has a key role to play specifically with information and communication technologies (ICT) (Stahl, Eden, Jirotka, and Coeckelburgh, 2014), HCI (Benford et al, 2016) and privacy (Stahl, 2013). Stahl, Eden, and Jirotka (2014) unpack the nature of responsibility noting it largely falls to individuals, who can be subject to many forms, for example software engineers may have professional responsibilities to customers, moral responsibilities to users, role responsibilities as leaders to peers, or legal responsibilities to compliance with laws (p201-202). A spectrum of ICT researchers interviewed for the FRRIICT[37] project, broadly showed less sense of responsibility for social consequences when conducting 'fundamental', 'generic', 'enabling' research than those closer to or working with specific end user groups, doing more 'applied', 'application orientated' work (p209-211). In terms of user centric regulation, there are clear crossovers with our arguments above about responsibility and reflection by designers around social issues. This needs sensitisation to societal implications of work, with greater reflexivity and anticipation around regulation and law (for example in how to operationalise PbD principles). This necessitates understanding what laws mean in practice and how they can be addressed in the design process. Appropriate responses necessitate inclusion of users as key stakeholders of design based regulation.

[37] Framework for RRI in ICT

Whilst invaluable for understanding the nature of responsibility, RRI is a more holistic process, often focused on the governance of research and funding. Accordingly, for our goal of incorporating legal values into technology design, we want to consider approaches that have emerged from within HCI, and which can be repurposed to regulatory ends. Accordingly, in the following section we consider how human values are considered in HCI and design before looking at the framework of value sensitive design, critiques and our proposal for inclusion of legal values in design.

Towards Legal Values in Design

There are many values that are relevant to consider in design of technology, but a turn towards more human values is occurring. With similarities to the third wave above, Nissenbaum (2005) argues technology should not just focus on *instrumental values* like 'effectiveness, efficiency, safety, reliability, and ease of use' but also *substantive values* like 'liberty, justice, privacy, security, friendship, comfort, trust, autonomy and transparency' (p 66). These latter values touch on many legal values. Similarly, Muller et al (1997), argue that instead of the dominance of values like productivity and efficiency as metrics of success, alternatives such as impacts on health, quality of life or user empowerment should be considered (p158). Nissenbaum (2005) argues that engineers/scientists need to look beyond technical concerns to consider social, ethical and political criteria, and equally, humanists/social scientists have to now go beyond theory and consider intricate technical details and how they interact with values. In seeking to structure how this can be done, Flanagan, Howe and Nissenbaum (2008) have proposed four considerations for getting values into design, and are meant to supplement normal design methods, improving the moral credentials of designs and to put values alongside "*functional efficiency, reliability, robustness, elegance, and safety*…" (p329-330)

- *Discovery* - listing the values involved in a project;
- *Translation* – looking to practically 'operationalise' such concepts for design;
- *Resolution* – use of philosophical approaches to address conflicts between values;
- *Verification* - check if values actually have been included adequately in the final design.

More holistically, Sellen, Rogers, Harper and Rodden (2008; 2009) outline an influential future vision of HCI [38] with three practical ways for HCI to engage with human values, hence we consider it in more detail.

[38] Sellen et al (2009) p60 "The HCI of today is exploring diverse new areas beyond the workplace, including the role of technology in home life and education even delving into such diverse areas as play, spirituality and sexuality. HCI is now more multidisciplinary than ever, with a significant percentage of the community coming from the design world. This shift has caused the field's practitioners to think more broadly about their design goals, taking into account not just how technology might be functional or useful but also how it might provoke, engage, disturb or delight"

Firstly, they highlight the need for "*folding human values in the design and research cycle*" by bringing values into "*studying, designing, building and evaluating"* technology with users. Similar to Flanagan, Howe and Nissenbaum (2008) step of *discovery*, they argue for an explicit preliminary step of *understanding* to focus on "*choosing the values being designed for*" (Sellen et al, 2009, p64-65).[39] With the new terrain of legal values, designers need increased support in understanding what legal values are, in order to understand how they may interact with user interests. Accordingly, our analysis in part two uncovers the types of legal values and regulatory challenges around two case studies, and in part four, we present a design tool to help sensitise designers to legal values, and prompt a response to these values.

Secondly, new cross-disciplinary partnerships are needed because the nature of values is too much for HCI to deal with alone (p65). As the authors say, "*HCI professionals need to engage in discourses that may at one time have seemed distant, if not entirely alien to them*" (p65).

Lastly, they advocate redefining "*the H, C and I*" in HCI. With *(H)uman*, definitions of users need broadened as computers are now used by many for a multitude of reasons beyond just improving workspaces. With (*C)omputers*, a 'physical-digital ecosystem' now exists where technologies are embedded in our daily lives (Greenfield, 2008). With *(I)nteraction*, the spaces and forms of interaction have changed vastly, thus so must the meaning of the term (p66)[40]. Development of a common language between researchers is important, as is considering users more holistically. Therefore, "*HCI must also take into account the truly human element, conceptualising 'users' as embodied individuals who have desires and concerns and who function within a social, economic and political ecology*" (p66).

---

[39] Sellen et al (2009) p64-65; "Key here is that the analysis should not just take into account people's interactions with computer technology but also with the environment, with everyday objects, with other human beings and with the changing landscape that the 'new tech' brings into the world"

[40] Sellen et al (2009) p66 "for example, interactions on and in the body, interactions between bodies, interactions between bodies and objects… and interactions at the scale of kiosks, rooms, buildings, streets and other public spaces"

We now consider one of the most well developed approaches to thinking about how to incorporate values into design: 'value sensitive design' (VSD).

For Friedman et al (2008), VSD is "*a theoretically grounded approach to the design of technology that accounts for human values in a principled and comprehensive manner throughout the design process*" (p70). By comparison, Van Den Hoven (2006) defines it as "*a way of engaging ICT that aims at making moral values part of technological design, research and development. It assumes that human values, norms, [and] moral considerations can be imparted to the things we make and use*…" (p67). [41]

In terms of actually defining values, with Friedman et al (2008) they are "*what a person or group of people consider important in life*" (p70), so called 'values with ethical import', those that 'centre on human well-being, human dignity, justice, welfare and human rights' (p1180). Similar to other arguments in this chapter, they adopt an interactional position for how values are embodied in a technology. That is they say "*whereas the features or properties that people design into technologies more readily support certain values and hinder others, the technology's actual use depends on the goals of the people interacting with it*" (p1179).

Practicalities of doing value sensitive design are intricate, but broadly involves establishing risks, benefits and costs; finding direct and indirect stakeholders, looking at value conflicts and their resolution in a specific context (Friedman et al, 2008, p87-94). VSD uses conceptual, empirical and technical investigations in an iterative way to unpack how values are involved in a system (Friedman and Kahn, 2006, p1187). This involves conceptually looking at abstract philosophical questions of establishing values, balancing competing values and potential impacts of the system (Friedman and Kahn, 2006, p1181)[42]; empirically grounding analysis with specific examples, to see how individuals, groups, or larger social systems that

[41] Van Den Hoven. (2006) p67 "…*and it construes information technology (and other technologies for that matter) as a formidable force which can be used to make the world a better place, especially when we take the trouble of reflecting on its ethical aspects in advance"*

[42] In addressing challenges of universal morality (Friedman and Kahn, 2006) state at p1183) generally "*designs need to be robust enough to substantiate the value under consideration and yet adaptable enough so that different cultures (or subcultures) can use the designs in their own way*"

configure, use or are otherwise affected by the technology or examining the technology context (Friedman et al, 2008, p71-73).

VSD has also been subject to critique, largely focusing on what (or whose) values are considered, and how they are formulated. Alongside arguing for reflexivity of researchers and greater reflection of views of participants in reporting VSD studies, Borning and Muller (2012) argue VSD often over-claims. For example, they say it should not impose a position of universal values as default, a discussion point in philosophy, and instead should be more pluralistic and open to different value systems from different cultural contexts, e.g. Alsheikh's (2011) work on use of technologies in Arabic countries.

Le Dantec et al (2009) and Borning & Muller (2012) have also raised the question of how the values VSD protects are formulated (Halloran et al, 2009). Acknowledging where these values come from is an important step, in this case western liberal democracies with commitments to human rights and civil liberties. Similarly, listing values can make them seem overly prescriptive. The non-exhaustive list of 12 values Friedman et al (2008) propose include human welfare, ownership and property, privacy, freedom from bias, universal usability, trust, autonomy, informed consent, accountability, identity, calmness and environmental sustainability. These values are not meant to be a definitive list, and as Borning and Muller (2012) recognise, pragmatism dictates the need to situate the concept of VSD within some concrete values. Interestingly, the high level values law seeks to protect are not too dissimilar to those listed by Friedman and Kahn (2006). Law is a mechanism for protecting many human values, for example if we take the example of a user's relationship with an IoT device like a smart watch:

- *Ownership and property* - protection through intellectual property law in the functionality of the device design and contract for its sale transferring a right of use; [43]

[43] Not necessarily ownership as Adams (2015) discusses.

- *Privacy* - data protection, consumer protection and human rights law seek to ensure transparency, accountability and fairness in how user data is handled, used, traded etc.

- *Environmental sustainability* - International trade laws control finite rare earth minerals or planning laws control where smart watch retailers can build stores.

Importantly for us, Le Dantic et al (2009) argue that whilst abstract lists of values sensitise designers to values generally, early empirical observation of 'local' values are necessary to really discover what values are at play in situ, i.e. "*where VSD has taken a discursive approach to values, we argue for an exploratory approach where empirical investigations treat values as local phenomena expressed in a local vocabulary. This in turn enables the development of a local classification of values which begets a local heuristic against which to evaluate systems and social interactions that arise from their use*" (p1148).

Building on the importance of human values in design and critiques of VSD, we recognise European regulatory and legal values are informed by a European philosophical and legal tradition. The nature of these values will be dependent on legal jurisdiction and differing underlying value systems (e.g. religious, cultural, social, economic, political, etc.). Consequently, we are not arguing for universalism, but acknowledging a pluralistic position. With law in particular, reflection and questioning of the sources, institutions and processes is possible through more critical methods of law, e.g. socio-legal, Marxist, postmodern, feminist, etc.

Practically speaking, need for compliance, fear of sanctions and existence within a legal system means law is not ignored, despite disagreement around its foundations.[44] It has to be considered, and accordingly, unlike ethics, the values underpinning it have a means for being brought into the design process. Law is not just a static box of rules and regulations that can be translated directly into a system. Instead, it is a set of often conflicting high level values, sometimes instantiated in legislation, sometimes in case law. Within this thesis, we focus on legal values, not

[44] Although, of course, people challenge or disobey law, as an institution it continues to exist despite challenge, although consider the literature in legal philosophy on civil disobedience Brownlee, K (2013)

in the philosophical abstract, but in their practical form, as they manifest in rights and responsibilities that need to be balanced and interpreted in context. [45] This becomes clearer in Part II as we examine iterations of legal values and principles in specific user rights or designer responsibilities, for example, DP rules around explicit consent or control over personal data as protecting autonomy of the end user.

Importantly, whilst law interacts with human values, a more high-level, abstracted sensitisation to these is needed for designers. As Le Dantic et al (2009) argue for more local understanding of *human values* in design, for 'user centric regulation' in practice, the high level legal rights and responsibilities need to be understood in more situated, local ways. However, designers first need to be sensitised to the importance of legal values in their work, and how they to do this requires discussion, development and action from both communities over time.

This thesis is quite exploratory, seeking to find practical approaches to help support designers in their new role as regulators, engaging with legal values, rights and responsibilities. Before looking at the various legal values at play in two case studies on emerging technologies and information privacy regulation, to increase clarity, we pull together our findings from these two chapters under the concept of user centric regulation.

[45] eg in law, in balancing freedom of the press and individual privacy rights, unpacking the 'public interest' is a key process – see Urquhart, (2016)

Towards User Centric Regulation

UCR is a concept that builds on our analysis and critique of perspectives from HCI and IT law. We outline these findings before outlining the concept.

IT Law

- **Broadening of Regulation:** There has been a broadening of the concept of regulation to incorporate non state actors, and an explicit turn to technology design as a regulatory approach within IT law. The state still retains a key role due to law and authority.

- **HCI Designers as Regulators:** Regulation is now sufficiently broad that HCI designers, as creators of technology, are now a new kind of regulator. The nature of their role is not settled and there are challenges, for example, around designers' legitimacy to regulate, as non-state actors.

- **New Models of Technology Design in Regulation:** IT law currently understands the role of design in regulation through systems theoretical models. These view users too abstractly, and do not consider how they actually interact with technologies in context.

HCI

- **HCI and Society:** There is an increasing focus in HCI on the societal implications of technology. Reflection on the ethical responsibilities and the incorporation of human values in the relationship between user, technology and designer can be extended to thinking about legal issues too.

- **User Centric Focus:** HCI has a range of tools and approaches to understand user interactions with technology in context. This is a key strength for the new designer regulators, as they can overcome shortcomings of current technology regulation models based on overly abstracted views of users.

User Centric Regulation

Building on these key findings, we propose bringing IT law and HCI closer together under the concept of user centric regulation. It entails the following:

- **Explicit Alignment of IT law and HCI:** User Centric Regulation builds on the turn in technology regulation to design, and the turn in design to societal concerns. Expressly linking the two requires IT law and HCI communities to understand how to move forward together. In particular, they need to critically reflect on and find means to support the new of role designers as regulators.

- **Legitimacy through User Proximity:** HCI designers need legitimacy as regulators. The proximity to end users and tools for understanding user relationships and interactions with technology can be extended to develop a richer picture of how regulation of technologies manifests in practice for users and to respond accordingly.

- **Legal Values, Ethics and Responsibility:** Increased incorporation of legal values into design is necessary by extending the existing focus on human values in HCI. This needs particular focus on end user legal rights, and related designer responsibilities. Through design, legal challenges can be considered earlier, making law more prospective than retrospective, offering scope for compliance with laws to be built into systems. However, UCR needs to go beyond just compliance, where ethical concerns are key too. Accordingly, structuring reflection and action by designers on the nature of their legal and ethical responsibilities to users is key.

Having posed the high level concept of UCR, we want to explore in detail how it might work in practice. Each subsequent part of the thesis will further inform the concept, and we follow three lines of inquiry to do this.

In part 2 we consider the types of regulatory challenges designers will face in doing UCR, the legal values at play and how they might respond accordingly. This provides greater insight into the nature of the role of designers as regulators. To narrow discussion, we use two case studies, the domestic internet of things and smart metering. We also constrain our focus to data protection law, particularly privacy by design (PbD). Importantly, UCR goes beyond just PbD, but we use it as a framing to understand how UCR may play out in practice, and learn from this.

In part 3 we consider the challenges of doing UCR in practice with PbD for the IoT by speaking to leading experts in the field. This gives us much deeper insight into **how** to align these two communities, by considering perspectives of thought leaders from each.

In part 4 we present a design tool developed to support designers' engagement with legal values from data protection, to move PbD from theory into practice. This section unpacks how a version of UCR may work in practice, and provides us insight into how designers negotiate with legal principles, where competencies exist and where support is necessary to enable them to act as regulators. It also provides designer reflection on responsibilities and ethical practices.

Part II Legal Perspectives: Two Case Studies

Part Overview

This part of the thesis analyses the kinds of legal and regulatory challenges HCI designers need to engage with in doing UCR. To make this inquiry more tractable, we use two case studies, **the domestic Internet of Things and Smart Metering.** We focus on a specific area of law, **data protection law**. As discussed in Part I, DP law contains provisions for **information privacy/data protection by design**, hence technology designers are explicitly being called upon to engage with regulation in this area.

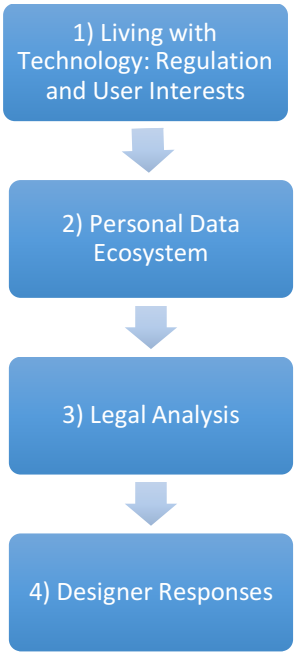
Before turning to these contexts, we briefly outline our approach in this Part. We use the case studies to help explore the regulatory landscape, underpinning legal values and we situate our analysis within real examples. For smart metering, this is the **UK Government Smart Meter Implementation Programme (SMIP);** and with the domestic Internet of Things, it is the **Works with Nest IoT device ecosystem.** These two case studies were chosen due to their differing regulatory backdrops. Smart meters are a **government** led programme. Accordingly, regulation is extensive, detailed, and largely top down through legislation, policies and strategies e.g. on regional installation targets and a metering installation code of practice for front-line engineers. Smart grids are following a similar route, due to the engineering and organisational scale of the challenge. In contrast, the domestic IoT field is largely **market** led. Accordingly, dominant platforms, protocols[46], products and ecosystems are emerging from consumer choice and market forces, mimicking other platforms historically (eg HD vs Blu-Ray).[47] The less top down nature adds complexity from a regulatory perspective, with contract law and consumer protection laws playing a larger role.

Within our **case studies** we analyse the emergence of these technologies, the underpinning **regulatory landscape**, the **issues users face living with them and the legal challenges that need to be addressed.** To conceptualise this analysis, we developed diagrams that map the actors, data flows and interactions within each

[46] Eg Zigbee, Z-Wave or Thread
[47] See interesting discussion of emergence of standards in Deakin et al (2015) p9-10

case study. We focus in more detail one legal challenge (control over personal data for IoT, access to consumption data for smart metering) to unpack the legal values at play, the regulatory challenges designers need to contend with, **and** how they can respond accordingly. For the IoT this involves considering how to **redesign consent mechanisms using the 'trajectories framework'**, an approach normally used for designing user experiences within human computer interaction. For smart metering we focus on how HCI designers can use methods like **tracking provenance of data and personal data vaults to give users greater control over who accesses their consumption data.**

Table 1 Process in Part II



1. **Living with Technology – Regulation and User Interests**: We build our case studies from analysing the technology, regulatory landscape and user challenges.

2. **Personal Data Ecosystem:** We map ecosystem focusing on the interactions, relationships and personal information flows between users, designers, technologies and third parties.

3. **Legal Analysis:** We analyse on specific legal challenges, namely access and control, as framed by parts 1-2, for each technology. This helps understand the various values at play.

4. **Designers Responses:** Through our analysis, we suggest how designers could respond to the legal challenges in line with our overarching concept of user centric regulation.

The diagrams and scenarios have emerged from **extensive documental analysis** of research papers, government, industry and third sector reports, technology installation guides, European and UK law and policy documents (eg DECC, European Commission etc), sales and service contracts, websites, standards etc.

This Part also draws on knowledge obtained through sources like:

- **informal conversations** whilst being a legal researcher in a human computer interaction lab e.g. with other researchers working on projects on smart energy management, HCI design methods, Internet of Things;

- **cross disciplinary academic networks and research visits** eg to Meiji University in Japan to conduct research on security and privacy issues of smart metering;

- **presentations and discussions** at numerous international and domestic conferences;

- **workshops, seminars and lectures** over the PhD in different disciplines and multi-stakeholder forums (eg small to medium enterprise/start-ups, multinational industries, government, regulators, academia, third sector).

When analysing the **challenges users face living with these technologies** we have not empirically collected our own field data but instead draw on secondary literature from those who have, through ethnographies, interviews or observation.[48] Such research would be useful future work, but our priority at this point is understanding the legal challenges designers need to consider so time and resources have been directed into building our detailed case study analysis. Furthermore, in Parts 3 and 4, we collect our own empirical data, by looking to practical challenges of how designers engage with legal concepts through **thirteen** detailed semi structured interviews with leading experts from technology law and design, and a series of **six** workshops with **twenty-four** technology designers using our **information privacy by design cards.**

A challenge for our analysis was narrowing down onto specific, tractable legal questions. IoT type and infrastructural energy technologies create broad, interdependent regulatory problems. As such, we knew we could not look at them all. In the end we focus on questions of choice and access, as they emerged from the analysis as key areas of concern, but see Appendix 8 for other areas we could have considered for smart metering. We chose to focus on data protection law due to the heavy emphasis on the **rights of individuals** (particularly protecting and empowering their decision making) and **associated responsibilities of companies or organisations**. Closely aligned with this is contract law and

[48] Unlike Sections 3 and 4.

consumer protection law, which we refer to when necessary. As we see in the case study analysis below, legal values like **user choice, control and ownership, or designer transparency, fairness, and, accountability often emerge**. In order to narrow our focus, we chose to ask specific questions around these issues, based on legal rights within data protection law. These are:

Control and the Internet of Things – How can designers ensure users have adequate control over personal data flows within IoT ecosystems?
Access and Smart Metering - How is access to consumption data regulated in the smart meter ecosystem?

Chapter 4. Understanding Information Privacy by Design

Chapter Overview

Before delving into the detail of our case studies, and legal analysis, we want to **briefly unpack in more detail:**

- What privacy by design and information privacy by design are.
- The legal nature of information privacy by design
- The challenges PbD faces in implementation.

Reintroducing Privacy by Design

To reiterate, in Part I we outlined that PbD broadly requires system designers to consider information privacy risks of their technology as early as possible, in order to embed safeguards from the beginning. **Ideally, this is before a system has been built**. PbD as a concept is broader than DPbD/iPbD, and legally speaking our focus is on the EU level GDPR provisions for iPbD, although we refer to both throughout. To understand the difference, we very briefly consider the technical distinction in European law between privacy and data protection/information privacy.

Privacy is a fundamental human right, protected in many international human rights instruments from bodies like the Council of Europe, Organisation for Economic Cooperation and Development, United Nations, and European Union.[49] Importantly for our purposes, every European has a non-absolute 'right to private and family life' [50]in Article 8 of the Council of Europe's European Convention on Human Rights. This right is not absolute, and needs to be balanced against other

[49] Council of Europe 108th Convention (1981); Art 12 UN Universal Declaration of Human Rights; 1980 OECD Guidelines on Protection of Privacy and Trans-Border Flows of Personal Data; Art 7 and 8 EU Charter of Fundamental Rights; European Convention on Human Rights Art 8.
[50] "Everyone has the right to respect for his private and family life, his home and his correspondence" UK Human Rights Act 1998 is important in for providing horizontal effect to human rights, in addition to vertical effect (i.e. not just state to individuals but between non-state actors and individuals like the press – see Urquhart (2016)

human rights, like freedom of expression or security, where necessary, proportionate and in accordance with the law.[51] It is much wider in scope than data protection, having been involved in European Court of Human Rights cases around medical capacity,[52] environmental nuisance from pollution[53] and state surveillance[54], to name a few. It is an enabling right for other human values like autonomy, identity or dignity.[55] Furthermore, where personal data is within the scope of private life, Article 8 applies there too. [56]Strictly speaking, PbD is broader than iPbD, considering the range of risks to private and family life a technology may pose.

Building on the same roots, data protection law is much narrower, focusing specifically on legalities of processing personal data, with the associated responsibilities of data controllers and the rights of the individuals to whom the data relates. Data protection is also a fundamental right[57] and the protections are outlined in a comprehensive legal framework, currently the EU Data Protection Directive (DPD) 1995[58] (as instantiated in the Data Protection Act 1998 in UK) which is being replaced by the new General Data Protection Regulation 2016.
The GDPR is the same law across all EU member states, without need for domestic legislation, and will be enforced from 25 May 2018. We consider more detail on the GDPR and its provisions in Part 4, when discussing the translation process for the information privacy by design cards. As it is not being enforced currently, our legal

---

[51] i.e. Art 8(2) which states:
"There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

[52] *Glass v UK* (2004); See case law in http://www.echr.coe.int/Documents/Research_report_health.pdf

[53] *Lopez Ostra v Spain* 1994; *Fadeyeva v Russia* 2005; See case law in http://www.echr.coe.int/Documents/FS_Environment_ENG.pdf

[54] See Edwards, L. and Urquhart, L. (2016) Privacy in Public Spaces: What Expectations of Privacy Do We Have in Social Media Intelligence? International Journal of Law and Information Technology *24 (3), 279-310*

[55]See Rogera, I (2012) *Protecting the right to respect for private and family life under the European Convention on Human Rights*, Council of Europe at https://www.coe.int/t/dgi/hr-natimplement/Source/documentation/hb11_privatelife_en.pdf and Council of Europe (2015) *Internet Case Law of the ECHR at* http://www.echr.coe.int/Documents/Research_report_internet_ENG.pdf

[56] *S and Marper v UK* (2008) para 41; http://www.echr.coe.int/Documents/FS_Data_ENG.pdf

[57] Article 7 of the European Union Charter of Fundamental Rights

[58] Directive 95/46/EC

analysis looks to existing law too (DPD), with the backdrop of looking ahead to new GDPR and what this might mean for designers.

Whilst we analyse iPbD as a tool for legal compliance with DP law, as mentioned before, for UCR, compliance is not enough. The ethical responsibilities designers have to users and their data need to be considered too, hence we refer to PbD more broadly too. The recent EDPS Opinion[59] on risks from IoT, for example, advocates the need for digital ethics (EDPS, 2015b, p12) looking beyond legal compliance to consider accountability and sustainable data practices and dignity of users (EDPS, 2015b, p14). Indeed, data protection law and the GDPR does much here, referring to importance of building trust and control between controllers/processors and data subjects.[60] However, we want to briefly consider the broader background to privacy, and privacy rights, to situate how designers might engage with it legally and ethically.

Privacy is understood in many different ways, socially, philosophically and legally (Solove, 2006). With privacy rights in particular, they can take many forms, from the classic, narrow 'right to be let alone' (Warren and Brandeis, 1890), to 'secrecy, solitude and anonymity' (Gavison, 1980), or a right to information control and self-determination (Westin, 1967). Privacy is associated with many human values like dignity (Brownsword, 2008), integrity (Clarke, 2006) and autonomy (Bernal, 2014). It can also be framed descriptively as it relates to context, from spatial and bodily privacy to behavioural and informational privacy (Jaap Koops et al, 2016).

Privacy has many attributes, roles and justifications. It makes little sense to abstractly define these elements here, as they vary greatly depending on the context. Whilst abstract legal instantiations for principles and rights exist, we are interested in how they obtain meaning in application. As Nissenbaum (2009) states "*believing that one must define or provide an account of privacy before one can systematically address critical challenges can thwart further progress*". (p2) In line with this, the following framings of privacy are useful for this thesis, as they focus on the importance of context, interaction and lack of desire to absolutely define the concept or its value.

---

[59] European Data Protection Supervisor Website, Duties (2016), accessed at https://secure.edps.europa.eu/EDPSWEB/edps/site/mySite/Duties

[60] Recital 7 GDPR

Solove (2008), inspired by Wittgenstein's (1953) 'family resemblances', argues 'privacy is an umbrella term for a plurality of things'(p45), where it obtains meaning from an association of values understood in context, not from the top down. Our discussions in the case studies around **control** over flows of information and **access** to data or **choice** around consent to processing, shows the diversity of values operating under the umbrella term of privacy.

Similarly, Nissenbaum (2009) frames '**privacy as contextual integrity'**, meaning privacy is ensuring the contextual appropriateness of flows of information, where privacy harms stem from breach of integrity of those flows. Appropriateness and integrity are not abstractly defined, but emerge from experiences of users. This provides a flexible framing, away from abstract absolutes of privacy, instead analysing information flows in context (Nissenbaum, 2009). This fits with the more interaction orientated views we propose here, understanding how we live with technologies and how regulatory issues manifest in context for users. Similarly, Dourish and Anderson (2006) frame **privacy as interaction,** where understanding of privacy cannot be externally defined, but instead emerges from negotiations and interactions of users with technology.

With information privacy rights, we focus our analysis on interpreting how these high level legal rights and responsibilities manifest in practice for designers, through use of case studies. These help situate our discussions in both legal questions of compliance, and the ethical challenges designers may face in managing information privacy rights and responsibilities.

The Legal Nature of Information Privacy by Design

We now turn to the legal nature of information PbD. Article 25 GDPR places obligations on **data controllers** to protect freedoms and rights of individuals, implement data protection principles and generally comply with requirements of the new law. This is done by employing safeguards during data **processing** (Article

4(2), GDPR, 2016).[61] Safeguards require adoption of appropriate **technical and organisational measures** that reflect the:

- *"state of the art,*
- *the cost of implementation*
- *the nature, scope, context and purposes of processing*
- *risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing"* (Article 25(1), GDPR, 2016)

Safeguards shall be considered at the *'time of the determination of the means for processing and at the time of the processing itself'* and the measures can consist of:

- "*minimising the processing of personal data,*
- *pseudonymising personal data as soon as possible,*
- *transparency with regard to the functions and processing of personal data,*
- *enabling the data subject to monitor the data processing,*
- *enabling the controller to create and improve security features.*" (Recital 78, GDPR, 2016)

In addition, **by default**, technical and organisational measures should be taken to ensure **processing is:**

- For *'personal data which are necessary for each specific purpose of the processing';*
- Controlling the '*amount of personal data collected, the extent of their processing, the period of their storage and their accessibility*'
- That '*personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.*' (Article 25(2), GDPR, 2016)

Compliance with Article 25 can be demonstrated by implementing **organisational and technical measures, adopting internal policies, or accreditation through new certification mechanisms**.[62] Legal compliance is important because a key attribute of the new GDPR is much **larger fines**. Data controllers or processors

[61] Processing is very broad – see below.
[62] These are proposed but not yet developed.

can now be charged up to the higher of €20m or 4% of global turnover (Article 83, GDPR, 2016) for failure to comply.

As we can see, the law establishes a range of challenging obligations and responsibilities. Safeguards have to balance a range of requirements, assessing risks to user rights, and responses need to be measured against costs, technical state of the art and so forth. Furthermore, these safeguards need to be implemented by **default**, a requirement that invites a design led response, for example providing greater user control through predefined settings or interface layout. In addition, following a data minimisation approach, Article 25 challenges practices of collecting as much data as possible. It reasserts processing has to be tied to specific justifications (purposes) of collection, and reminds controllers of wider responsibilities to managing the storage, access and control of personal data.

As we argued at the beginning, these rather technical legal requirements fall to technology designers. The legal definitions of **data controllers**, as drafted in Article 4(5) GDPR, and the nature of **processing** of **personal data** are sufficiently broad to **encapsulate a range of system designers. This brings a range of designers from manufacturers to third party services and their activities within the scope of iPbD**.

The legal definitions of personal data, data controller, and data processing are as follows:

- Data controllers are "*the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data*" (GDPR, 2016, Article 4(5))

- Data processing is "*any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction*" (Article 4(2), GDPR, 2016).

- Personal data is "*any information relating to an identified or identifiable natural person*" (GDPR, 2016, Article 4(1); DPD 1995, Article 2(a)). Difficult to contextualise, examples include "*name, address, date of birth, contact details, financial, medical, and social work details, identifiable photos, relationship status, political allegiance, sexual, genetic, biometric, racial and ethnic details, school records, domestic situation and so forth*" (Edwards, 2009, p445)

In addition to these wide, all-encompassing definitions, looking at GDPR Recital 78[63] we get a sense of the breadth of actors and processes envisaged as being captured by Article 25. It states:

"*When* ***developing, designing, selecting and using applications, services and products*** *that are based on the processing of personal data or process personal data to fulfil their task,* ***producers of the products, services and applications*** *should be encouraged to take into account the* ***right to data protection*** *when* ***developing and designing such products, services and applications*** *and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations* (GDPR, 2016, Recital 78)."

Accordingly, the law is explicitly putting **those designing new personal data driven technologies at the forefront of compliance with information privacy laws.** As HCI designers are most proximate to end users, this pulls them into being regulators. We now turn to **conceptual** challenges in doing PbD, before looking to the kinds of legal questions these raise in our case studies. We return to **our empirical data** on challenges of doing PbD in part 3 and 4.

Challenges for Privacy by Design

How PbD might be implemented is uncertain. A detailed understanding of the law and policy environment is not prevalent with engineers. Birnhack, Toch and Hadar (2014) have argued "*whereas for lawyers PbD seems an intuitive and sensible policy tool, for information systems developers and engineers it is anything but intuitive*" (p3). Similarly,

[63] Recitals are interpretative guidance at the start of an EU legislative instrument

Danezis et al (2014) ENISA Report on Privacy by Design Tools highlighted "*we observed that privacy and data protection features are, on the whole, ignored by traditional engineering approaches when implementing the desired functionality. This ignorance is caused and supported by limitations of awareness and understanding of developers and data controllers as well as lacking tools to realise privacy by design. While the research community is very active and growing, and constantly improving existing and contributing further building blocks, it is only loosely interlinked with practice*" (p4). Legal commentators, like Jaap Koops and Leenes (2014) echo this, arguing guidance on PbD in practice is lacking (p161), as does Brown (2015) who recently stated "*the specifics of implementation [for PbD] have so far only been developed to a limited extent*" (p26). Nevertheless, privacy by design (PbD) is often cited as the solution to many challenges of IoT (Brown, 2015; Danezis 2014). **Solutions are needed to bridge the gap between these two communities, and our information privacy by design cards in Part 4 aim to do this by moving PbD beyond theory into practice.**

Nevertheless, technical work addressing privacy challenges of systems exists, offering options to doing PbD, so we turn to these. Privacy enhancing technologies (PETS) (Camp and Osorio, 2003), privacy engineering (Dennedy, Fox and Finneran, 2014; Oliver 2014; Spiekermann and Cranor, 2009), usable privacy (Iachello and Hong, 2007) and human data interaction (Mortier et al, 2014) all have much to offer here. Gürses (2014) taxonomy of privacy research in CS and privacy engineering helps us categorise the types of research being conducted from the technical perspectives. She states research broadly falls into three camps:

- **Privacy as confidentiality** – data minimisation approaches, robust information architectures and scrutiny of solutions

- **Privacy as control** - procedural protections, informing user decisions around processing eg improving readability of privacy policies; designing for compliance with data protection law/fair information principles

- **Privacy as practice** - privacy is viewed as interactive and negotiated, with designers/engineers adopting a role that supports this.

Within privacy engineering, both policy and architectural responses can be adopted (Spiekermann and Cranor 2009; Cranor, 2013). With architecture, issues like control over the network, linkability of data to individuals, anonymity of data and database management are central (Spiekermann and Cranor, 2009). Policy approaches focus on notice and choice, providing users access to data for users, inform users of data sharing and technical approaches to auditing.[64] Spiekermann and Cranor (2009) conclude hybrids can work, but favour technical approaches, stating "*the privacy by architecture approach generally provides higher levels of privacy to users more reliably and without the need for them to analyse or negotiate privacy policies. In some cases, it can provide better privacy protection while still offering a viable business plan*" (p79).

The area of **usable privacy and security** involves technical responses to regulatory challenges of privacy in a way that is comprehensible and usable for end users. It is a wide field, but some examples include increasing user control by setting machine readable permissions for data collection from devices/browsers (Cranor et al, 2002); using software agents to manage privacy or consent on a user's behalf (Gomer et al, 2014); improving quality of notice and choice mechanisms; creating 'nutrition labels' for users to compare privacy policies (Kelley et al, 2009), or nudging users towards more cautious sharing practices (Wang et al, 2014). Hong (2009) stresses the methodological importance of HCI in usable privacy and security for usability analysis tools, and looking at wider interests of users when balancing trade-offs in design (Iachello and Hong, 2007, p4).

Human data interaction (HDI) shares characteristics with usable privacy and security, engaging explicitly with law (Mortier et al, 2014). Their focus is on personal data created by and about us through devices, networks and our daily interactions. They want to place "*the human at the centre of the flows of data, and providing mechanisms for citizens to interact with these systems and data explicitly*" by focusing on **legibility, agency and negotiability** (p2-6). ***Legibility*** is more than transparency, seeking tools to raise awareness of data, its collection and the implications. ***Agency*** puts users at centre of systems, empowering them through control and information around practices of personal data use, collection, and storage (p8). ***Negotiability*** is the ability of users to act and change how their data is used. Chaudhry et al (2015)

[64] Section 5

Databox personal data container takes these principles and embodies them in a technical system that stores streams of data from different devices into one place, allowing users to control access, for third parties like companies. The focus on usability, control, and protecting the interests of the users is useful.

As law is dependent upon interpretation, formalist attempts to build compliance with DP rules into a system have to contend with subtleties and nuances of legal language. Addressing this, Hildebrandt and Jaap Koops (2010) have argued for a notion of 'ambient law' to reflect the "*shift from the use of technologies to interaction with technologies*" (p454), considering how legal rules and their meaning may be reframed if transposed within the medium of technology. To do this Hildebrandt recognises lawyers need to *"uncover what language computer systems speak, and [this] invites us to come to terms with the way computer scientists who design such systems actually 'think'"* (Hildebrandt, 2013, p5). Similarly, Jaap Koops and Leenes (2014) argue for focusing energy on communication between lawyers and designers, "*fostering the right mind-set of those responsible for developing and running data processing systems"* (p168). In the HCI literature, Dourish and Anderson (2006) contend privacy and security are integral considerations when designing systems, and "… *support for effective privacy protection cannot be grafted onto a system because it is a pervasive aspect of how that system it is designed…it is a pervasive aspect of how the system will be used, the context in which it is put to use, the values that it is used to support, the interpretations that others will make of its use*" (p337).

Accordingly, whilst there is a body of work looking at technical aspects of privacy, and the user interests within, **fostering the mind set and awareness of law for designers is key**. **This aligns with our goals of how to practically do PbD, and support interaction between these the legal and design communities**. Law is not intuitive or accessible to non-lawyers, yet by calling for privacy by design, the law is mandating non-lawyers to be involved in regulatory practices. **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, principles and regulatory frameworks framed in complex, inaccessible legalese is not a good starting point. However, the fundamental rights and values (e.g. liberty, autonomy, or dignity), explored in **case law** (e.g. from the European Court of Human Rights and the European Court of Justice, **legislation** (e.g. the new

General Data Protection Regulation or e-Privacy Directive), and **expert analysis** (e.g. from experts in academia, practice and government, like the Article 29 Working Party) are an invaluable resource to inform HCI designers about PbD and their role within it. What we need is to present the regulatory backdrop in a way that designers can engage with, and to help them understand how law factors into their work, and how they can respond accordingly. Case studies are a good tool here, accordingly, we now turn to the detail of our studies to unpack the regulatory challenges designers may face in doing user centric regulation, and importantly, what role they may have and how they can respond. Follow this we turn to our empirical data around the practicalities of doing privacy by design in parts 3 and 4.

Chapter 5. User Centric Regulation in Practice I: The Case of Privacy by Design and the Internet of Things

Chapter Overview

We contextualise our discussions of user centric regulation by looking at the regulatory environment of privacy by design for the domestic internet of things (IoT) and smart metering. Firstly, we look at the IoT, considering **the nature of IoT and what we can learn for UCR from its predecessor technologies**. Secondly, we look at the **regulatory challenges of the IoT, what went before, and issues users face living with these technologies**. Thirdly, we look at our case study diagrams and ask 'how can designers ensure users have adequate **control** over personal data flows within IoT ecosystems'? This focuses our attention on a specific legal value, control, to unpack the kinds of **designers need to engage with in the practice** of doing privacy by design. We also conclude by considering how designers may respond to these challenges. We propose the repurposing of the trajectories framework (Benford et al, 2009) which is ordinarily used for designing user experiences with technologies, to designing consent mechanisms in the IoT.

Characterising the Internet of Things

The Internet of Things is sitting at the 'peak of inflated expectations' as an emerging technology (Gartner, 2015). Various technology and consultancy firms predict numbers of internet connected devices over the coming years, from Cisco at 24 billon by 2019 (Cisco, 2016) to Huawei at 100 billion by 2025 (Huawei, 2016). In terms of drivers, the Internet Society argues market forces like cloud computing, advanced data analytics, miniaturisation of devices, Moore's law, dominance of IP networking and ubiquitous connectivity have all fed the growth of IoT (Rose et al, 2015, p8).

Nevertheless, **a problem exists in narrowing down what IoT actually is**. Ashton first used the term in 1999,[65] framing IoT around tracking objects via machines, not humans in a product supply chain. Yet, technically speaking, no canonical definition of what is, or is not, IoT has emerged. McAuley (2016) has

[65] Ashton, K. (2009), That Internet of Things Thing, *RFID Journal* at http://www.itrco.jp/libraries/RFIDjournal-That%20Internet%20of%20Things%20Thing.pdf

questioned the utility of concentrating on this issue because "*IoT is not about technical capabilities or novelty, rather it is a social phenomenon that reflects a significant proportion of society, and importantly businesses, who have started to recognise that there is value in building a virtual presence for many of our everyday physical things*" (p1). Nevertheless, **definitions help us appreciate what different organisations mean by IoT. We focus on perspectives from different stakeholders below, namely the** UK Government, Office for Science; EU Article 29 Working Party; UN International Telecoms Union, International standards setting body the Internet Engineering Task Force and cross disciplinary academic group, Cambridge Public Policy:

Table 2 Definitions of the Internet of Things

Organisation	Definition and Focus
Government Body: UK Government Office for Science	Descriptive and clear: IoT "*is made up of hardware and software technologies. The hardware consists of the connected devices – which range from simple sensors to smartphones and wearable devices – and the networks that link them, such as 4G Long-Term Evolution, Wi-Fi and Bluetooth. Software components include data storage platforms and analytics programmes that present information to users"* (Walport, 2014, p13)
Industry: Cisco	"*the networked connection of physical objects*" but they have extended it to the 'Internet of Everything' which means the more holistic "*networked connection of people, process, data, and things.*" (Cisco, 2013, p1)
Regulatory Body: EU Article 29 Working Party,[66]	Simple, but focuses on connectivity, and ecosystem: devices "*that can be controlled remotely over the internet…most home automation devices are constantly connected and may transmit data back to the manufacturer*" (Article 29 Working Party, 2014, s1.3).
International Organisation: United Nation's International Telecommunication Union	Vague: "*a global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on existing and evolving interoperable information and communication,*" Where a 'thing' is: an "*object of the physical world (physical things) or the information world (virtual things), which is capable of being identified and integrated into communication networks"* (ITU, 2012, p1).
Standards Body: Internet Engineering Task Force (IETF)	Technical focus on mechanisms and infrastructure: "*trend where a large number of embedded devices employ communications services offered by the Internet protocols. Many of these devices often called smart objects are not directly operated by humans, but exist as components in buildings or vehicles, or are spread out in the environment*" (Arkko et al/IETF, 2015, p1).
Cross stakeholder academic group: Cambridge Public Policy	Technical: "*sensors which react to physical signals; software in these sensors transmitting information; a network for this information to be transmitted on; a database and control system which receives and processes this data, and sends a message back out over the network to instruct the initial device or another one that is networked*" (Deakin et al, 2015, p8).

[66] An advisory body made of representatives of the data protection authorities of the EU

The application areas for IoT are growing just as significantly built environment (smart homes/cities), energy (smart grids/metering), transport (autonomous vehicles), health (wearables, quantified self) or agriculture (smart farms) (Walport, 2014, p9-11). Across all groups we'd characterise key aspects of IoT as being:

- **Socially embedded,**
- **Remotely controllable,**
- **Constantly connected devices with networking for information sharing between people, processes and objects,**
- **An ecosystem of stakeholders around the personal data e.g. third parties,**
- **Physical objects with digital presence**
- **Backend computational infrastructure (e.g. cloud, databases, servers)**
- **Device to device/backend communication without direct human input**

Our interest is in application area of domestic IoT as a domain of users in the intimate setting, raising regulatory challenges around privacy. Homes are heterogeneous socially as well as technologically, and in this domain, the IoT is not new, but builds on a long lineage of research, accordingly it is useful to briefly reflect on that trajectory to further situate the term, outlining lessons learned from these previous streams of work.

Learning from the Origins of the Internet of Things

There are many labels for the lineage of work IoT develops from and it is useful to unpack what these are, and the lessons we can learn from them. The technologies include the following:

- **Ambient intelligence** (Aarts & Marzano, 2003; Wright et al, 2008);
- **Ubiquitous Computing/Ubicomp** (Weiser, 1993; Caceres & Friday, 2012; Bell & Dourish, 2006)
- **Pervasive Computing** (Satyanarayanan, 2001)
- **Calm computing** (Weiser & Seely Brown, 1997; Rogers, 2006),
- **Smart Homes/Home Automation** (Crabtree and Rodden, 2004; Harper, 2003).

Weiser's (1991) original, influential vision of post-desktop (Grudin, 1990)[67] ubiquitous computing is one where computing has disappeared, there systems "*weave themselves into the fabric of everyday life until they are indistinguishable from it*" (p94). Managing ubiquity, requires computing to become 'calm' because "*if computers are everywhere they better stay out of the way, and that means designing them so that the people being shared by the computers remain serene and in control*' (Weiser & Seely Brown, 1997, p78)". This requires awareness of context, because as Dourish (2004) states, "*when computation is moved 'off the desktop' then we suddenly need to keep track of where it has gone*" (p20). Achieving 'context aware computing' needs engineering approaches for "*detecting, identifying and locating people's movements, routines or actions with a view to using this information to provide relevant information that may augment or assist a person or persons*" (Rogers, 2006, p408).

A cohesive community and research agenda has grown around the goals of calmness, contextual awareness and invisibility in use. Liu et al (2014) analyse leading ACM conference *Ubicomp*[68]over 15 years, showing between 1999-2007, the field focused on location based applications and mobile devices, networking challenges and determining user context from.[69] Around the same period, there was significant industry and government investment, like the European Commission's 'Disappearing Computer programme',[70] ISTAG[71] (Ducatel et al, 2001), Philip's 'Vision of the Future' and the 'HomeLab'.[72] These typified the early wave of research, and related variations of Weiser's visions emerged, with subtle variations and similarities, but broadly similar attributes. These include:

- Pervasive Computing - Satyanarayanan (2001) focuses on invisibility, defining it as "*a pervasive computing environment as one saturated with computing and*

[67] *Ubicomp* i.e. many computers to one person was framed as the next trend in the transition from *mainframe computers* i.e. many people to one computer to *personal computers* i.e. one person to one computer, via the transition of the *internet/distributed computing*. See Weiser and Seely Brown (1997) p1-2

[68] Handheld and Ubiquitous Computing which became Pervasive and Ubicomp (which later merged to just be Ubicomp)

[69] From 2007-2014 it moved away from location and networking topics to sensing, crowd-sensing, and data analysis

[70] http://www.disappearing-computer.eu/resources.html

[71] Information Society and Technology Advisory Group

[72] http://www.research.philips.com/technologies/download/homelab_365.pdf

communication capability, yet so gracefully integrated with users that it becomes a "technology that disappears" (p2).

- Ambient Intelligence (AmI) - Aarts and Marzano (2003) AmI is typified by five features, systems are embedded, context aware, personalised, adaptive and anticipative. Lindwer et al (2003) capture what AmI is, stating it is: "*the vision that technology will become invisible, embedded in our natural surroundings, present whenever we need it, enabled by simple and effortless interactions, attuned to all our senses, adaptive to users and context and autonomously acting. High quality information and content must be available to any user, anywhere, at any time, and on any device*" (p1).

- Everyware - Greenfield (2006) focuses on the holistic experience of designing for computing being everywhere around us.

Many of these visions and streams of research have been subject to criticism, particularly the various **visions, areas of focus, and underlying principles**. We present these here to learn propose lessons IoT can learn.

Firstly, big, future orientated technological **visions** are predominant in this area of computing, as Reeves (2012) states, "*mixing fiction with extrapolations, and notions of forecast and trajectory, offered a highly attractive and motivating envisioning"* (p1576). However, such future visions often never materialise, indeed, after 25 years Weiser's original vision still remains aspirational (Caceres and Friday, 2012, p15). Instead, Reeves (2012) argues visions are a commentary of the present, because "*in reality envisionings only ever (and can only ever) reflect the concerns of the time, and should be read as such…this means envisioning can only create principles about the present…not predictions of future"* (p1580). Similarly, Bell and Dourish (2006) argue we are already existing in the Ubicomp age, just not the 'yesterday's tomorrow' Weiser envisaged.[73] Instead of trying to achieve his vision of a clean, seamless[74] future, an alternate present has

[73] Bell and Dourish (2006) "*From this perspective, the future that ubicomp has been attempting to build is not our own future, but 1989s future—yesterday's tomorrows*"

[74] Where there are no issues with connectivity or networking for devices, seamless interactions for users with systems

appeared, one that is seen not in labs, but in the real world.[75] Bell and Dourish (2006) argue such visions allow the present, and the difficult challenges therein, to be ignored. For example, in arguing for seamless networking, it means the "*…messy present can be ignored, although infrastructure is always unevenly distributed, always messy. An indefinitely postponed Ubicomp future is one that need never take account of this complexity*" (p140).

There is also a **shift away from the underlying principles** of these visions, such as calmness (Rogers, 2006, p406) or invisibility (Tolmie et al, 2002). With the latter, Tolmie et al (2002) argue invisibility is not just physical invisibility, but instead where computing has become such a part of routine life that it is no longer 'remarkable'. To build such systems require situated understanding of the social context of computing, the actions and routines of daily life, including what makes activities routine.[76] Instead of Weiser's vision of invisibility, they advocate designers look at human actions, not just artefacts, to "*augment the resources, tangible or otherwise, available to the action and to what is done in the doing of that action. Put simply, we need to embed computation within life not just cups*" (p201).

Continuing with the home, Wilson et al (2015), argue the **human focus** is often neglected in technically driven smart home research. Increased efficiency, comfort, convenience, energy management, care, security are oft cited benefits of more technology in the home. However, designers need to look at "*how the use and meaning of technologies will be socially constructed and iteratively negotiated, rather than being the inevitable outcome of assumed functional benefits*" (p466), recognising homes are '*internally differentiated, emotionally loaded, shared and contested places'* (p470). Mirroring this point, Leppänen and Jokinen (2003)[77] state "*inhabitants themselves make a home and little*

[75] Bell and Dourish (2006) "*…by looking outside of the research laboratory, we are looking at ubiquitous computing as it is currently developing rather than it might be imagined to look in the future.*"

[76] Tolmie et al (2002) "*An orderly aspect of things with a routine character is that they can serve as resources for the mutual coordination of unremarkable activities…these resources are mutually available and mutually accountable for those involved in the routine. Also things do of course go wrong in domestic life, alarms can fail – but failure, in contrast to accomplishment, is remarkable and the elements held to account when part of a routine fails are the very ones that are unremarkable at other times*" (p402)

[77] See D Randall (2003) *Living inside a smart home: A Case Study* in Harper (2003) where he argues that practical considerations to thinking about for family life in smart homes include: control over the home and within family relations; location of home members; and social connectivity i.e. internally and externally within the family and broader networks.

everyday practices make the known life go on. People also want to make decisions concerning their use (or non-use) of technology themselves. That is why there should always be the possibility of managing everyday life both with and without technology...a smart home should not be smarter than its inhabitants" (p223).

We return to issues of routine and challenges of living with IoT below, but this earlier research can teach three lessons about understanding IoT (and accordingly regulating IoT). **Visions** can provide useful insight into the present, for example current visions of the IoT see it as being socially embedded, remotely controllable, constantly connected physical objects with digital presence and backend computational infrastructure (e.g. cloud, databases, servers), networking and an ecosystem of stakeholders. However, this is merely commentary of current IoT perspectives, across government, standards, industry, academic stakeholders etc. Whilst descriptively useful, from a regulatory perspective it is useful to remember this vision of IoT is not canonical or absolute, it reflects current attitudes, but may not define the research agenda over the coming years.

These original visions turned away from **focusing** on commitment to engineering implementation of these underpinning technical goals like invisibility or calmness. Instead, there was a turn to the human context, to understand how these technologies may manifest in context. Similarly, for IoT, rather than excessive focus on practicalities of networking, or defining what is or is not IoT, keeping sight on the end user, their interests, and how the technology impacts these in context is key. Indeed, as we see, historically, user interests are sometimes neglected, for example in smart home research discussed above, the human focus is not prioritised. With a turn to UCR for IoT, understanding how user rights and their regulatory interests are impacted will be key.

We now look in more detail at the kinds of regulatory challenges these technologies can pose, and what designers need to respond to.

Regulatory Challenges of Domestic IoT

General privacy concerns around predecessors to IoT have been raised (Belotti and Sellen, 1993; Čas, 2009; Wright et al, 2008, Spiekermann and Pallas, 2005; De Hert,

2009). With Ubicomp, Čas (2009) worries "*ubiquitous computing will erode all central pillars of current privacy protection*" (p167) and reconciling ubicomp benefits with privacy risks is a challenge. Spiekermann and Pallas (2005) fear **paternalism** through ubicomp, where non-negotiable binary rules enable **automatic compliance**, **limit control** and **reduce user autonomy**. With AmI, the SWAMI project (Wright et al, 2008) consider a multitude of threats[78] and vulnerabilities[79] posed by AmI, highlighting privacy, security and trust issues from technical, regulatory and socio-economic perspectives.[80]

Brown (2015) sees **IoT as challenging** for privacy precisely **because it operates in private settings, like homes**, and presents an **attack target that is harder to secure**, and can compromise **physical safety** (e.g. pacemaker hacks) and other home systems (e.g. smart fridges as part of spambot networks) (p25). **Profiling** is also a concern (Article 29 Working Party, 2014, p8).[81] For example, the A29 WP worries **detailed inferences can be drawn about daily life** (Article 29 Working Party, 2014, p8) where "*analysis of usage patterns in such a context is likely to reveal the inhabitants' lifestyle details, habits or choices or simply their presence at home*"(Article 29 Working Party, 2014, p6). Deakin et al. (2015) note **combinations of non-personal data may create sensitive personal data** (which consequently need explicit user consent), for example, systems that collect "*data on food purchases (fridge to supermarket system) of an individual combined with the times of day they leave the house (house sensors to alarm system) might reveal their religion*" (p15).

More generally than the domestic setting, the A29 WP Opinion on IoT highlights privacy concerns regarding **data collected being repurposed, users' insufficient knowledge of data processing by physical objects, and inadequate consent or lack of control over data sharing between such objects** (A29 WP, 2014 p6; Rose et al, 2014, p26-29). Commensurately, there is significant **user concern over**

[78] Chapter 4.6 – eg 'lack of transparency'; 'loss of control and technology paternalism'; 'system complexity, false positives and unpredictable failures'
[79] Chapter 4.7
[80] p269 "*This book has identified many threats and vulnerabilities and many safeguards for dealing with them. Perhaps we have identified too many safeguards or made too many recommendations, at least, in the sense that so many may seem daunting*";
Short Version of legal risks - P De Hert et al "Legal Safeguards for Privacy and Data Protection in Ambient Intelligence" (2009) Personal and Ubiquitous Computing 435-444; Long Version Chapter 5, Wright, (2008)
[81] On profiling generally see Custers (2004) and Hildebrandt (2005)

control of personal data in Europe. A recent Eurobarometer Survey (2015) of around 28,000 EU citizens attitudes to personal data protection showed 2/3 of respondents were "*concerned about not having complete control over the information they provide online*" (European Commission, 2015b, p6). Nearly 70% think prior explicit approval is necessary before data collection and processing, and worry about data being used for purposes different from those at collection (European Commission, 2015, p58). Around 60% also distrust telecoms firms, internet service providers and online businesses (p63).

In responding to these kinds of regulatory challenges around IoT, the Article 29 Working Party (2014) have mapped relevant data protection responses as they relate to various actors in the IoT supply chain.[82] As with PbD, this involves organisational approaches like PIA's and more technical approaches such as making direct changes to design of IoT devices, providing functions for increased end user control of data. We present a selection of these in this table to show the different responses to DP challenges and how they may be spread across different actors in the IoT supply chain.

Table 3 DP Strategies for the IoT Supply Chain

Actors	Responses
All[83]	o Conduct **privacy impact assessments** (PIAs) prior to releasing new applications (share publicly where possible).[84] o If using **raw personal data** is being used, delete quickly after use. o Create **'user friendly' methods** for interacting around consent, rights to refusing processing and when providing information. o **Provide users with more control over their data**[85] o Broadly apply the principles of **Privacy by Design and by Default.**

[82] A29 WP "Opinion 8/2014 on the Recent Developments on the Internet of Things" 14/EN WP 223 Section 6
[83] Section 7.1
[84] Drawing on the 2011 RFID PIA Framework as a reference point
[85] According to the principle of self-determination of data

Operating Systems & Device Manufacturers[86]	○ Comply with **'security by design'** ideals eg encryption, '*provide simple tools to notify users and update devices when security vulnerabilities are found*'. ○ **Increase information available to users** around type, time and frequency of data collection, including providing a '**do not disturb' type function** that has timed disabling of sensors. ○ **Provide tools to allow users to locally read, modify and edit data** (which will be in an interoperable/portable format) before it travels to any other data controllers in the network. ○ For shared devices: "*A setting should be available to distinguish between different individuals using the same device so that they cannot learn about each other's' activities*." [87]
IoT Device Owners and Additional Recipients of data [88]	○ Let **non-user data subjects know about any IoT data collection related to them** and respect their wishes of they don't want their data to be collected.
Standardisation bodies & Data Platforms[89]	○ Promote **portable, interoperable, clear data formats** that enable easy transfers and support user understanding of sharing. ○ **Certify baseline standards** around users' security and privacy ○ Create "*lightweight encryption and communication protocols adapted to the specificities of IoT, guaranteeing confidentially, integrity, authentication and access control*".[90]
Social Platform	○ Social platform[91] applications based on IoT devices need to **let users edit and review information before it is shared on social networks**. ○ Default for any information published on such platforms should be to "*not become public or be indexed by search engines*".
Application Developers	○ **Aggregated data should be used where possible**, instead of raw personal data ○ Incorporate **frequent notices and warnings in systems** to remind users of sensor data collection.

Beyond privacy, other regulatory concerns around IoT include: **interoperability** issues between devices and across platforms (Deakin et al, 2014, p7); problems of **market dominance and inadequate competition** (Brown, 2015, p19); **inadequate spectrum and addresses for devices** (IPv6 solves much of this) (Brown, 2015, p19); need for **leadership on industry standards** (Bouverot, 2015, p16-17) **responsibility** and **liability for harm** from IoT devices (Rose et al, 2015, p38); **technical education, appropriate regulation** and **trust in the security** of these systems(Walport, 2014).

[86] Section 6.1
[87] Section 6.1 p23
[88] Section 6.4
[89] Section 6.5
[90] Section 6.5
[91] Section 6.3

In responding to these regulatory challenges, UCR also requires a turn to the context of technology use. Designers awareness of how domestic IoT impacts users in situ can help inform their role as regulators, and lead to development of more effective regulation. Accordingly, we turn to user experiences around domestic IoT, specifically energy and security, focusing on challenges aligned with regulatory issues.

User Experiences of the Domestic IoT: Energy and Security

Ownership of domestic IoT devices is predicted to rise. The OECD forecast by 2022, a family of four will own 2 connected cars, 7 smart light bulbs, 5 internet connected power sockets, 1 intelligent thermostat and so on.[92] Bouverot (2015) found[93] high interest among 2000 technology enthusiasts across the world in buying a connected ~security system (80%), ~thermostats (79%), ~lighting, car or smart meter (78%) (p5). 23% of their respondents currently own connected security or lighting and 24% a connected thermostat or washing machine. Their interests in domestic IoT varies from drivers like money saving (25%), convenience (19%) and security (16%) (Bouverot, 2015). **To get a deeper understanding of the challenges, we draw on studies of how people live with domestic IoT/smart homes, with particular focus on smart locks and smart thermostat.**

As introduced above, **the home as a setting for domestic IoT is critical.** Homes are complex social spaces where different practices and routines persist (Crabtree and Rodden, 2004, p211). As Tolmie et al. (2002) put it, "*routines are the very glue of everyday life…Routines help provide grounds whereby the business of home life gets done. Routines mean that people can get out the door, feed themselves, put the children to bed, and so on, without eternally having to take pause and invent sequences of action anew…*" (p185). Any technology for the home has to reflect these diverse routines, whilst not disrupting the underlying practices (Tolmie et al, 2003, p203). Furthermore, the house will not become 'smart' overnight. As Edwards and Grinter (2001) have long recognised,

---

92 https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=DSTI/ICCP/CISP(2012)3/FINAL&docLanguage=En

93 A GSMA/KRC survey of 2000 'technology enthusiasts' across the US, Germany, UK and Japan. The participants may skew results somewhat

"*new technologies will be brought piecemeal into the home*" (p257) and as Rodden and Benford (2003) argue, "*domestic environments evolve. They are open to continual change and the need to understand and support this change will be important to ensure the successful uptake and management of digital devices in domestic spaces*"(p11). Capturing the everyday nature, Abowd and Mynatt (2000) acknowledge designing for home computing means interactions are '*continuous in time, a constant ebb and flow of action that has no clear starting or ending point* (p31)' meaning they need to account for interactions being interrupted, concurrent and spread across time.

There are a number of studies on how individuals live with these smart home technologies for energy and security. Brush et al (2011) US study found user's frustration caused by unreliability, devices requiring iterative tweaking over time, and **security concerns about unauthorised remote access (particularly for locks and home cameras)**. They observed users avoiding complex user interfaces eg the mother of a participant sat in the dark to avoid touching controls, and despite this, these systems are still appealing to occupants (Brush et al, 2011). The Bouverot (2015) report cited above showed that for **connected security systems**, owners highly valued benefits like **providing peace of mind (69%), feeling of protection against theft/hazards (67%) and automatic alerts to a phone (64%)**. In practice these benefits are contested, due to the space of the home.

Mäkinen (2016) study of home surveillance systems [94]in Finland found internal tensions for 13 residents around trade-offs, for example balancing benefits of a sense of safety and protection of the home against fear of being watched without knowledge or implications of monitoring other home occupants, such as perceived spying (p75). Similarly, Ur et al (2014) studied US teen and parent attitudes to use of home security cameras and smart locks to audit home entry/exit, with particular reference to privacy and surveillance. They interviewed 13 teens and 11 parents and found there was **broad support with participants for connected locks due to remote control, improved safety and convenience** (p129). They also found **trust between teens and parents could be damaged by increased monitoring**, and that teens would find ways to **resist the monitoring** e.g. "*many teens said a security system would not deter them; they would leave the door or a window unlocked the entire*

[94] systems were access control eg intruder sensors, or cameras.

time they were out of the house" (p135).[95] Choe et al (2011) similar US study[96] of 22 participants cited **benefits of sensing applications like health and safety** (eg keeping an eye on elderly relatives) or **saving money** (eg watching which appliances use too much electricity (p65). However, their participants were concerned about **sensitive, private activities of the home being captured** (being used against them by other members of the home eg in a divorce) and also being **hacked/leaked externally** (Choe et al, 2011, p66).

In contrast, Oulasvirta et al (2012) Finnish surveillance study where 12 participants were 'surveilled' over six months, through sensors like cameras, smartphones, microphones, logging keystrokes on computers, monitoring network traffic etc. found they became **accustomed to surveillance, changed behaviour to 'regulate what the surveillers perceived'** and interestingly, over the six months "*showed no negative effects on stress and mental health attributable to surveillance*" (p49). **Clearly, the setting of the home for security systems involves balancing the benefits like safety and protection, against adverse impacts on family dynamics or risks of unauthorised access to data.**

We now look at **smart thermostats** like Nest's Learning Thermostat.[97] A recent US study shows parents and children often see traditional thermostats as "dangerous or even confusing" with parents afraid of adjusting them, and children avoiding them due to lack of awareness or interest (Horn et al, 2015). Yang and Newman (2013) study of 23 participants living with Nest learning thermostat for at least a month shows a number of **user concerns about control over the technology**, ranging from **frustration** that it ignores what users want ("*NEST is*

[95] See full discussion in Urquhart and Rodden (2016) p34-35 on children's DP rights and home CCTV. Under the Rynes case (C-212/13), where residents home CCTV also points to public spaces (eg adjacent street, shared garden) they cannot claim the former 'household processing' DP law exemption (see Lindqvist case- C101/01). Now they are subject to DP laws, in the same way as companies. This raises challenges around consent, subject access rights and the right to be forgotten for domestic CCTV operators, especially for children visiting the house or playing in front of it.

[96] p62; Looking at attitudes and tensions around in-home systems that sense and make inferences through video, audio, electricity use and movement data for 22 subjects in 11 US homes.

[97] Nest's Learning Thermostat monitors the temperature of a room, builds up a picture of the behavioural patterns of the home occupants (through movement sensing) and creates a schedule for adjusting temperatures and switching heating on or off. It is remotely controllable from a smartphone app, interacts with the boiler and can communicate with other IoT technologies in the home like smart lights, plugs, wearables, washing machines etc through the 'Works with Nest' ecosystem.

doing its own thing and doesn't tell you what it is doing. It just doesn't. So you really don't know – It's very hard to do anything but what it wants to do quietly" (p97) to **lack of comprehension** about how it builds up a schedule ("*It's unclear to me whether [the learning] is done or if it is continuing to learn patterns…the very minimal Nest instructions do not discuss these decision making parameters, but basically ask for trust, (perhaps before trust is earned)*" (p97). Despite these early issues, a follow on study (Yang et al, 2014) shows users who continued to use the Nest found it became **mundane in the home, that they rarely interacted with it** and basically "*as long as the Nest did not set the temperature abnormally, it did not call for our participants' attention, and he or she did not need to actively get involved in controlling or interacting with it*" (p829).

These kinds of accounts about the home are invaluable for unpacking the kinds of social dynamics and reactions to technology that users face in context. Regulatory strategies in these settings could benefit from understanding these dynamics. Heterogeneous devices, routines, family dynamics and user interactions in different homes complicate the landscape for managing legal rights in the home. Nevertheless, thinking about technologies and users in terms of relationships and interactions between them gives us a richer setting to reflect on how legal interests manifest in context**. To understand how designers can engage with these user issues, we now look at legal questions around adequate *control* over personal data in the home, outlining the challenges, and how designers, as regulators, can respond.**

Control over Personal Data in the Domestic Internet of Things

As explored above, the umbrella term privacy is underpinned by a range of human values. We are particularly interested in **control and self-determination** over data, as legal values that have legal grounding in data protection law. Legally speaking, the GDPR states "*natural persons should have control over their personal data*"(GDPR, 2016, Recital 7)[98] and accordingly, when thinking about PbD in practice, user control over personal data is a major element in designing technical and organisational measures. Indeed, as described above, PbD may require, by default, transparency around data handling, with users able to monitor and control access to their data (Article 25(2)). Furthermore, PbD calls for respect of the GDPR as a whole, which includes rights aimed at ensuring user control over their personal data, like the right to be forgotten, data portability and the right to object to data processing (GDPR, 2016, Ch III). Designers also have responsibilities in GDPR, around record keeping and transparency of processing, provision of adequate information to users or conducting privacy impact assessments (GDPR, 2016). We look at these in more detail in Part 4.

As we saw above, adequate control over personal data is a key worry for end users, especially in the domestic setting of the home. Designers, given their proximity to users, and their new role as regulators, have the opportunity to respond to these concerns. How user control is achieved is important to consider, so whilst designers need to respond to the law, reflection on how they do so exposes contentions in the legal values underpinning the rights and responsibilities. This section shows the challenges in how designers respond to legal requirements, and how engaging with underlying legal values can inform their response.

Reflections on Human Rights and Ownership of Personal Data

Many of the challenges consumers have stem from lack of control of their personal data. This sits against a backdrop of the dominant digital business models for online services, like apps, search engines or social media, where payment is through end user's data collection, mining and use by an ecosystem of actors, like advertisers,

[98] Recital 7

marketers and data brokers (Bourgesius, 2013). The user has very little control over what is done with their data after it is collected. Some argue privacy is already dead as a social value,[99] and this claim is strengthened by the commercial reality that users often trade privacy for convenience (Rauhofer, 2011). The paradox between what users say and what they do also supports this postion i.e. they value privacy yet they share data widely on social networks, with third parties and direct marketers (Bennett and Raab, 2006). Nevertheless, users still look for more control over their personal data (European Commission, 2015b).

In response, ownership led models are put forth to increase control over personal data, seeing it as something to be owned and thus protected (Hern, 2014).
Intuitively, ownership grants **control** through the power to decide how an asset is used, managed, sold or even destroyed. Even when someone is dispossessed of their asset, ownership persists, for example, if a car is stolen and someone else buys it from the thief, they gain no rights of ownership because the thief did not have title of ownership to give in the first place.[100] Whilst easy to understand with tangible assets like houses, cars, smartphones or laptops, complexity emerges with intangible assets (Edwards and Harbinja, 2013). Data varies in volume, variety, ephemerality, and temporality. It is generated actively or passively across a vast number of services, devices and interactions. It is spread across different contexts, communities and spaces. It is complex to create practical ways of sourcing, managing and storing all the data a user **'owns'** and then them having digital literacy to manage it and anticipate the social implications of selling it. Nevertheless, the law does provide different means for control and ownership of information, such as protection through personality rights, or intellectual property law e.g. with databases rights or copyright, coupled with contractual licensing (Rendle, 2014; Edwards and Harbinja, 2013). Ownership led models ideologically see data as an asset class (World Economic Forum, 2011), something to be traded that users should benefit from (Schwartz, 2003) captured by Kuneva's (2009) famous statement "*personal data is the new oil of the internet and the new currency of the digital world*" (p1).

[99] K Noyce (2015) Scott McNealy on Privacy, You Still Don't Have Any, *PC Advisor*, Jun 25, 2015 at http://www.pcworld.com/article/2941052/scott-mcnealy-on-privacy-you-still-dont-have-any.html
[100] Legal principle 'nemo dat quod non habet' – i.e you cannot give what you do not own.

This brings us to the tension in underlying legal values in how control is achieved. As an analogy, how designers respond to data protection responsibilities can be framed in terms of European vs US approach to personal data. In Europe, as we know, informational privacy is a fundamental human right, and accordingly data is given high general levels of protection (Edwards, 2009; Solove, 2008). In the US, personal data has no such general protection, and only sector specific rules exist e.g. for health or children's data.[101] In the US, academics have argued for market led approaches, where data is seen as property (Westin, 1967), and subjects should be paid for its use (Laudon, 1996). As human rights cannot be bought and sold, this position is more objectionable in Europe (Harbinja, 2013)[102] although Prins argues a property based model is possible (Prins, 2006).[103] Generally, many tensions in Europe between regulators and large US companies stem from the different mind-sets in US and Europe, as we have seen in recent cases like Google Spain[104] or the Schrems decision.[105]

Ideologically, the human rights approach is important because such rights are inalienable i.e. everyone has them irrespective of power or wealth and they cannot lose these due to sale (Urquhart, 2016). [106] An ownership model sees data, and the associated values, being traded away for a price. This may create inequalities between those who can afford privacy, and those that cannot. In the future, personal data trading platforms may emerge and if used for trading energy consumption data for income, for example, risks to the rights of financially and socially vulnerable, especially those dealing with fuel poverty, may emerge (Fischer et al, 2014).

Privacy and data protection law already provide mechanisms for **controlling** data from subject access or rectification rights to rights to object to data processing; to

---

[101] Children's Online Privacy Protection Act (COPPA); Health Insurance Portability and Accountability Act (HIPAA)
[102] See comprehensive overview, especially section 4.2
[103] Prins (2006) p232 - property in data may mean less data collection, as new costs for would be incurred, challenging their default model of collecting as much personal data as possible.
[104] C -131/12 http://curia.europa.eu/juris/liste.jsf?num=C-131/12
[105] C-362/14 http://curia.europa.eu/juris/documents.jsf?num=c-362/14
[106] Although they cannot always afford litigation to enforce them. In UK common law, the action of Misuse of Private Information is primarily used by celebrities - see Urquhart (2016)

data erasure upon request, to restrict data processing and to portability for moving data between services (GDPR, 2016, Ch III).
The challenge is implementation, and designers have a key role here to play. Designers as regulators can decide how to increase control over personal data. By incorporating technical responses to data protection and privacy rights into design process, as PbD aims to do, they can increase control without moving to an ownership led model.

To further understand the challenges that surround control of personal data in IoT ecosystems, and how designers can respond appropriately, we focus on answering the question of **how can designers ensure users have adequate *control* over personal data flows within IoT ecosystems?** using diagrams and specific examples to structure our answer. In contrast to the more state led smart metering regulatory framework, legal relationships and flows of data in IoT ecosystems between user and technology are more heavily mediated via contracts. With market led IoT infrastructure, designers have greater freedom in how they respond to regulatory challenges, and in this section we consider two approaches they may adopt.

For our example, we consider the smart thermostat, the Nest Learning Thermostat and its associated ecosystem, 'Works with Nest'. The thermostat monitors the temperature of a room, builds up a picture of the behavioural patterns of the home occupants (through movement sensing) and creates a schedule for adjusting temperatures and switching heating on or off. It is remotely controllable from a smartphone app, interacts with the boiler and can communicate with other IoT technologies in the home like smart lights, plugs, wearables, washing machines etc. through the 'Works with Nest' ecosystem.

Below, we map the actors and personal data flows in this ecosystem in figure 2, following the legend provided below in figure 1. These diagrams are based on our methodology explained at the start of this section i.e. extensive documental analysis, informal conversations, conferences, events etc. **Despite this, there are still uncertainties about the nature of the information flows, as figure 2 captures. Indeed, this is one of the challenges that designers may need to address in**

doing UCR, as the lack of transparency about data flows in this ecosystem pose challenges for end user control over their personal data.

We now turn to figure 2 where the actors and data flows can be explained as follows:

<Home Occupants> buy a *NEST Learning Thermostat* <**IoT device**> to help with energy management. The personal data flows from them to the physical device, NEST Labs <**IoT Device Manufacturer**> and their cloud setup <**Cloud Data Storage**>. This data stored in the cloud is accessible by the smartphone or tablet app used to manage the system <**IoT Device Management Application**> which shares data with the phone's local and cloud storage, **<cloud data storage>** likely owned by the **<Mobile Platform Operating System>** or Mobile **<Device Manufacturer>.** Less certain is to what extent information is shared by the various actors with **<third party business>** eg advertisers, **<social networking platform>** eg Facebook or Twitter, **<law enforcement agency>** e.g. the police or the **<smart metering infrastructure>** eg is the networking hub used for IoT devices too? Equally, there are other IoT Devices in the home, in our example a *Yale Smart Key* **<IoT Device>** and how these flows and infrastructure intersect is complex. Thus, it is considered separately below by looking at the *Works with NEST ecosystem* which links security, energy management, lighting, healthcare devices together, each with their own respective approaches.

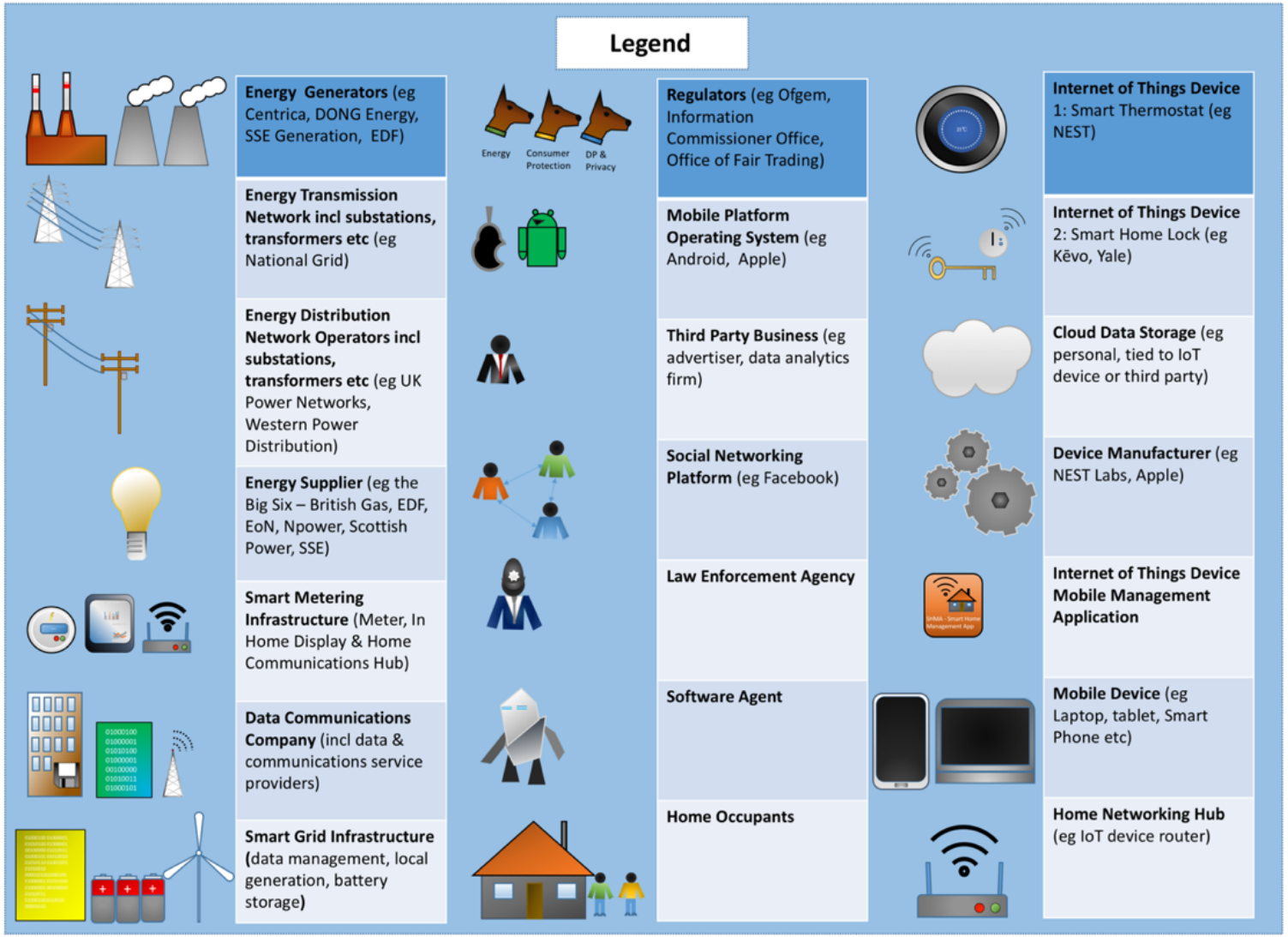


Figure 1 Legend for Diagrams

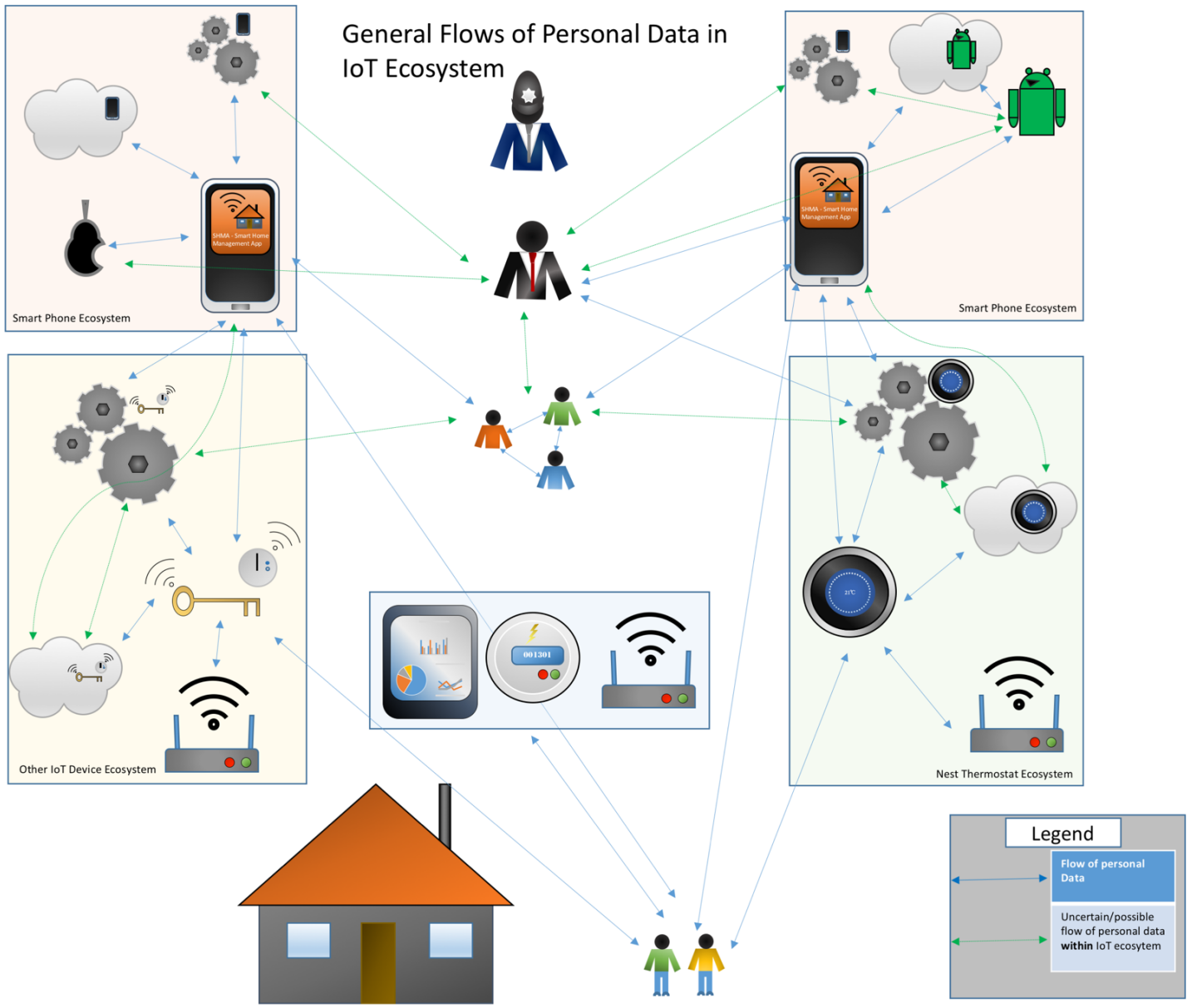


Figure 2 Personal Data Flows in Domestic IoT Ecosystems

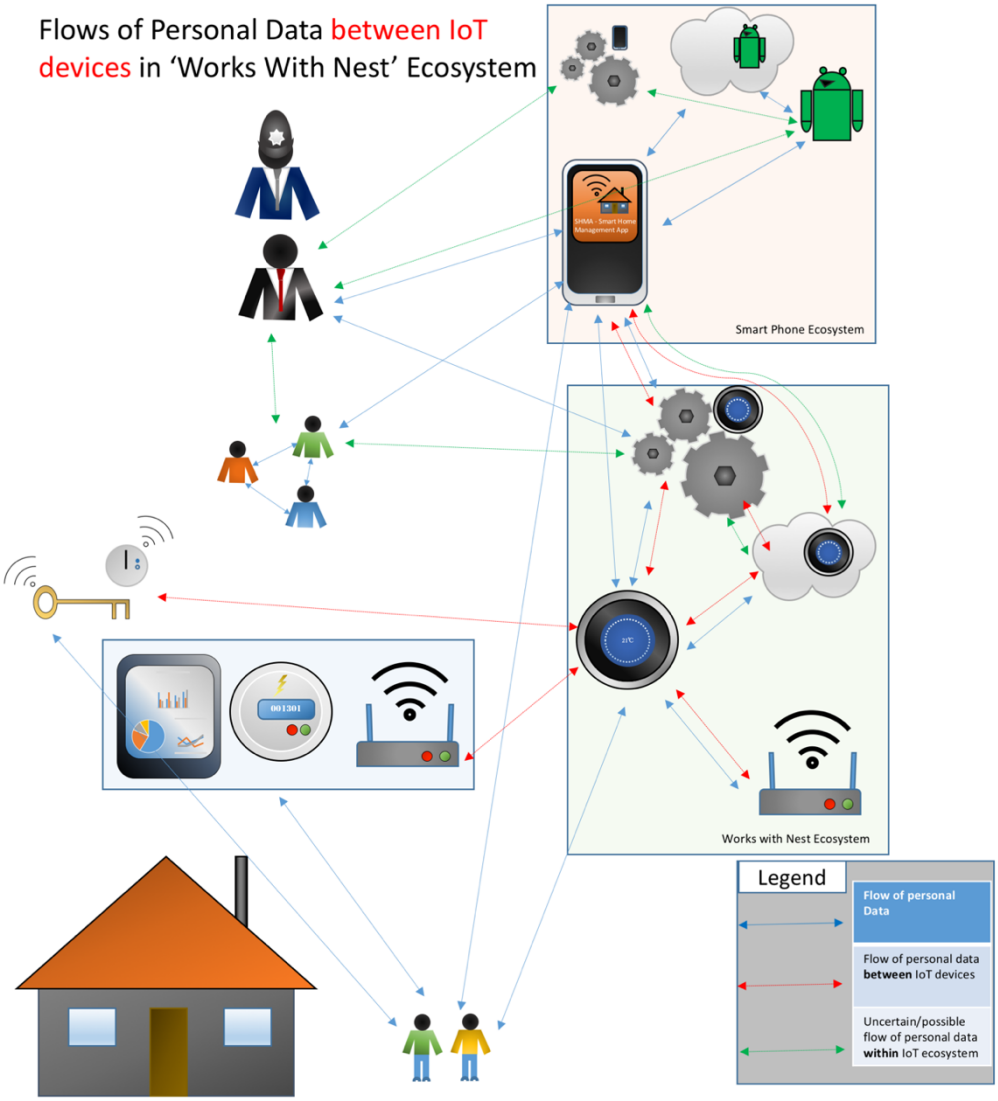


Figure 3 Personal Data Flows in the 'Works with Nest' Ecosystem

In figure 3, data from the **<home occupants>** goes to the Nest Thermostat **<IoT device>** and could pass to the other device directly eg via networking protocols like Bluetooth, ZigBee[107], z-Wave[108] etc[109] or to **<smart metering infrastructure>**, or it between the respective cloud solutions **<cloud data storage>, <home networking hubs>, <IoT device management applications>** or directly between **<IoT device manufacturers>**. However, given different industry

[107] Zigbee Website - http://www.zigbee.org/
[108] Z Wave Website - http://www.z-wave.com/
[109] Guide on Smart Home Wireless Networking- http://www.tomsguide.com/us/smart-home-wireless-network-primer,news-21085.html

approaches, it remains uncertain talking in the abstract so we look at a specific approach, how the Yale Smart Lock talks to the Works With Nest ecosystem via their networking protocol, Nest 'Thread'.

'Works with Nest' is an IoT device ecosystem where Nest devices can link up to partnered third party devices like smart lights, plugs, wearables, and washing machines. [110] Devices are verified on the Nest mobile device app, enabling communication and sharing of device sensing capabilities, for example:

- When a smart doorbell senses movement at the door and Nest get Cam to record who is there.

- When a pet eats from the smart pet-food feeder, Nest Cam can take a snapshot and send it to the owner.[111]

How personal data might flow between IoT devices depends on their underpinning architecture. Nest devices like the 'Cam' Home Security Cameras, the 'Protect' Smoke alarm and the 'Learning Thermostat' are already designed to work together. Cam, for example, records constantly when the Learning Thermostat is set to Away from home mode.[112] With third party devices it is more complex, so we look at the Yale Linus Smart Lock and how it integrates with 'Works with Nest'.

Linus is a home entry system that allows the resident to issue temporary passwords to different people for home access and to get updates to their smartphone about entry/exit and to remotely lock/unlock the door. Whilst Nest devices have an ecosystem of internet connected services like device management apps or Nest Cloud, **Linus does not have these**. Instead, through a networking protocol called Weave,[113] devices communicate peer to peer, i.e. Linus speaks to Nest and Nest

[110] Nest Cam website - https://nest.com/uk/camera/meet-nest-cam/
[111] eg Petnet website http://www.petnet.io/works-with-nest or Skybell website http://www.skybell.com/
[112] Works with Nest Website https://nest.com/uk/support/article/Learn-how-Nest-products-work-together
[113] Thread Group Website - http://threadgroup.org/Join.aspx -

speaks to its ecosystem of services. For the user, the new device is managed by adding Linus to the Nest App, as opposed to a standalone Linus app.[114]

Looking at a bit more detail on the networking protocol, Weave is based on Thread (figure 4)[115], a protocol developed to be simple to use, secure, power efficient, support IPv6 and available for different home devices.[116] Importantly, it encrypts data end to end, and Thread has industry support from members like ARM, Samsung, Qualcomm, although rival approaches like Zigbee or Z-Wave exist. Weave creates a mesh network, directly connecting different devices with information passing along the network on multiple possible routes, until it reaches an internet enabled node, where it can then access internet based services. In the diagram[117] Nest devices would be 'internal' and 'border routers', and Linus would be a 'host'. The heterogenous capabilities of IoT devices, for example different power supplies preventing support for WiFi connectivity or lack of processing capacity for complex data analytics, leads to new design responses, like Weave.[118]

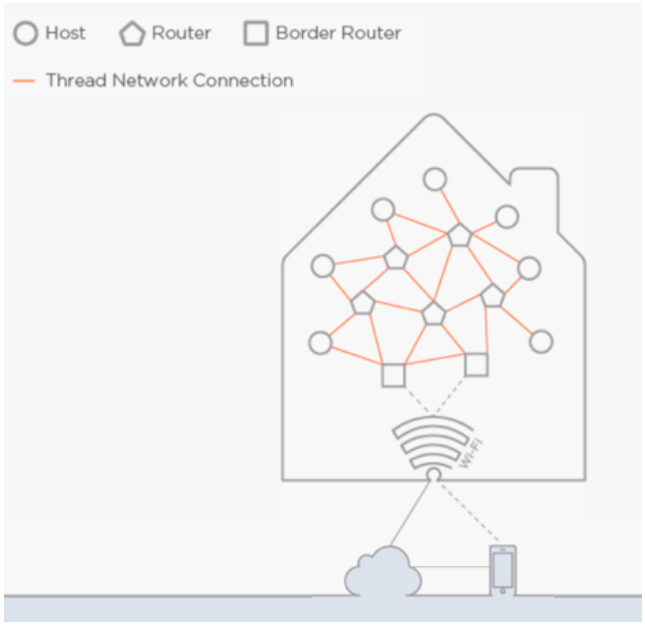


Figure 4 Thread Networking Protocol

Nest's position in this device to device to internet setup creates an interesting business model. As Nest themselves argue "*if Yale had chosen to connect their lock to the internet without Nest, they would have had to build and maintain all the services themselves. By*

[114] Nest Weave - Website https://nest.com/press/nest-introduces-nest-weave-creating-most-comprehensive-developer-platform-for-the-home/
[115] Nest Developer Documentation on Nest Weave https://developer.nest.com/documentation/weave/weave-overview; See also The Register - http://www.theregister.co.uk/2015/10/01/nest_app_protocol_open_to_devs/
[116] Thread Group Website - http://threadgroup.org/About.aspx
[117] Thread Diagram from http://threadgroup.org/Technology.aspx
[118] Nest Weave - Website -https://nest.com/press/nest-introduces-nest-weave-creating-most-comprehensive-developer-platform-for-the-home/

using Nest Weave, Yale was able to skip the time and effort spent on infrastructure and jump straight to building features that differentiate Linus lock from other locks on the market." [119] Works with Nest is more than just compatibility or simplicity for consumers, Nest becomes a key gatekeeper and services platform in the home network. Whilst the home IoT domain is growing, Nest becomes a point of control for flows of data, making them an information gatekeeper for information from other IoT devices. This market will be supported by a 'Works with Nest store' to find compatible devices.[120] Whilst commercially this position makes sense, and strengthens Nest's market position to becoming the dominant smart home platform, from a regulatory perspective it creates obligations. As we've seen in other domains, gatekeepers are a leverage point in the regulatory chain (Laidlaw, 2015) for example with ISPs providing browsing behaviour to police;[121]social networking sites removing offensive material;[122] or search engines liability being questioned for content on search results (Edwards, 2010). A key question is how Nest, and 'Works with Nest' ensure adequate user control over transfer of personal data within their ecosystem.

Accordingly, we need to turn to IoT device and service contracts to understand the legal relationship with users, and third parties. There are many sales and service contracts between users and devices in the IoT ecosystem, for example service contracts with cloud storage, mobile platform operating systems or IoT device management applications, or sales contracts for mobile and IoT devices. As we are interested in how users exercise control, we focus on elements across the Nest privacy policy, service and sales contracts that pertain to this, especially around third parties. The contractual analysis was concluded in Summer 2015, and is based on Nest contracts from 17 June 2015.[123]

---

[119] Nest Developer Page on Yale https://developer.nest.com/stories/yale

[120] See ARS Technica http://arstechnica.co.uk/gadgets/2015/10/nest-updates-cam-connects-third-party-devices-through-thread-network/

[121] Crown Prosecution Service Guidelines on Guidelines on prosecuting cases involving communications sent via social media https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/473770/Draft_Investigatory_Powers_Bill.pdf

[122] Draft Investigatory Powers Bill 2015 http://www.cps.gov.uk/legal/a_to_c/communications_sent_via_social_media/

[123] Long after our contractual analysis finished in summer 2015, reassuringly, in late Sept 2016 (time of submission), EJLT published a paper on doctrinal legal analysis of Nest contracts (La Diega and Walden, 2016 at http://ejlt.org/article/view/450/658). It offers private law insights, particularly around unfair contract terms.

Most detailed is the *Privacy Statement for Nest Products and Services* which covers all **products** i.e. Nest Learning Thermostat, Nest Protect Smoke Alarm, Nest Cam and **services** i.e. their web interface, mobile applications, Works with Nest etc. [124]We consider detail on **types of data collected, purposes of collection and sharing practices with third parties.**

Clause	Explanation
Data Collected	• Data collected by individual Nest Devices and Services varies. Nest Thermostat, for example, collects: **temperature; humidity; ambient light; movement; temperature adjustments; post code (for weather information); HVAC/boiler data and; usage information**.[125]
Why data is collected	• Data is collected for **provision, development and improvement of Nest products and services** especially recommendations on products, safety, and energy use. • **Non-personal, aggregated, anonymised data** is used for a number of purposes. This includes **sales, marketing and business decisions** eg sharing user data with partners on restricted basis like active thermostat statistics when forming partnerships with energy companies.
Sharing with third parties through Works with Nest	• Sharing data with third party partners (eg Yale) through Works with Nest requires users to be **shown details of the proposed data exchange**, **developers need to give reasons why they need data**, and users need to **provide explicit consent**. • Their **default is not to share data** – as they state, "*under no circumstance do we share personal information for any commercial or marketing purpose unrelated to the delivery of Nest Products and services without asking you first. Period. We do not rent or sell our customer list*s". However, they may **share data in certain circumstances**: o when users give **explicit consent**; o when **externally processed by technicians** and vendors involved in processing and storage of data; o where there are **explicit controls on their employees** using data and their access to video data (eg from Nest Cam); o if **Nest is sold** and data is part of the sale; o to comply with a **legal request from the government**.

[124] Privacy Statement for Nest Products and Services 17 Jun 2015 (it is not paragraphed hence quotes are drawn from across the agreement without specific attribution)
[125] "What Information does the Nest Learning Thermostat Collect"

	• **Any data from Nest then possessed by a third party is subject to a third party privacy policy**. Nest warn users to always check third party privacy policies, as Nest have no control over them. • Any data that Nest receives from third parties will be treated under the **Nest Privacy policy.**

Table 4 Analysis of Privacy Statement for Nest Services and Products

Service contracts are very important as they mediate the legal relations between customer and manufacturer over the life of the product, so we now consider *Nest's Terms of Service.* This governs personal access and use by users of Nest Web and mobile apps, and various extra subscription services. [126] It provides a bit more insight into the ongoing relationship between Nest and the end user especially around retained device control, third party relationships, liabilities and redress for consumers.

In terms of control, they retain a lot of control over functionality of the device, for example they can activate Bluetooth on mobile devices (with or without prior notification) to ensure products work properly and can speak to each other, and to 'enable certain features'[127] or can do remote, automatic updates to devices, like patches, upgrades, bug fixes, without needing additional user consent. Users only redress to this is to stop using the product/service.[128]

In terms of third parties, Nest use Amazon Web services for storage, synchronisation, communication with devices, and they may use mobile operators for notifications.[129] Furthermore, with third party services/product, like Works with Nest, users are given more responsibility. They need to decide if they want Nest to share information with a third party, then provide explicit consent/authorisation, and once data is shared with the third party, their privacy policy or terms and conditions governs it, not Nest's.[130] They push responsibility

[126] Nest Terms of Service 17 Jun 2015 part 3(a)
[127] part 3 (e)
[128] part 3(b); This is also in the EULA para 3
[129] part 5(b)
[130] part 3(c)

to users who need to not just be reading Nest's Ts and Cs but those of other platforms that Nest works with.

Whilst Nest do not guarantee any specific energy savings/monetary benefit from using their products/services,[131] they also extensively deny responsibility for harms and losses arising from third parties. As they do not control these devices/services, even though they provide the Works with Nest platform, eg excluding responsibility for third party links, app stores, ISPs, equipment, harms like compromised safety, property damage, death etc.[132]

Further impacting control, routes for disputing contract terms vary. For example the sales contract is governed by binding arbitration (as opposed to lawsuit) where the outcome cannot be appealed, and will be conducted in California, USA.[133] Arbitration costs are split between Nest and the user and class action suits are not allowed.[134] Interestingly in the EULA (i.e. the agreement governing the software in the device), Nest state California law cannot be applied in all disputes, and in that case the user's countries law will. [135] This is more in line with consumer protection laws around unfairness of foreign arbitration clauses in consumer contracts.[136]

The contracts have some positive features, such as focusing on the need to control data sharing with third parties, increasing transparency of data processing to users, a default position to not share data, and ensuring explicit consent is obtained when data is shared. However, Nest shift a lot of responsibility to end users to be prudent in checking third party Ts & Cs. Whilst pragmatic, given the issues around consent, which we consider below, this could cause issues for end user rights. Indeed, as the diagrams on personal data flows in Works with Nest ecosystem shows, user understanding of who is accessing data, for what purposes, for how long, where it is stored etc is no easy task. Ethically, an ecosystem like Works with Nest has third

[131] part 3(f)
[132] part 5(d)(g);
[133] Sales Terms para 11 (b) and (c)
[134] para 11(d) and (e)
[135] EULA (2015) para 13
[136] Unfair Terms in Consumer Contracts Regulations (UTCCRs) 1999 govern unfair contract terms for contracts entered before 1 Sept 2015, Consumer Rights Act 2015 for those after;

party data sharing as the key feature of its functionality, hence we'd argue designers need a more user centric approach to ensuring legal rights are protected therein.

Accordingly, we suggest that designers, as regulators, could address issues in the current notice and choice approach to explicit consent by **redesigning IoT consent mechanisms using the 'trajectories framework'** (Benford et al, 2009)**.**

Design Responses: Redesigning Consent Mechanisms for the IoT

Before explaining the 'trajectories framework', we firstly need to understand what consent means so we briefly set the scene legally as to **what consent is, why it is important, and how it is normally obtained**. Consent has a longstanding ethical value, for example within medicine, as a mechanism to ensure the choice, autonomy and dignity of individuals (Manson and O'Neill, 2007). The normal approach to obtaining user consent for personal data driven technologies is **form contracts.** These standardised contracts create a model of **notice and choice**, where the **notice** is the details of processing provided in the contract (eg a privacy policy), and the '**choice**' is if the user accepts or declines these terms by accepting (eg ticking a box). We now consider in more detail why the notice and choice model can be problematic in the context of PbD for the IoT.

Under EU DP law, the processing of personal data needs a legal basis. Ordinarily this is satisfied by obtaining the **data subject's unambiguous consent**. Importantly, consent is not the only grounds for legally processing personal data, and others exist[137] e.g. where necessary for the **legitimate interests** of the processer, as balanced against the subject's rights.[138] The type of consent required differs depending on if personal data (PD) or sensitive personal data (SPD) is being processed.

With **personal data**, the current DPD states consent needs to be a "*freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal*

[137] Art 7 DPD
[138] Recital 30 DPD

data relating to him being processed"(DPD, 1995, Article 2(h)).[139] As we can see, key features of general consent are:

- that it is freely given (i.e. not through coercion),
- specific (i.e. for understandable, defined purposes),
- informed (i.e. subjects are told why), and
- unambiguous (i.e. it is clearly provided).

Many of these terms are open to interpretation, and Article 29 Working Party (2011b) has clarified different elements. The **informed** requirement, for example, needs clearly visible and accessible, jargon free, easily understandable information to be directly provided to subjects before the point of consent (p19-20). [140] Similarly, the **unambiguous** element needs "*the indication by which the data subject signifies his agreement must leave no room for ambiguity regarding his/her intent*" (p24). Use of **express actions** that individuals carry out, or can be inferred to have carried out, and ways to verify consent are encouraged (p24).[141]

At the UK level, consent is not defined separately in the UK Data Protection Act 1998. The UK Information Commissioner Office flags that consent needs active communication between parties but not necessarily in writing; that consent does not last forever; and that it should be tailored to context e.g. age, capacity and particular circumstances. [142]

With **sensitive personal data**, consent also needs to be **explicit,** but again this is not defined in the current DPD. The Article 29 Working Party (2011b) note that explicit consent is similar to normal consent eg "*all situations where individuals are presented with a proposal to agree or disagree to a particular use or disclosure of their personal information and they respond actively to the question, orally or in writing*" (p25). However, they stress the evidentiary value, but not necessity, of obtaining such consent in writing (p25). This is open to online means too, like digital signatures, confirmation emails or clickable buttons (p26). For both type of consent, the A29 WP argues

[139] Article 2(h) DPD; Art 7 DPD – Unambiguous consent
[140] Opinion 15/2011 p19-20
[141] A29 WP Opinion 15/2011 p24
[142] https://ico.org.uk/for-organisations/guide-to-data-protection/conditions-for-processing/

how an indication or agreement is made is not limited to just writing, but *any* indication of wishes i.e. "*it could include a handwritten signature affixed at the bottom of a paper form, but also oral statements to signify agreement, or a behaviour from which consent can be reasonably concluded*" (p11). Passive behaviour is not enough, and action is necessary (p11).

As the nature of **consent giving** is not tightly prescribed in law, it opens up possibilities for designers, as regulators, to design different mechanisms and actions into the technology to signify consent. With physically embedded technology like those in the Works with Nest infrastructure, this could mean prompting users to respond to lights, video or sounds by gestures eg waving at a flashing light and obtaining verification of agreement for explicit consent.[143] We return to these points below.

Overall, new approaches are necessary because the existing model of notice and choice for consent are problematic for end users for a number of reasons, especially for the IoT where interactions may be ambient, pervasive and longitudinal. As Edwards (2016) has argued "…*even if methods can be found for giving some kind of notice/information, the consents obtained in the IoT are almost always going to be illusory or at best low-quality in terms of the EU legal demand for freely given, specific and informed consent.*" (p32). The underpinning challenges for notice and choice are as follows.

Firstly, the **terms of these contracts often provide terms that are not favourable to end users**, from arbitration clauses to handing over a first born child or soul to the service provider (Fox-Brewster, 2014; Caddy, 2013). Consumers are unlikely to read these contracts in any case, hence they do not know what they are signing up to when using a service (Smithers, 2011; Bakos et al, 2014). Broadly, individuals are not informed about the nature of processing, and thus the idea that they have provided **informed** consent becomes a legal fiction.

Secondly, the **nature of these contracts is dense, illegible, lengthy legalese, hence even if they did read them, it is likely they would be incomprehensible**

[143] http://www.cnet.com/uk/news/nest-protect-smoke-detector-gets-an-upgrade-still-no-gesture-control/

to the majority of users. Luger et al (2013) browser plug in Literatin showed that to understand many of the most popular Ts&Cs requires higher levels of literacy than large proportions of the UK population have. Contracts of services like Paypal are longer than Hamlet (Parris, 2012), hence reading contracts also takes a lot of time. McDonald & Cranor estimate it would take US citizens an average of 201 hours annually to read all privacy policies they are meant to (2008).

Lastly, as contracts are effectively 'shopping lists' for what data controllers want to collect, **even if users could read and understand them, these are form contracts and as such are non-negotiable**. For consumers the choice is either to accept these terms or to abstain from using the service. Neither are optimal and challenge the utility of notice and consent as currently framed.

Accordingly, many aspire to creating alternative legal mechanisms to consent as regulatory challenges posed by technologies like big data or IoT grow. Different mechanisms for protecting the values it encapsulates, like choice, control and autonomy are necessary. Luger and Rodden (2013) argue consent should be seen as a social process, not a one-time act. Greater communication and a stronger relationship between different parties is necessary to avoid the 'severance' model between data and user we currently see. Others argue from moving away from consent and notice and choice, such as Tene and Polonetsky (2013) who advocate regulating data use instead of collection. This perspective is controversial, and on one hand Rosner (2016) has stated "*use regulation is an attractive, flawed, contentious proposal, and ultimately a valuable discussion*" (p32) whereas Edwards (2016) is more sceptical stating "*[use regulation] could be the kind of loophole, well meant or otherwise, which might actually spell the final death of data protection*." (p34).

We agree with Edwards (2016) that use regulation is not the answer, and consent as an institution of collection regulation is valuable. The challenges are not insurmountable, it is an established concept and despite pleas for a replacement, no viable alternatives have the same level of traction.

Indeed, consent remains a key legal tenet in the new GDPR, hence, how legal consent mechanisms are designed for the IoT era needs improvement. Within the

new law, there is a broadening of special categories of personal data (sensitive) to include new classes of information like biometric and genetic data (Article 9(1), GDPR, 2016),[144] which may impact new IoT devices such as wearable, quantified self-technologies or those interfaces and experiences using physiological data to detect emotion through biometrics (McStay, 2015). For such data, when consent is the grounds for legal processing,[145] it has to be **explicit,** although, again, what that means in practice is not defined. For general consent (Article 4(11), GDPR, 2016) the requirements are similar to the current DPD law:

"*Consent should be given by a clear affirmative act establishing a* ***freely given, specific, informed and unambiguous indication*** *of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement.*

This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data.

Silence, pre-ticked boxes or inactivity should not therefore constitute consent...."
(Recital 32, GDPR, 2016)

In the GDPR, again consent should be provable, individuals have a right of withdrawal, and where consent is part of a bigger contract, transparency is to be increased as it should be flagged and clearly written in plain language. (Article 7, GDPR, 2016). **Furthermore, consent goes beyond just personal data, to other information too**. Article 5(3) of the Privacy and Electronic Communications Directive 2002, requires users to be provided with clear and comprehensive information about information processing and for them to provide their consent to information being stored or accessed on their terminal equipment (Kosta, 2013). This has been used extensively around browser tracking activity on the web using cookies (Gomer et al, 2013). However, the provision may also apply to data from

[144] Article 9(1) GDPR
[145] Other grounds for legal processing exist – see Article 9(2)(b)-(j)

IoT devices (Edwards, 2016),[146] and go beyond cookies to new tracking techniques like 'device fingerprinting' (Acar, 2014), i.e. where fingerprints are sets of information that identify devices or applications (Cooper et al, 2013) where information can " *single out, link or infer a user, user agent or device over time*"(A29 WP, 2014b, p4).[147] In the web browser domain this largely relates to browser configurations, formatting, header or plugin information(A29 WP, 2014b, p5),[148] but importantly, for our purposes, the A29 WP (2014b) recently stated the law goes beyond web based systems to cover fingerprinting in the IoT too[149], i.e. for a "*broad range of Internet connected devices, consumer electronics and applications, including those running on mobile devices, smart TVs, gaming consoles, e-book readers, internet radio, in-car systems or smart meters*"(p3).[150] This is important for ethical conduct of designers doing iPbD, where the legal obligation for iPbD may not extend to non-personal data, but ethically, and under a different legal framework, the information still requires protection through consent mechanisms.

Clearly, a solution that reformulates notice and choice and consent to increase user control over both personal data and information processing is needed. We argue that designers as regulators have the tools to do this, and we propose redesigning consent mechanisms using the 'trajectories framework'.

[146] Recital 56 PECD – connected to public internet (eg in the home); See discussion about terminal equipment and public internet in Edwards (2016) p18-20
[147] Opinion 9/2014 p4
[148] Opinion 9/2014 p5
[149] A29 WP (2014b) - they recommend OS and device manufacturers should prevent location tracking by limiting see s6.1 - "*device fingerprinting by disabling wireless interfaces when they are not used or should use random identifiers such as a random MAC Addresses to scan wifi networks, to prevent a persistent identifier from being used for location tracking*"
[150] p3; See also, p6 – where they discuss that such fingerprints can also be deemed personal data where two non-unique pieces of information are brought together to create something sufficiently unique to identify the device or application. Consequently, in addition to Article 5(3) protections, rules in the Data Protection Directive will also become relevant e.g. subject access rights etc.

Contractual Trajectories

Benford et al's (2009) **trajectories framework**[151] can help structure thinking about how consent mechanisms are built into user experiences with technologies, especially IoT. Trajectories have significant traction within the HCI community, and are used to design interactive user experiences, often in performative and cultural settings e.g. an interactive performance in a theatre, art installation or a mixed reality game taking place across an entire city involving remote and physical players. Importantly, by focusing on designing **experiences** with technology it involves looking beyond just the usability of a technology, instead considering "*affect, sensation, pleasure, aesthetics and fun, and their contribution to the idea of there being an overall user experience*" (Benford et al, 2009, p709). The process of designing the trajectory of a user experience involves considering the factors like, **the temporal nature, the actors involved, the physical space itself, and the computer interfaces.** The interactions and transitions between these factors are key points of reflection for designers shaping the end user experience. A challenge is the difference between what the designers intend users to do during the experience, the so called *canonical trajectory*, and what the users actually do, the *participant trajectory*. Work goes into managing these multiple trajectories (as there may be multiple users involved in the experience), as Benford et al (2009) describe "*there is a fundamental tension between an author's ideal trajectory that is designed into an experience and a participant's actual trajectory, with orchestration being required to resolve the two, enabling participants to temporarily diverge from and reconverge with the pre-established path*" (p715).

We argue for reframing trajectories for designing user experiences with technology but factoring in how their rights manifest in these experiences. How is control over personal data managed in the experience and how can legal consent mechanisms be redesigned over the lifetime of the interactions with the technology, not just when it is unboxed or installed.

As trajectories have an established lineage within HCI they are useful because they can engage designers with law on their own terms, thinking about consent

[151] See Trajectories resources at https://stevebenford.wordpress.com/themes-and-key-papers/trajectories/

mechanisms so designers can integrate responses and approaches into the end user experience. Work still needs to be done to communicate legal requirements around what proper legal consent requires to designers, but working within the trajectories framework provides a forum for designers as regulators to respond to user concerns over control of data, and DP law compliance, in a pragmatic manner. We now take key elements of the trajectories framework, **Time; Actors; Space and Interface**, in turn, and map them onto designing consent process for a smart thermostat. Importantly, consent is just one example, we could equally use this tool for thinking about implementing data portability over the life cycle of a system, or implementing the right to be forgotten.

- Time – with a smart thermostat, as with many domestic IoT systems, the relationship between user and system is not transient, but long term as these technologies are embedded into the home. Accordingly, designers and lawyers can think longitudinally, changing how tailored information is provided over the lifetime of the product, as opposed to presenting it all at once, as is the model with form contracts. Asking for renewed consent, at appropriate time intervals, may require reflection on important time markers in the experience of users with the system, eg when quarterly or even monthly bills from are issued energy supplier. A shift away from consent at the point of unboxing the hardware, as is the case with shrink-wrap contracts, and mapping the information about and provision of consent over a long period will be beneficial.

- Actors – the goal of domestic IoT is not for all devices to sit in isolation, but to speak to each other, working together to provide value added services. Manufacturer provided platforms like Works with Nest, link together multiple stakeholders via products and services from different manufacturers. There may be varied interests in the personal data from actors across domestic IoT ecosystems. Accordingly, thinking about the range of third party data flows and factoring these into the design of end user experience, with explicit reference to end user legal rights, may foster more transparency for end users. Furthermore, the home is a social space, where visitors like distant family members, family friends, trades people

may come and go. Thinking about their experience with the system, which may be more transitory, is important, as their legal rights are equally important. The design of mechanisms to inform, obtain and allow withdrawal of consent will require creative thought from both lawyers and designers.

- Space – As we highlighted above, the home is a complex, often contested social space. There may be domestic politics, for example, around how heating is managed in the home hence designers may need to think about managing domestic tensions. Reflecting on how legal interests, for example around control of data exists within spaces with domestic hierarchies adds another layer of complexity e.g. between teenagers and parents, or older relatives. Many IoT technologies seek to understand their context and environment, in order to tailor their service, for example the Nest Thermostat builds up a profile of occupancy of rooms based on motion detection in order to create a profile to tailor heating to the needs of occupants. Different occupants, especially if it is a shared space, may want extra control over their footprint in the profile, depending on internal domestic tensions or routines hence it is important to consider how consent mechanisms enable withdrawal. Lastly, as mentioned above, the home will not become smart overnight, hence designers and lawyers will need to think about how interactions and consent mechanisms differ across a range of different devices and services.

- Interface – the computer interface can both limit and enable how information is communicated to end users. Different signifiers could be used to interact with users, from beeping noises to flag when the system wants to share data with third parties, flashing lights when wanting to collect new types of data and even speech to advise of new information. Text based approaches may not even be possible due to size of screens and computational limitations of the system, such as balancing function, aesthetics and cost. The interface may also afford different means of signifying consent from gestures like waving and pointing and providing feedback to users to notify them their consent is logged. Collaboration

between designers and lawyers could lead to more innovative and rewarding approaches for communicating with end users around consent through the interface.

As we see, by thinking of user experiences with technologies in terms of trajectories, we can start to unpack how they intersect with legal considerations, like consent, and think of new ways for tackling regulatory challenges, such as the legal fiction of informed consent from form contracts. This is one of the ways designers as regulators can do PbD and realise user centric regulation in practice. We now turn to our second case study which looks at how access to data is regulated in the government led smart metering programme, and how designers can build in safeguards in this context.

Chapter 6. User Centric Regulation in Practice II: The Case of Privacy by Design and Smart Metering

Within this section, we follow the approach of chapter 5, but within a new context and focusing on controlling **access** to personal data. We analyse the social and technical nature of smart metering, the policy and regulatory context, particularly data protection law challenges. We look at user perspectives, and within our case study diagrams we ask: how is **access** to consumption data regulated in the UK smart meter ecosystem? Again we conclude by discussing how designers may respond to the regulatory challenges to ensure users have sufficient control over access to data.

This requires analysing how the role of designers in providing control to users differs for a government led context, where there is a more systematic, comprehensive approach to addressing privacy risks. The role of designers therein is more closely prescribed, but nevertheless, there are still gaps in the regulatory framework where designers can respond. So, whilst restructuring how consent mechanisms are designed is one approach, as we saw in chapter 5, designers can also increase user control over access by using personal data vaults and increasing transparency around access using provenance tools. For now, we begin by unpacking what smart metering is and how the programme has been developing in the UK.

Smart Metering

Smart meters are '*electronic systems that can measure energy, consumption, providing more information than a conventional meter, and can transmit and receive data using a form of electronic communication*' (European Commission, 2015, p3).[152] As mentioned earlier, smart meters are backed by a strong legislative mandate, supported by extensive policies and government strategies. We focus on the UK Smart Meter Implementation Programme (SMIP) here run by the (former) Department of Energy and Climate Change (DECC), now BEIS,[153] with an installation target of 53 million gas and electricity smart meters across the UK by 2020. It is part of the wider EU shifts,

[152] from Article 2 Energy Efficiency Directive (2012/27/EU)
[153] Department for Business Energy and Industrial Strategy

namely the EU Third Energy Package[154] and specifically, Directive 2009/72/EC which requires 80% of Europe to be using smart meters by 2020. This means around 200 million electricity smart meters (72% of all European consumers) and 45 million gas meters (European Commission, 2014).

SMIP has been delayed extensively (DECC, 2015), partly attributed to lack of installation engineers, and lack of engagement with vulnerable populations, early meters not working with networking infrastructure and meters not working properly in shared or tall buildings (House of Commons, 2015). Other issues include, the negative impact of meters on low income and vulnerable populations; over reliance on the market to control costs/deliver benefits may lead to poor consumer protection; being too costly and lacking transparency[155] to consumers on costs and benefits (Public Accounts Committee, 2014). Nevertheless, by 31 March 2016, official UK statistics show there are 2.75 million smart meters across UK operating in smart mode, representing 5.8% of total domestic meters in UK (DECC, 2016).[156]

Smart metering programmes are underpinned by a number of purported benefits for both energy providers[157] and users. For energy *providers*, smart meters provide insight into consumer demand. This allows them to develop more efficient practices for producing and supplying energy.

To explain in a little more detail, when UK electricity consumers are billed, little granular information on consumer demand is provided. Ordinarily, the energy supplier sends an estimate of aggregate monthly energy consumption to the consumer, based on approximations of metered energy use. [158] The consumer has an opportunity to provide the supplier with more accurate readings, and representatives of the supplier periodically visit premises for physical meter readings. Importantly, this consumption information is only really used to ensure

[154] Electricity Directive (2009/72/EC) Annex I.2
[155] eg not publishing the assessment by the Major Projects Authority publicly – see MPA website https://www.gov.uk/government/groups/major-projects-authority
[156] Meters operated by big energy firms eg British Gas, SSE, E.On etc
[157] i.e. Energy Generation, Transmission, Distribution and Supply
[158] Prepayment systems and tiered off peak tariffing structures already exist too e.g. Economy 7 in UK http://www.uswitch.com/gas-electricity/guides/economy-7/ accessed 15 Sept 2015

accurate billing, and the level of knowledge suppliers have on their consumers' everyday energy consumption is limited.

With smart meters, the picture changes. Digital energy consumption data is relayed from consumers' homes to energy suppliers with much greater frequency and granularity of detail. This has many benefits for suppliers, for example, any missed readings can be a sign of network failure and help pinpoint the source of the problem more quickly (Goater, 2014).

More broadly though, smart meters are a key component for realisation of the smart grid i.e. "*an upgraded energy network to which two-way digital communication between the supplier and consumer, smart metering and monitoring and control systems have been added*".[159] The grid aims to create more efficient energy production by industry, smarter consumption by citizens and works towards domestic, regional and international CO2 emission reduction targets.[160] Levelling off inefficient peaks in consumer demand is a goal of the grid. This relies on more than just understanding consumer behaviours, it needs tools to change them. Pricing is one mechanism, and consumers could be incentivised to change habits through time of use (TOU) tariffs i.e. where electricity pricing changes at different times of the day (Goater, 2014, p3).[161] Future visions, predict greater automation of load management in the home. Namely, real time dynamic pricing structures will emerge i.e. prices from suppliers change many times a second (Constanza et al, 2014). The complexity of these would be too much for consumers, and accordingly artificial software agents may help them manage this (Rodden et al, 2013).

For the consumer, the benefits are less clear. Given the huge cost of the SMIP, financial benefits are meagre. Official figures suggest smart electricity meters cost around £215 and consumers will save 2% on average bills, around £26 a year (Public Accounts Committee, 2014). Financial benefits vary greatly across EU Member states, where the average cost per electricity meter is €223 (±€143), and the average overall benefit per consumer is €309 (±€170) per meter with annual

[159] Communication 2012/148/EC Section 3(a) Definitions
[160] The UK DECC need to reduce CO2 by 80% by 2050 from 1990 levels, in line with the UK Climate Change Act 2008 and Energy Act 2011
[161] eg cooking between 5 and 8pm or having showers between 6-8am

savings of 3% (±1.3%) (European Commission, 2014). Smart meter support of in home displays (IHDs) may play a role in forecasted cost savings. IHDs provide near real time feedback of energy consumption data from the meters to consumers. Raw and Ross (2011) state changes in user behaviour encouraged by IHDs could reduce consumption between 3-19%.

Beyond costs, the overarching EC European Energy Market strategy stresses the importance of consumer centricity. Providing consumer control over their data, increased information about their energy habits and empowerment to change tariffs as they see fit are key to this. Ensuring the technology 'works for them', as opposed to energy suppliers, and protection from unfair commercial practices are important too (European Commission, 2015). Smart meters fit into this agenda, aiming to provide more general control and information, giving consumers access to real time energy use information and a better understanding of their energy consumption practices, ending the practice of estimated bills and enabling them, in theory, to switch more easily between suppliers (Goater, 2014; DECC, 2015).[162]

Regulatory Challenges of Smart Metering

Despite these purported benefits, smart meters pose many regulatory issues. Highest on the agenda is data protection and privacy challenges, with profiling, controlling third party access to data, and protecting storage of personal data being three key issues. We break them down a range of them in the table below:

Table 5 Data Protection and Privacy Challenges of Smart Metering

Issue	Details
Profiling	**Profiling** of consumers from their consumption data is a risk, due to the frequency of energy data readings (European Commission, 2014, p7). The European Data Protection Supervisor argues meter data can provide a detailed picture of daily life meters enabling spotting of **patterns** of behaviour or routines. For them, inferences and predictions from electricity usage can be made about "…*when members of a household are away on holiday or at work, when they*

[162] 37% of UK energy bills are based on estimates that may be inaccurate - Goater (2014); Directive 2009/72/EC see Recital 50 "…*consumers should have access to their consumption data and associated prices and services costs so that they can invite competitors to make an offer based on those data. Consumers should also have the right to be properly informed about their energy consumption. Prepayments should reflect the likely consumption of electricity and different payment systems should be non-discriminatory. Information on energy costs provided to consumers frequently enough will create incentives for energy savings because it will give consumers direct feed back on the effects of investment in energy efficiency and change of behaviour.*"

	sleep and awake, whether they watch television or use certain tools or devices, or entertain guests in their free-time, how often they do their laundry…". (Buttarelli, 2012, para 19)
Lack of user understanding	Consumers need to **be informed about how smart meters' work**, what data is being collected and the risks around this. As Cuijpers and Jaap Koops (2013) warn, without doing this, "…*our home will no longer be our castle, the house may be energy efficient but it will be a cold place to live*"(s5).
Controlling Access	**Controlling access to and protection of** stored energy consumption data is another concern (European Commission, 2014, p7). Such data can be useful to third parties like "*law enforcement agencies, tax authorities, insurance companies, landlords, employers*" and of course marketers/advertisers to name a few, but would foreseeably negatively impact occupants (Buttarelli, 2012, para 19). Third party **access** was raised as part of the UK SMIP Privacy Impact Assessment, alongside concerns around granularity of data, and transparency to consumers about data collection/use (DECC, 2012).
Home Security	The ease of **monitoring building occupancy** through observing energy loads on smart meters is a technical concern eg to spot when the home is empty for burglaries (Kleiminger et al, 2015).
Personal Data	Information from smart meters is ordinarily **personal data**, and handling it is regulated by data protection law (Article 29 Working Party, 2011). As the EU Article 29 Working Party (2011) states, information like a smart meter ID, meter configuration metadata, or energy load graphs are personal data because, for example, when data is linked to a customer's registration details, the device can single them out from other customers.
Beyond Personal Data	Looking **beyond personal data** is also important. In the UK, case law has, incorrectly, narrowed the definition of 'personal data'.[163] This prevents some information benefiting from data protection safeguards, as DP law only applies to 'personal data'. More broadly, Savirimuthu (2013) has criticised the focus on DP law compliance in the SMIP, as it misses the importance of privacy as a fundamental right i.e "*unlike Directive 95/46/EC, the scope of Article 8 ECHR covers all activities regarded as constituting private and family life…it extends for example, beyond the biographical information of a data subject and provides an extra layer of safeguards for physical, personal and psychological development, namely gender, religious and political beliefs, sexual choices and identity*" (p173)

Beyond these privacy and data protection risks, how large scale smart meter programmes are implemented across Europe has varied (Cuijpers and Jaap Koops, 2013; Brown, 2013; Savirimuthu, 2013). In general, the dominant EU implementation model is industry led. Energy firms install and own the meters and handle processing of energy consumption data. [164] Importantly, despite this

[163] Durant v Financial Services Authority [2003] EWCA Civ 1746– where the definition of personal data was constrained to data where there was focus on the individual or data was biographical. In 2014 Edem v The Information Commissioner [2014] EWCA Civ 92 limited the scope of Durant. See Pounder (2014)

[164] Distribution System Operators (DSOs)

freedom, high level common functional requirements of smart meters have been defined for meters across the EU (European Commission, 2011). Meters should give local readings to the consumer and other installed equipment (eg IHDs or mobile devices) at least every 15 minutes; provide fraud and data breach detection; and ensure secure communications between all actors (p9).

Importantly, the UK (alongside Denmark, Estonia and Poland) have adopted a less industry led model where **a central data hub (established by the state) handles third party access to data**. In the UK, it is the **Data Communications Company** (DCC), which we discuss later.[165] Again there has been **criticism of the UK approach**. A 2015 UK House of Commons Report holds the DCC responsible for likely missing 2020 EU meter installation targets. Infrastructural challenges of integrating older smart meters and the length and complexity of their 900 page Smart Energy Code, which governs access to data, are just two examples of why it will be missed (House of Commons, 2015, p11-12). Having unpacked the regulatory context of smart metering across Europe, we now turn to the impacts of living with smart meters.

[165] Czech Republic, Germany and Slovakia have not confirmed their approach, and may follow a similar model.

User Experiences of Smart Metering

As with IoT in Chapter 4, we consider studies user responses to smart metering and, where possible, field studies of actual home use in the UK.

As Parkhill et al (2013) show, public acceptance of changes in the energy system is shaped by concerns around environmental protection, minimising wastefulness, supply reliability, social justice and respect for user autonomy (p23-30).[166] Participants are largely willing to share data, but they want to know "*who the data is shared with, their motives, what data is used for and who it stands to benefit*" (p16). People are more likely to share with energy firms than government, but broadly energy firms are deeply distrusted (p16).

Indeed, users ideally want to preserve control over their home energy use in any demand side management (DSM) setup. As one participant stated "*the point of government isn't to control, it's to guide. The day someone sitting in Parliament decides when you can do your washing is the day I reckon we should probably leave. Even if it is the best for everybody*" (p16). Similarly, external control over energy use in the home e.g. by remotely controlling when people can shower or through automation systems,[167] was perceived negatively (p29).

Spence et al (2015) work on adoption of demand side management (like smart metering) found consumers[168], particularly those who were financially vulnerable, would be 'uncomfortable' with sharing energy use data, and they would need more control and autonomy to become comfortable (p553). Similarly, Goulden et al (2014)[169] argue that advocating DSM on financial benefits is not enough for consumers, especially those in complex **social** circumstances (p23) (eg living in shared housing - Leygue et al, 2014).[170]

[166] Parkhill et al (2013) document public attitudes to energy supply, use and governance in the UK drawing on various stakeholder interviews; large survey and deliberative workshops across UK
[167] Automation for switching off products is seen in more favourable light.
[168] 2,441 participants
[169] A study with focus groups of 72 participants in UK.
[170] Leygue et al (2014) p 8

This raises interesting questions about acceptance of smart metering by those at risk of fuel poverty. Importantly, Goater and Casey (2015) estimated between 2003 and 2013, fuel poverty across all households across the UK grew from 7% to 17% (where fuel poverty is 10% of income being spent on fuel). From a public policy perspective, it is important to ensure smart energy management does not negatively affect poorer consumers.[171] Goulden et al (2013) also found **distrust in energy firms and uncovered concerns at who owns smart infrastructure**. If it can monitor and centrally control energy consumption, participants worry DSM may impact their ability to live their daily lives, and more broadly exercise their **autonomy** (p26).

These concerns carry forward to future visions of the **smart grid** too, as mentioned above, the complexity of dynamic tariffing may necessitate software agents to manage tariff switching on behalf of consumers (Rogers et al, 2012). In this regard, Rodden et al (2013) found UK consumers concerns about privacy, trust and control with such agents. Distrust of energy firms drives apprehensions about agent ownership, user control, in whose interests it acts (energy firm or user), if data is shared with third parties, and to what extent the agent disrupts established routines and energy use patterns.[172] As a design response, Rodden et al (2013) suggest agents be designed to reflect who owns the system, what they can do (especially with data); provide energy data openly; design agents so they are accountable (i.e. agents show why decisions are made a certain way) and enable ongoing consent relationship (where users can withdraw at any time).

Clearly, there are a range of elements that emerge from living with smart energy management, now and in the future. Designers, as regulators, can respond accordingly. We conclude by mapping some of the challenges smart metering systems pose for users in table 6.

[171] See CHARIOT Project looking at the interface of IoT, fuel poverty charity advisors and designers https://www.cse.org.uk/projects/view/1277; For a similar US perspective see Dillahunt (2009)

[172] See Constanza et al (2014) for a study of agents for washing machines and how these fit with social practices of washing

Table 6 User Concerns with Smart Metering

1)	**Control** over **access** to smart meter data is a big concern. Consumers are worried about energy data **accessed** by third parties. The **sharing** of data, and who collects it, why, when, and for how long are all key issues. This is particularly pronounced for **vulnerable people.**
2)	There is **distrust** in energy firms as institutions. Consumers are worried about who owns the infrastructure, and how control might affect their **autonomy.** Building trust relationships is an important response
3)	The detailed patterns of everyday activity that can be deduced from energy data raise fears about **profiling.**

We could look at any of these issues, like profiling or distrust, but we continue to focus on concerns around control, hence we look at how to increase user control over access to consumption data. To frame our discussion, we turn to the question of **how is access to consumption data regulated in the UK smart meter ecosystem?** Below is figure 5 documenting the flows of consumption data between different actors in the UK smart meter ecosystem. We explain the data flows before analysing how **access** to consumption data is regulated.

In figure 5 **<Home Occupants>** consume energy in the home by using devices like washing machines, televisions or boilers. Their energy consumption data is logged by the **<Smart Metering Infrastructure>**, where the smart meter logs consumption data, and shares it with the in home display, feeding it back to the **<Home Occupants>**. The **<Data Communications Company>** provides infrastructure and controls access to the consumption data for other actors. Various actors can apply to the DCC to access this data, including **<Energy Suppliers>, <Third Party Business>, <Energy Distribution Network Operators>**and **<Law Enforcement Agency>.** The **<Data Communications Company> Smart Energy Code** and **DECC SMIP Data Access and Privacy Code** prescribes how they can access data. Access to the data is via the home area network using the communications and data infrastructure that is provided by outsourced services (eg Telefonica and BT). The **<Energy Transmission Network>** cannot access the data. Data protection law still applies underneath these rules.

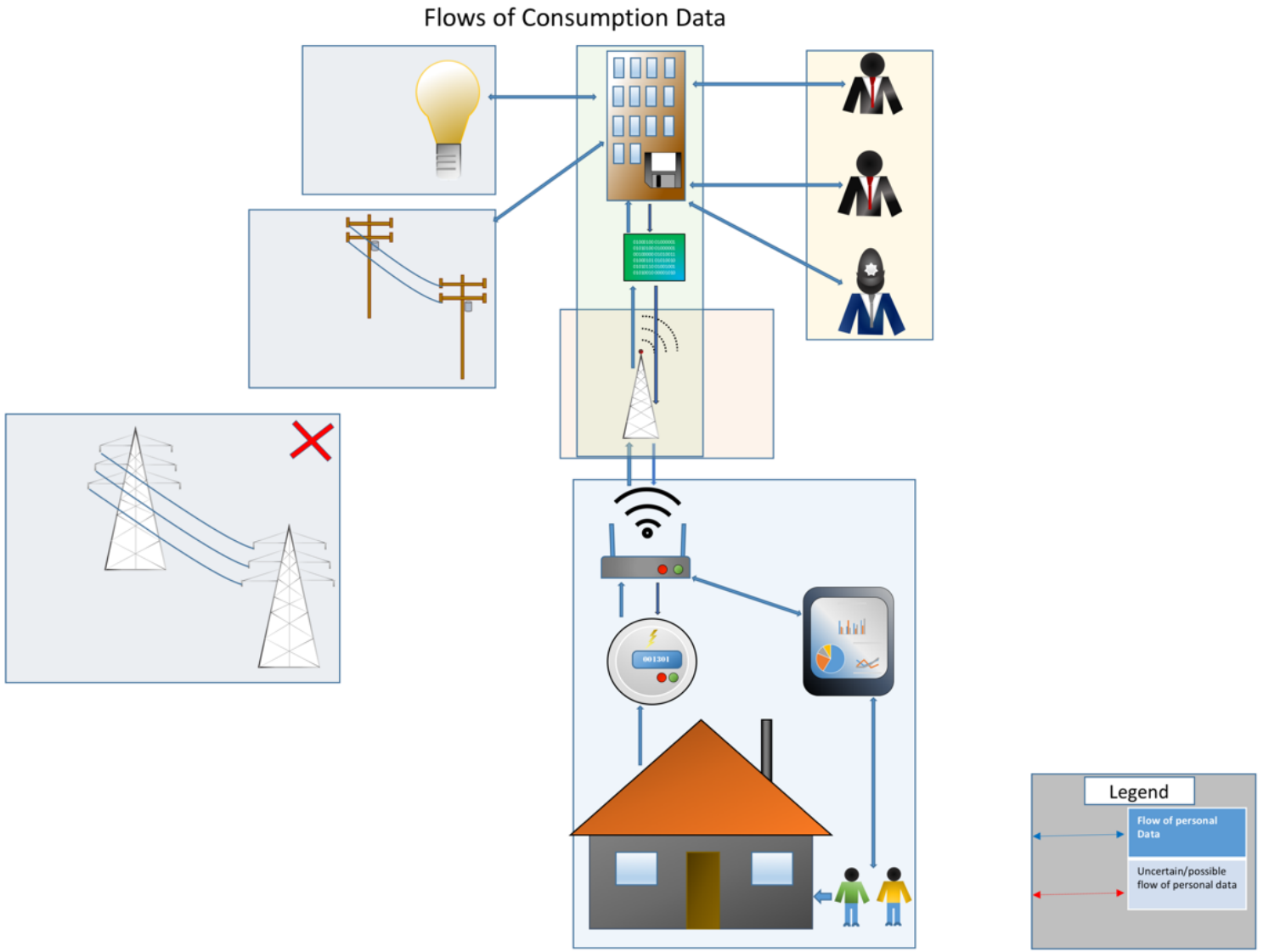


Figure 5 Flows of Consumption Data in Smart Metering

As this description highlights, the DCC are a key gatekeeper in controlling access to consumption data, so we look at their role in a bit more detail below.

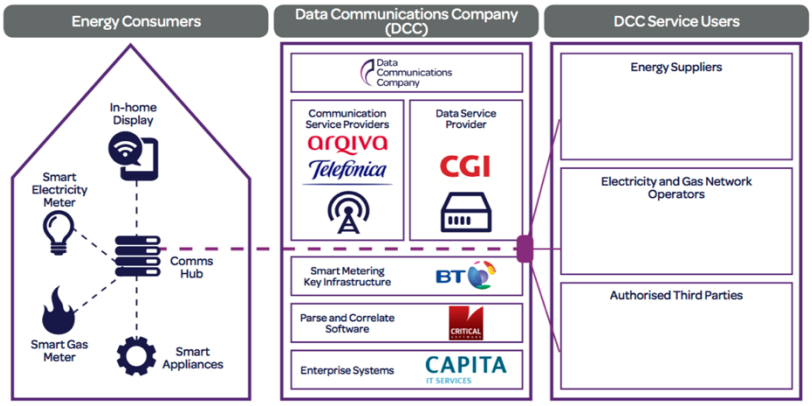


Figure 6 Structure of the UK Data Communications Company

In the UK, access to smart meter consumption data is handled by the Data Communications Company, see figure 6 (DCC, 2015; Beard, 2014). [173] The DCC should "*provide communication services between smart meters and the business systems of energy suppliers, network operators and other authorised service users*".[174] The wireless network enables data from the home to be shared via the DCC with suppliers, electricity network operators and third parties (Goater, 2014, p2). The UK energy regulator Ofgem [175] oversees the DCC, and enforces the so-called Smart Energy Code (SEC, 2015)[176] that governs DCC activities. Ofgem have investigative powers to address harm to consumers (Ofgem, 2014)[177] particularly enforcing consumer protection legislation and challenging unfair contract terms.

In addition to the DCC and its governing SEC (2015), the **2012 UK Data Access and Privacy Framework** (DAPF, 2012; DECC, 2014)[178] regulates **access** to

[173] Note the diagram suggests IoT devices may access smart meter data via the HAN)
[174] Data Communications Company Website "About Us" Accessed 15 Sept 2015 (all links in this Part checked for this data) at https://www.smartdcc.co.uk/about-dcc/ ;
[175] Ofgem Website Document Hub – see Transition to Smart Meters at https://www.ofgem.gov.uk/electricity/retail-market/metering/transition-smart-meters
[176] Smart Energy Code Company Website at https://www.smartenergycodecompany.co.uk/
[177] Under the UK Enterprise Act 2002 part 8 or UK Unfair Terms in Consumer Contracts Regulations 1999
[178] See Ofgem (2015) p5 and p12 where it discusses DAPF (2012) applies to both full smart meters, and remote access meters that can 'remotely send consumption data to the supplier' to give those consumers more control over data (p5); remote access meters are declining in use (p12)

consumption data by different actors.[179] DAPF (2012) is additional guidance to European DP law and it is not a replacement (para 1.23-1.24). Compliance with DP law by parties handling consumption data is important because suppliers, network operators and third parties will all 'likely' be data controllers and the DCC is a data processor (DAPF, 2012, para 1.19-1.21).

Having outlined the relevant regulatory tools, we now turn to the different actors in the energy grid, and how these regulatory tools are applied to control access to consumers' consumption data. To understand the range of actors, it helps to think about ownership of infrastructure in UK energy supply chain, as figure 7 shows.

Ownership of the infrastructure is quite separate. In the UK the **<Energy Supplier>,** likely to be one of the "Big Six"[180], owns the **<Smart Metering Infrastructure>** i.e. smart meters, in home displays and home area network devices. The energy supply chain of **<Energy Generators>, <Energy Transmission Network>** and **<Energy Distribution Network Operators>** fragmented following the privatisation of the energy market in the UK by the Electricity Act 1989.[181] Whilst the same company may have formerly handled generation, transmission, distribution and supply, the move to a competitive market means the current supply chain is composed of a range of different actors owning different parts of the infrastructure.[182] The **<Data Communications Company>**, is a corporation run by Capita PLC, which oversees a number of outsourced providers of data services (CGI), Communications Service Providers (Telefonica and Arqiva), Public Key Infrastructure (BT). These enable the DCC to operate. **<Third Party Business>** and **<Law Enforcement Agency>** handle their own infrastructure. Interestingly with the **<Home Occupants>,** they have no ownership over **the <Smart Metering Infrastructure>**, which is provided by the **<Energy Supplier>** in the same way as current infrastructure (eg loaned and paid

[179] DAPF (2012) para 3.40 - it does not apply to other smart metering data like 'technical data, alerts and alarms'
[180] More Information at uSwitch website "Big Six Energy Suppliers Guide" https://www.uswitch.com/gas-electricity/guides/big-six-energy-suppliers-guide/
[181] Legislation available at http://www.legislation.gov.uk/ukpga/1989/29/contents
[182] More information at Energy UK Website "The Energy Market"-see http://www.energy-uk.org.uk/energy-industry/the-energy-market.html

for by a fee on the bill). [183] The question of ownership of data by **<Home Occupants>** has been considered above.

[183] More information at uSwitch website "Smart Meters Explained" - http://www.uswitch.com/gas-electricity/guides/smart-meters-explained/#step5

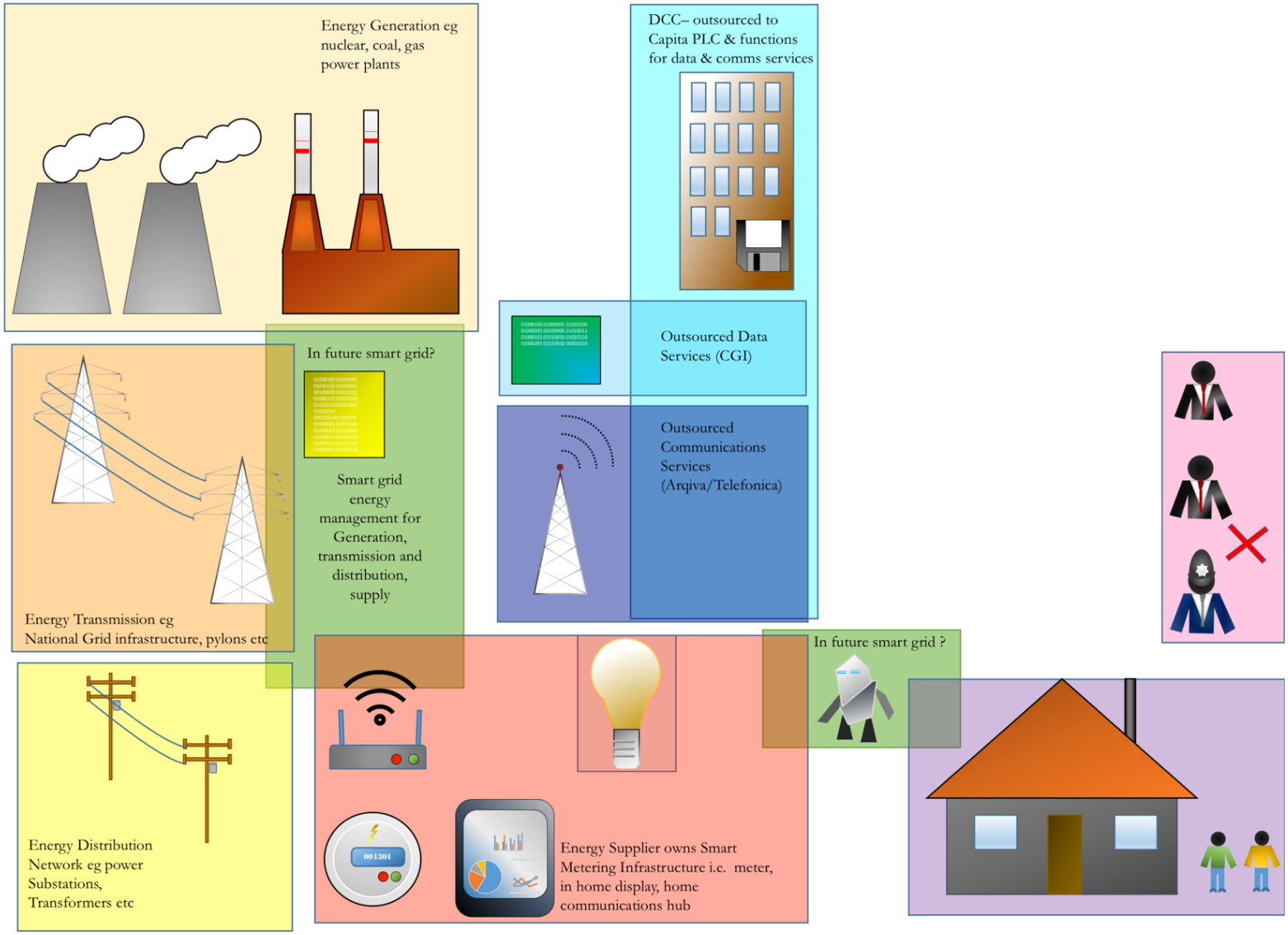


Figure 7 Ownership of Smart Metering Infrastructure

We now focus on access to consumption data for the following actors:

- Consumers
- Energy suppliers (eg EoN, Scottish Power, nPower)
- Data Communications Company (including outsourcing to Telefonica, Capita, Arqiva etc)
- Energy generators (eg Centrica, EDF), distributors (eg Western Power Distribution) and transmission network operators (eg National Grid)
- Commercial third parties (eg advertiser, data analytics service)
- Law enforcement bodies (eg police)

Consumers, access their own consumption data in three main ways (DAPF, 2012, para 2.3-2.12):

i) Through in home displays (IHDs)
ii) By connecting 'consumer access devices' (eg tablets) to the home area network,
iii) By requesting an electronic, machine readable copy from the energy supplier via the midata initiative (we return to this below).

Energy suppliers can access consumption data for a number of different purposes. DAPF governs access to different levels of detail. Granularity, as opposed to frequency, of meter readings is key. The DAPF (2012) states there is a "*difference between the granularity of data that may be collected (i.e. whether the data shows consumption over a half hour, day, week, month etc) and the frequency with which reads may be taken (i.e. whether data is collected once per day, once per week, once per month etc)*" (para 3.42). The nature of readings are provided below:

- Monthly access is allowed for billing purposes and other regulated purposes, like detecting theft, **without** consumer consent. (DAPF, 2012, para 3.36)

- Daily smart meter readings are the **default,** with the user having an option to 'opt out' from these (DECC, 2015b, para 2.4 -2.5).[184] The UK government argues consumers should get advance notice (7 days before data collection) electronically or on paper, about daily meter readings and how to opt out. (DECC, 2015b, para 3.61)

- Explicit 'opt in' consent is required for energy suppliers to collect readings of half hourly consumption (DECC, 2015b, section 2.5).How suppliers obtain consent is not defined, but they need a record showing they did do it, and they recommend incorporating phones, websites, email and tick boxes. (DECC, 2015b, para 3.62)

Enforcement is generally through requirements in an energy suppliers' license. DAPF (2012) looks for suppliers to explain to consumers **why** data is collected, reminding them regularly about what they agreed to (para 3.77-3.80), but **how** they do so is up to them (DAPF, 2012, para 3.55-3.57). Importantly, where consumption data is to be used for marketing i.e. "*information about goods or services, regardless of whether or not those goods or services are free of charge or paid for*", **explicit opt in consent is** needed (DAPF, 2012, para 3.31).

Furthermore, because the **Data Communications Company** is providing public networking[185] they cannot spam consumers with unsolicited messages via the IHD (DAPF, 2012, para 3.35).[186] Whilst these safeguards exist, how they will play out in practice is another matter. **Contracts may remain the primary means of obtaining consent, but as discussed above, these are not the ideal mechanism for ensuring consumers are adequately informed of their rights.** With the 'trajectories framework' (Benford et al, 2009) the user interaction with smart meters may be designed in more compliant ways.

[184] DECC (2015b) is a consultation on review of DAPF (2012) and contains useful additional detail. DAPF (2012) will undergo a full review by 2018.
[185] Legally speaking they are a 'public electronic communications network' within scope of Communications Act 2003
[186] "consumers would be afforded protections against unsolicited marketing messages via an In-Home Display"

Energy Distribution Network providers[187] can access consumption data with consent. up to half hourly (DAPF, 2012, para 4.19) for network development or maintenance on certain conditions (DAPF, 2012, para 4.1). They need to ensure data is aggregated, and cannot identify specific homes. They need an Ofgem approved data aggregation plan, that includes a privacy impact assessment, their anonymisation and aggregation approach, and data management setup(DAPF, 2012, para 4.14-4.17). In the future, if privacy concerns are addressed, they may get access to more data about individual homes, for smart grid goals like peak levelling (DAPF, 2012, para 4.18). This aligns with goals of privacy by design, where safeguards, either technical or organisational are built into the system.

Interestingly, the **energy transmission network** (i.e. the UK National Grid) requested similar access, but were not granted this as they could not convince Ofgem they needed it (DAPF, 2012, para 4.21). Similarly, **energy generators** do not have access currently.

Commercial third parties, like advertisers or data analytics firms, are regulated by the convoluted and lengthy **Smart Energy Code (SEC, 2015)** we introduced above. This inaccessible document, drafted in esoteric language seeks to regulate data flows between the consumer, Data Communications Company, the energy suppliers and third parties.[188] Its length and complexity has been cited as causing delays in the overall SMIP (House of Lords, 2015, p11-12). It requires third parties to have 'appropriate permission' to access consumption data, i.e. provision of explicit consent from consumer to third party. [189] The form of this explicit consent is not specified. Third parties need to periodically notify consumers about how long data is collected for, the purposes of collection, and inform them of their rights

[187] eg Western Power Distribution, Scottish Power Energy Networks
[188] Newest version (SEC 4.4) released on 14 Sept 2015: analysis based on this code
[189] We provide the definition of 'Appropriate Permission' from SEC (2015) Section A1.1 – Definitions. It means
"*in respect of a Communication Service or Local Command Service to be provided to a User in respect of a Smart Metering System at a premises that will result in the User obtaining Consumption Data, either:*
(a) (where that User is the Import Supplier, Export Supplier, Gas Supplier, Electricity Distributor or Gas Transporter for that Smart Metering System) that the User does not need consent to access that Consumption Data in accordance with its Energy Licence, or that the User has consent (whether explicit or implicit) in accordance with the requirements of its Energy Licence; or (b) (where that User is not the Import Supplier, Export Supplier, Gas Supplier, Electricity Distributor or Gas Transporter for that Smart Metering System) that the Energy Consumer has given the User explicit consent to obtain that Consumption Data and such consent has not been withdrawn."

to withdraw consent and object to data processing.[190] If the DCC handles any data requested by a third party they will implement security measures, [191] not process personal data outside the EEA,[192] and provide third parties with assistance in any consumer subject access requests brought under data protection laws.[193] Interestingly, third parties handling consumption data need to conduct separate PIA's to consider their privacy risks, and how to mitigate these (DAPF, 2012, para 1.16).

Law enforcement bodies, like the police or councils detecting fraud, are considered in the DAPF, by reference to access requests under s29 DPA (DAPF, 2012, para 5.37).[194] DAPF advises the DCC and energy suppliers need to have procedures and safeguards in place for requests, before disclosing any data. Accordingly, they need to be satisfied disclosure is **necessary** for the '*purposes of crime prevention or detection, or the apprehension or prosecution of offenders*' (DAPF, 2012, para 5.37). There is also strategy from DECC on government access to data (DECC, 2012b), but primarily for evaluating the success of the SMIP programme eg with statistical analysis (para 4.5-4.7).

Access to consumption data is governed by a complex regulatory framework, where the DCC is a key gatekeeper, and rules differ depending on **who** wants to access the data and **why**. **The rules from DAPF (2012) are clear on issues of access for energy suppliers, transmission and distribution networks, and to an extent, law enforcement**. **Less clear is the picture on third party commercial access, as governed by the SEC (2015)**. The SEC tries to address privacy concerns, but in practice it is so complex that consumer knowledge of their rights and protection is likely to be poor. The lack of specificity on the nature of explicit consent in SEC is also concerning. Similarly, an industry led data charter from Energy UK (2013) outlines consumer rights but it lacks detail for them to take action beyond contacting the Information Commissioner Office or energy supplier for further guidance. Furthermore, given the unusual structure of the DCC where third parties obtain data through them, as opposed to consumers directly, these

[190] SEC Section I1.2(b)(i)-(iii)
[191] SEC Section I1.7(c)
[192] SEC Section I1.7(d)
[193] SEC Section I1.7(e) the UK Data Protection Act 1998
[194] Consumers are not informed of such requests, and lose their subject access rights.

safeguards are critical. To balance this, we need designers to provide users with more control over access, and a turn to underlying DP law to provide additional insight. In particular, the GDPR broadens user rights over their data further, but this is not reflected in the SMIP, DAPF or SEC currently. We look at how designers may be able to incorporate more control over access.

Designer Responses:

Whilst access to data by different actors is more strictly regulated with smart metering, there are still areas where designers can respond to help users exercise more control over who is accessing their consumption data. Designers can increase control by giving consumers the choice over who accesses the data, and keeping logs of who does. We look at two concepts aimed at doing this, provenance and personal data vaults. As a bit more background, clearer organisational and technical safeguards need to be designed into the smart metering ecosystem to enable consumers to control commercial access to their data. As mentioned above, the SEC requires third parties seeking access to data to:

- have **appropriate permission** (explicit consent), but does not define the form this needs to take.

- periodically **notify** consumers about how long data is collected for, the purposes of collection, and inform consumers of their rights to withdraw consent and object to data processing, but again, does not define the form this needs to take.

- conduct separate PIA's to consider their privacy risks, and how to **mitigate** these.

Given this recognition of the need to mitigate privacy risks, and a broader commitment to PbD within the GDPR, we consider a couple of approaches designers could adopt to increase control for end users of smart metering.
The general GDPR provides users rights over their data, like a right to object to processing, to data portability, to increased information around processing. These rights will be complex to implement, but coupled with the lack of clarity around explicit consent mechanisms for access, designers can respond by finding mechanisms to put users in control of data and access, such as personal data vaults,

and tools for tracking provenance of who accesses data. This would address a number of the SEC and PbD requirements around notification or mitigating risk (SEC) or data portability and rights to object by putting control in the hands of end users. Critically, these approaches would need to be implemented in a way that was usable, comprehensible and legible for end users. Indeed, the GDPR advocates PbD measures that increase transparency and monitoring of processing for the data subject (Recital 78, GDPR, 2016). If form contracts are the dominant approach for third parties obtaining explicit consent, the 'trajectories framework' (Benford et al, 2009) could prove useful for redesigning consent mechanisms within access to consumption data too, but for now we focus on provenance and personal data vaults.

Personal data containers,[195] lockers, stores or personal clouds are a useful mechanism for providing users control over their data by storing it in a way that they decide where it is and who can access it (Out-Law, 2014). They are a practical tool that increases control over personal data, whilst avoiding viewing personal data as an owned asset. The voluntary UK midata initiative is not a personal data locker, but instead a scheme to help consumers get easier access to their personal data. It is government led (BIS, 2012) and has industry backing across different sectors eg energy, banking, telecoms. It aims to '*give consumers access to their transaction data in a way that is electronic, portable and safe*' (BIS, 2013, p1), and requires organisations, to provide mobile apps that help consumers, to use their data more effectively, e.g. spotting trends in their consumption habits (Sloan, 2014).

MyDex is a prominent example that provides a lifelong, secure, free, data store for consumers. Users create an encrypted store for all their personal details. When different services or organisations (both public and private sector) require personal details, users choose how, when, why and what to share from their store and a record of sharing is kept.[196] Such a service requires user trust in MyDex, as they are effectively providing an identity authentication service. MyDex does this by using multiple standards accreditations, memberships, a charter, and guarantees that the

[195] Dataware
[196] https://mydex.org/individuals/

user has the only encryption key, and they do not look at the data, to foster trust. [197]

Databox is particularly useful for thinking about the domestic environment, and the Internet of Things. It develops from the principles of Human Data Interaction, discussed above. A databox indexes and stores data from different devices and services to make it more transparent and legible, enabling users to negotiate who accesses it and for what reasons. The goal is "*to selectively and transiently make those data available for specific purposes*" for third parties to access like companies (Chaudhry et al, 2015, p1). A challenge Crabtree and Mortier (2015) highlight with Databox is that data is often not only about one individual, but is relational and shared, and as such management of data needs collaboration, a possible challenge in the contested space of the home. Research project Hub of All Things has a similar goal, creating a data container that collects data from all devices in the home, and allows access through a 'multi-sided trading platform' where consumers choose to share their data with companies.[198] A key component of these approaches is ensuring that, in line with earlier discussions, whilst data containers increase user control over access and sharing of data, they do not require a property led ownership model. As discussed, seeing data is a commodity to be traded can neglect the underpinning human rights basis of privacy, and the legal values it seeks to protect.

An important element of these services is the infrastructure used to store the data. The data may be on a 'personal cloud' hosted on commercial cloud infrastructure, or a local physical server, in the home for example. As there are data protection challenges around third country data transfer for cloud based services, physical hubs in the home may be preferable for users seeking greater control over access.

When third parties do access data, another tool could be tracking provenance of that data, who has accessed it, why, how long they need it, when they will delete it and so forth. Provenance can be as simple as tracking and recording movement or changes made to pieces of information. The standards body W3C created a model for designing for provenance called the PROV model. It defines provenance as "*a record that describes the people, institutions, entities, and activities involved in producing,*

[197] https://pds.mydex.org/mydex-charter
[198] http://hubofallthings.com/what-is-the-hat/faq/

influencing, or delivering a piece of data or a thing" (Moreau and Missier, 2012, p1) and uses so called PROV graphs to record and represent the nature, source, relationships between and changes with information. It has been adopted by the UK public record office, the Gazette, but more playfully Bachour et al's (2015) digital game, *Apocalypse of MoP (Ministry of Provenance)* explores provenance from the players' perspective. Players pose as government officials in an Orwellian institution, assessing provenance of information using PROV graphs and secretly leaking details to a resistance seeking to overthrow MoP. Whilst entertaining, it helps unpack players' attitudes to provenance, which vary from worries about linking of otherwise distinct information to privacy concerns about the permanency of information they may want removed. (Bachour et al, 2015, p245).

This highlights a key element of designer led responses: ensuring usability and comprehensibility to users. Technical means to provide greater transparency to the end user about the flows of data and control over access need to be tailored to their needs and skillsets to manage these tools. Accordingly, the role of HCI designers in user centric regulation comes to the fore again, as they are those that can ensure these tools correspond accordingly, moving towards user centric regulation in practice.

Conclusions

We looked at the IoT and smart metering to consider the nature of these technologies, situating them within their social and regulatory context. Following this analysis, we uncovered a range of legal challenges and user concerns posed by the different technologies. In order to explore issues in more detail, we focused on two specific legal values that emerged for users, control and access to personal data flows within the respective ecosystems. Within the more market led IoT domain, there is less prescription over what can and cannot be done. Accordingly, designers have greater scope for creative responses to realise PbD and picking up on the inadequacies of existing consent mechanisms for exercising control over personal data, we suggested the value of using the trajectories framework to redesign these. Within smart metering, there is more top down guidance over how data can be accessed and by whom. Nevertheless, in practice user control over access is still a challenge, and designers, as regulators, can again respond with their tools and

practices. In this instance, they can incorporate approaches, like personal data containers and provenance tracking, to ensure users control who accesses their data and why. These approaches still need user interests at the core, hence HCI designers are well placed given their proximity to users and methods for understanding user interests in contexts. This is particularly important given the context of the home, as a complex, contested social space.

However, having used the case studies to uncover the types of legal values at play, and the possible responses of designers, **we want to turn to practice, to understand how privacy by design manifests in action**. Accordingly, the latter two parts of the thesis are empirically led, firstly turning to practical insights from **thirteen experts** from technology law and design from across different areas of expertise, a variety of sectors, and levels of experience. We focused on a wide range of issues including the roles and relationship between these communities and practicalities of compliance with privacy by design, the internet of things and smart metering in their professions.

Following this, we introduce our approach for practically doing privacy by design, a set of information privacy by design cards that translates the GDPR into playing cards. These were then tested in a series of **six** workshops with **twenty-four** technology designers from a large global media firm ("MOZ"); a small technology businesses trade association ("SBA"); and an innovation network centre for SMEs/start-ups ("INC")). This section provides us rich insight into how user centric regulation can work, a range of insights into how technology designers navigate around legal concepts and values, the approaches they take to compliance, their strengths and weaknesses as regulators, and we frame our findings around our concept of 'regulatory literacy'.

Part III Expert Perspectives on User Centric Regulation in Practice

Overview

In this part we present findings from **thirteen** semi structured interviews conducted with **leading UK experts in information technology law and design**. As this thesis is very exploratory and multidisciplinary, we felt the need to go beyond the theoretical and legal analysis of Parts I and II. Accordingly, we make a turn to practice, to understand the nature of user centric regulation in more detail. Accordingly, through PbD and IoT we examine experiences of experts to uncover practical perspectives on how these two communities currently interact. We also consider barriers and opportunities around **doing** 'user centric regulation'.

Expert interviews are useful for our exploratory approach because these are senior thought leaders in their areas of expertise. They help us obtain detailed insight into complex practical challenges, but also strategic overviews of how they perceive their professions and roles, allowing us to consider how these communities may interact and align. We complement this high level exploration with a more operational focus in Part IV through our workshops with a range of technology designers in different organisations.

In terms of practicalities, following our case studies, we focused our questioning around a specific kind of user centric regulation, privacy by design, and the Internet of Things (where smart metering emerged as a theme). The questions varied for technology or legal experts, but broadly revolve around:

- definitions and regulatory challenges of IoT;
- nature and understanding of PbD, including reception in their industry and practical challenges it will bring,
- solutions to regulatory challenges of IoT and role of designers in regulation and protection of end user rights therein;
- practical challenges engaging with law or design (respectively).

The transcript of questions is in Appendix 5. Whilst structured using questions, we gave flexibility to participants to speak freely. Following Kvale and Brinkmann (2004) we also aimed to develop Socratic dialogue. This involved showing experts we also had detailed awareness of the area when asking questions, to prompt deeper answers, but being careful to restrain 'conversation' and 'discussion' enough to maintain the dynamic of an interview.[199]

The expert participants were drawn from a range of backgrounds to get a broad understanding of the perspectives on PbD and IoT in practice. We prioritised resources on speaking to experts from industry and legal practice, to complement the theoretical discussions outlined in Part 1. Nevertheless, we did still manage to speak to a couple of senior academics too, and the tables below provide more detail on their backgrounds. The recruitment was through direct contact (eg emailing known experts), gatekeepers to professional networks, and the snowball effect of interviewed experts putting us in contact with other experts. As these are very senior figures, setting up interviews often took a long time which limited the number of participants we could access. However, our saturation criteria was that we stopped once there were no new topics of discussion and our analytical categories could not be developed further.

For analysis we broadly cluster the participants under the labels of technologists and lawyers. We provide pseudonyms to protect the identity of all participants, providing their years of experience, current position and areas of expertise as metrics instead. 12 interviews were conducted remotely, via Skype or telephone calls, and 1 was conducted in person. The average length of interview was **44 minutes**. The participants were given an information sheet and consent form to sign, prior to the interview, and this is provided in Appendix 4**.** This study, and all studies in this thesis passed through the University of Nottingham Computer Science ethics approval process.

---

[199] Kvale and Brinkmann (2004) p147 "*Elites are used to being asked about their opinions and thoughts, and an interviewer with some expertise concerning the interview topic may provide for an interesting conversation partner. The interviewer should be knowledgeable about the topic of concern and master the technical language, as well as be familiar with the social situation and biography of the interviewee. An interviewer demonstrating that he or she has a sound knowledge of the interview topic will gain respect and be able to achieve an extent of symmetry in the interview relationship*."

The interviews were audio recorded, transcribed verbatim, coded and analysed using **thematic analysis**. We followed a qualitative methodology developing our analysis from a deep reading across the transcripts. We created initial codes and then clustered these into broad themes by looking at patterns within the text. We retained the detail in these broader themes by creating sub themes for different dimensions, refining these as the analysis continued (Braun and Clarke, 2006). These categories were tweaked throughout the analytical process as they emerged from the empirical data. Accordingly, our analysis was inductive and interpretative, where we focused on all actors' practical experiences, not on quantifying how frequently a topic was mentioned or discussed. We now turn to more detail on our participants, before presenting our findings.

Lawyers

The six 'lawyers' interviewed have an average of **14 years** of experience. We focused on speaking to practicing technology lawyers. Technology law is a broad field of practice, often incorporating expertise on contracts, data protection, intellectual property, software, e-commerce, accessibility, procurement and outsourcing, dispute resolution, and litigation. Many of our participants work across these areas but we highlight specific, self-identified specialisms below too.

We have two technology law partners (one co-lead), Ewan (14 years) and Duncan (25 years). Duncan specialises in procurement law, and Ewan in data protection law. Innes (8 years) is a commercial associate focusing on commercial information technology and data protection law. Similarly, Blair (9 years) is a technology lawyer, researcher and managing director of a law firm, specialising in telecoms law. Findlay (20 years) is a consultant specialising in privacy, information management and policy, and whilst he is not a lawyer, his work deals with many legal issues. Lastly, Campbell (8 years) is a reader in law, concentrating on media and technology law.

Table 7 Legal Experts

Pseudonym	Job	Years of Experience	Specialism	Industry
Blair	Managing Director Law Firm	9 years	Internet, Technology and Telecoms Law	Practicing Law
Campbell	Full Time Academic (Reader)	8 years	Teacher & Researcher in Law	Academic Law
Duncan	Partner & co-lead tech law	25 Years	Tech law and public procurement	Practicing law
Ewan	Partner in law firm	14 years	Specialise in tech and IT law, and also DP and information law	Practicing Law
Findlay	Consultant	20 years	Privacy / information management policy	Industry/ Consultancy
Innes	Associate in commercial and IP team in law firm	8 years	Commercial IP and Technology; Data Protection	Practicing Law

Technologists

The seven 'technologists' interviewed had an average **32 years** of professional experience. We have a range of expert participants, some with decades of experience in the IT sector, and many who are now working at a strategic level. Participant positions vary and include: managing consultant, senior researcher, CTO, director, professor, vice president and their expertise draws from specialisms like wireless networking, information security, privacy and identity, data science, ethics, big data, telecoms, cloud computing, interaction design and digital media.

To provide more detail. We have input from two lead industry consultants, Hamish (30 years) and Gordon (30 years). Hamish specialises in information security, and Gordon in wireless networking, sensors and Internet of Things. Allan (32 years) is a director in a global non-commercial organisation, and he specialises in privacy and identity. Jess (28 years) is a senior level researcher in a multinational computing firm, specialising in information security, data science and ethics. Iain (25 years) is a university professor specialising in interaction design and interactive digital media. Kenneth (42 years) is vice president in a global telecoms firm. Magnus (40 years) is a chief technology officer with extensive experience in the technology sector,

especially wireless networking and connected devices. Following this detail, we now turn to our findings in Chapter 7.

Pseudonym	Job	Years of Experience	Specialism	My Classification
Allan	Director and Technical Specialist	**32** years	Digital Identity & Online Privacy;	Non-Commercial /Policy
Iain	Professor and Chair	**25** years	Interaction Design; digital art	Academic/ Research
Jess	Senior Level Researcher	**28** years	Cybersecurity and big data; ethics of data science	Computing/Industry and Research
Gordon	Vice President and Primary Consultant	**30** years in technology industry, specialism in wireless semiconductors (**27** years)	Wireless networking and sensors	Digital Technology/industry
Kenneth	Vice President	**42** years electronics and telecoms; 15 years visiting professor	Engineering in Telecoms	Telecoms /Industry
Magnus	Chief Technology Officer	**40** years	Wireless technologies; IoT, smart devices	Consultant/ Industry
Hamish	Managing Consultant	**30** years	Cybersecurity and identity management	Information Security/ Industry

Table 8 Technology Experts

Chapter 7. Understanding Privacy by Design and Regulation of the Internet of Things in Practice

Within this Chapter we present insights obtained from practitioners and thematically group them under four sections: **the nature of the internet of things, realising privacy by design in practice, the compliance process, and the relationship between technologists and lawyer**s. We focus on presenting our detailed analysis of the data, contextualising it in relation to previous sections where necessary, but overall we use the final section to situate the data within our broader narrative around realising user centric regulation in practice. We now turn to our findings, beginning with how practitioners understand the nature of the Internet of Things, particularly how they define the IoT and the regulatory challenges both generally and for data protection and privacy.

1. The Nature of the Internet of Things

As we argued in Part II, the current vision of IoT can be defined as physical objects that are socially embedded, remotely controllable, and constantly connected. They have both a digital presence and backend computational infrastructure (e.g. cloud, databases, servers), networking and an associated ecosystem of stakeholders. We want to see how this corresponds with our participants' experiences. Within the law and policy community (hereinafter 'lawyers'), IoT is framed quite openly. It goes beyond traditional notions of computing, and is broadly viewed as any networked sensor or device. As Campbell [**University Reader, 9 years, Media and Tech Law**] contends, IoT is "…*things that aren't computers that are connected to the internet. Computers in the sense of desktop, laptop, higher spec mobile devices, basically everything that is not one of them but is somehow internet connected....*". Nevertheless, established systems, like the smart phone, are still IoT as they mediate end user interactions with other IoT devices and services. As Findlay [**Consultant, 20 years, Privacy and Information Management**] maintains: *"more and more digital services and devices are being created where the smart phone is the hub if you like, and the router in your home is the hub to your connected life."*

The legal community tend to contextualise their rather open definition of IoT using illustrative examples from a number of **application areas** drawn from their own practical experience. This includes:

- machine to machine industrial and retail applications,
- consumer products like autonomous cars,
- wearables like fitness bands,
- a range of smart home systems for security, lighting, energy management, entertainment and comfort.

Whilst the technology community (hereinafter 'technologists') also classify IoT by reference to different applications and sectors including smart cities and homes to Industry 4.0 and autonomous cars, some argue **navigating the margins of IoT is also important**. As some stated, point of sale terminals, card scanners, factory automation, sim cards, and even printers all have internet connectivity, yet it is debatable that they are truly IoT.

Some experts argue IoT is just the next hyped technology trend, like Web 2.0, Cloud Computing, M2M or connected devices that went before. Technologist Magnus captures this well:

"*they changed name from connected devices to M2M to internet of things – the cynical would say when something doesn't take off you just change the name –and it hasn't really taken off, the IoT is still predominantly hype… over the years [I've] ended up helping people putting wireless into everything from sex toys to snow ploughs.*"

Overall, the technologists provide **tighter, but more contested definitions of IoT.** Core attributes focus on the **physicality of objects, embedded computation, pervasiveness of communications infrastructure, global nature of internet and variations in user interface**. We return to the theme of heterogeneous devices below, but Allan's [**Director, 28 years, Digital Identity & Online Privacy**] definition captures these various elements, positing IoT is:

"a device that has processing capability that has some degree of user interface but where the user interface is partial, in other words, so for example if you have a smart lightbulb, part of the user interface would be you can turn it on and off, part of it might be you can remotely control times that it goes on and off, but that is not all the functionality the device has, so it also might have network capability that you don't have an interface to, it's almost certainly got backend cloud communication capabilities, and data transfer capabilities that you're very unlikely to have an interface to." [**Allan, Director**]

For some technologists, **framing IoT around the nature of objects or networking is misguided**. Instead, they want to go beyond just the vision of a 'connected product' to a more **holistic vision**, focusing on the user, their data flows and various practices around a technology. As Iain [**Professor, 25 years, Interaction Design and Digital Art**] puts it, IoT is:

"…about flows of data through practices, and most social personal practices involve physical artefacts, environments and other people, they are not just selves, data is often co-produced making it hard to identify ownership, it tends to be ubiquitous in a networking sense. Geography has become very complicated, it is very difficult to understand a geographic boundary around a thing, practice or dataset. The bug for me is to assume the things are objects, whereas things are far more complicated concept… [it's about] an internet of practice, but you can't practice without some objects, without other people." [**Iain, Professor**]

Beyond this more human centric vision, some technologists stress the centrality of data as a commodity, its importance for analysis and creation of new services. These participants were also wary of regulation, insofar as it may limit their access to data, as Magnus **[Chief Technology Officer, 40 years, Wireless Technology and Smart Devices]** says

"*…IoT is about taking data off a device and then doing data analytics on that somewhere in the cloud. The stuff in the middle doesn't really matter it just needs to be there and work…from my mind where I'm involved in a lot of data analytics on large databases, people always say, oh god data overload is terrible, I think it is an aspiration, I want more data, the more I have, the more I can do with it. Somebody tells me to minimise my data is basically trying to restrict a business model.*"

Overall, the lack of an absolute definition of IoT emerging from the two communities is useful. The more open approach, especially the strong focus on IoT applications, shifts attention. Instead of arguments about where the margins of IoT lie, or what networking approaches define the technology, the **applications** are key. This moves away from a vision led approach, committed to principles of what is or is not IoT. With applications come contexts of use and importantly, end users who have various needs and interests. By considering this level, a richer, situated picture of IoT can emerge, looking at the practices, interactions and relationships end users have with technology. For user centric regulation, this provides the context for understanding how regulatory issues play out in practice, and it is to those we now turn.

Regulatory Challenges of the IoT in Practice

In Part II we saw that IoT is challenging for privacy for a number of reasons. These include the technology being embedded in the intimate setting of the home, inadequate security, profiling and inferences being drawn about daily life from often disparate data sets, fears over data repurposing, inadequate consent over data sharing between objects to name a few. There were also general concerns about interoperability between devices and platforms, trust in security, spectrum and addressing, liability for harm, lack of standards, market dominance and appropriate regulatory approaches. Again, we want to understand how these concerns manifest in practice, so we begin with general challenges before looking at data protection and privacy in more depth.

Generally

Both lawyers and technologists recognise IoT poses many regulatory problems, but the lawyers, understandably, show greater familiarity with them due to their daily roles of looking at practicalities of achieving compliance. Between both sets of participants, a holistic view of the overarching issues emerges, **moving beyond the clear privacy and data protection concerns to safety, liability and responsibility for harm, data security, intellectual property, funding and interoperability**. In some respects, this corresponds with what we observe in Part

II, however understanding the detail is useful, so we consider a couple of examples below.

The technologists **question the fitness for purpose of regulatory frameworks and legislation** and how IoT impact existing legal principles and consumer rights. As Gordon [**Principal Consultant, 30 Years, Wireless Networking and Sensors**] frames it, "*fundamentally it is such a new tech, new area, it is fairly wild west*" and in some contexts, this is more apparent than others. A good example is the contrast between **safety and security**. Whilst devices will be subject to strict market access controls around electrical safety, similar oversight has not emerged for IoT security. Good security practices may require focusing on the diligence of designers to use best practices, as opposed to post hoc responses like insurance for security breaches. However, this requires systematic consideration of IoT security risks in design, again as Gordon, argues:

"*so you'll look at whatever the thing is that you're doing, you'll look at the platform, the operating system, the communications network, the security of that network, of how the data is transported on the network, what platform it ends up with, look at where the data is, how secure it is, the whole permissions side of it. We are pushing people to be more aware of that, where they bring security in by design***" [Gordon, Principal Consultant]**

Interestingly, **security, as opposed to privacy,** often emerges as a more legitimate concern for the technologists. Some feel data protection is limiting business models, stifling innovation or creative practice, and instead regulating misuse of personal data should be favoured. Magnus, who is largely sceptical of the role law had to play in regulating technology, argues a largely utilitarian perspective on regulating misuse:

"*I'd much rather see regulation of misuse, to say data will get out, it will get lost, and no amount of legal regulation will change that because you have human beings in the process. I think we need to look at a way of destigmatising and preventing the misuse of data which gets out. Accept reality, it will get lost, people leave things lying around, there are a lot of governments out there doing an awful lot to hack data.…I think we need to be careful we don't prohibit it, there is a balance somewhere and my feeling at the moment is that people who are scared about data are trying to*

force the agenda. …I think there are real benefits to be had from data, especially personal medical data and the law should be such that society can use data to reap benefits, rather than prevent it because of individual concerns."

Performing any systematic analysis of risks for IoT has to be framed by the nature of the IoT industry. **The embryonic market, the heterogeneity of the device ecosystem, and lack of industry standards complicate any application of regulations.** For Gordon, "*the [IoT] industry itself is very immature, very young. I've described it before as a 'primordial soup' there are a few things that have crawled out on land, some are slithering about, some have got legs, some have arms but we do not have many fully formed creatures yet*". Accordingly, dominant industry standards are yet to emerge. The commercial process of establishing dominant platforms or communications protocols is in progress. As we highlighted above in Part II, different communications protocols like Thread, Weave, Z-Wave ZigBee are emerging. Legally, this poses challenges for interoperability of devices, as Duncan **[Partner, 25 years, Technology and Procurement Law]** contends:

"[legally] *…it's always quite difficult in terms of the standardisation process, for it [IoT] to work together there have got to be effective standards to make everything work and at the moment, obviously everybody is jostling to become the hub, so that they want their thing to be in the driving seat, to be the heart of what is going on in the IoT, and obviously time will tell who will be the winners and who will be the losers.*" [**Duncan, Partner**]

Notwithstanding, the **technical heterogeneity of the IoT ecosystem** means the **standards** landscape is likely to remain unsettled for some time. Communications protocols, for example, need to reflect that different devices serve different functions, and users have different expectations around their use. As Gordon argues:

"*so a thermostat that chimes in every 15 minutes might be wireless, might be wired, is very different to a wireless doorbell, maybe used once every 3 days, so in terms of either its connectivity characteristics or amount of data, it is going to be very different. Other things, like if you had condition monitoring on your boiler, you need to know about it in 50-100 milliseconds, not next week.*" [**Gordon**, **Principal Consultant**]

Long term, the technologists argue that lack of device interoperability may enable **market dominance by market actors** with resources to invest in setting commercial standards, minimising competition from smaller actors.

The heterogeneity of the **IoT ecosystem impacts end users** in two other key ways. The technologists are concerned about how **variations in device interfaces shape the end user interactions**. Allan argues, "*there is a general direction of travel you can plot a line from browsers to smart phones to devices that run an app to ambient devices. At each stage along that line, the end user gets access to a more restricted user interface, and gets fewer and fewer controls over what the device is actually doing, and in the case of ambient, passive collection is at zero interface*" [**Allan, Director].** Secondly, devices mediate actions of end users and variations in customisability of devices can **shape control and choice in a subtle**, everyday ways. As Blair **[Managing Director of Law Firm, 9 years, IT and Telecoms Law**] puts it "…*at what point do you [as a consumer] find that actually you are not benefitting from all this wonderful technology but you're actually living in an environment where it is your fridge telling you when you can or cannot eat, because you've exceeded the number of times you've opened and closed the door in a day*…" [Blair, Managing Director]

We can see from these experiences, in practice the experts engage with a wide range of regulatory issues around IoT, where safety and security are particular concerns. Furthermore, **the embryonic nature of the IoT, the heterogeneity of the device ecosystem, and lack of industry standards are additional practical factors complicating application of regulations. We now turn to perspectives on challenges for privacy and DP.**

Data Protection and Privacy

Data protection and privacy regulation prompt rich reflection from the lawyers. Three primary areas of concern emerged around compliance and the IoT, namely, **consent; personal data flow management; end user rights and system designers' responsibilities around data handling.** These align with many of concerns discussed in more detail in Part II.

Consent

Starting with consent, whilst it is not the only legal grounds for processing personal data, it is an important one, especially for sensitive personal data. With IoT, obtaining freely given, informed end user consent can be challenging, especially when users are unaware of the nature of data collection. As Allan argues, "*consent is being tampered with, it's being assumed in some cases because the default setting for many devices may be that they connect and communicate, whether they ask or not, and consent is also being undermined because you don't necessarily know what data it is collecting or sharing, and you don't know what is being done with the data.*" **[Allan, Director]**

The requirement to inform end users about data collection, brings us back to the issue of **device heterogeneity**. Data protection compliance requires informed end user consent. The variations in IoT device interfaces necessitate more reliable mechanisms for delivering information during the consent giving process. As discussed above, **smart phones play a key intermediary role in the IoT ecosystem,** and can be a conduit for information, provided it belongs to the end user. Findlay outlines an approach:

"*In the IoT the challenge is many devices don't have a user interface, like the Nest smart thermostat. It is the smartphone, the web and email which you are using. You have two things right, your authentication device, the thermostat, but you can't present that info on the authentication device, so you need a consumption device like a smartphone, laptop or desktop, so it is going to require some thinking there, particularly when the law also says you also have to secure evidence of consent. So that needs to give some rise. So when it comes to an IoT device, and then the consumption device for information, how do you know if the consumption device is mine.*" [**Findlay, Consultant**]

The practicalities of designing **cross device consent making processes requires reflection and tailoring to different contexts and end users**. Nevertheless, such mechanisms offer a starting point for lawyers and technologists to work together to address compliance requirements in innovative ways. One consideration is that IoT devices often operate in settings where consent of multiple end users is required. Lawyers need to create approaches that provide notification of data

processing and obtain consent from all data subjects affected, for example visitors to the home being captured by a domestic security system. Innes [**Associate, 8 years, Commercial IT and Data Protection Law]** frames this challenge by contrasting consent mechanisms for a personal fitness band with one user and a connected building with multiple users:

"*…it's quite straightforward if you've got something like a fitness band that connects to an app, and you've got a single user who signs up to that app and has an account and it's in a kind of closed network, that is quite straightforward to put a privacy policy in and a consent process in place… if you start thinking about connected buildings, where you've got everything from cameras to thermostats to infrared sensors, light sensors, temperature sensors that are collecting data relating to lots and lots of different people, it starts to get a lot more complicated in terms of getting consent from all those different people, and also in terms of those people knowing what data is being collected and what is being done with it.*" **[Innes, Associate]**

Lastly, the power asymmetries between consumers and IoT product/service providers become evident when terms of service change and renewed user consent is required. Consent is meant to be freely given, but consumers are often faced with a choice of accepting contractual changes or stop using the product. Blair questions this practice, stating "*the idea that something is freely given, when you've paid £250 on your smart thermostat, the idea of use it or lose it because of a change of terms makes it very questionable if any consent is ever freely given.*" **[Blair, Managing Director]**

To conclude, particularly interesting here is how device heterogeneity complicates obtaining consent, especially for multiple users across multiple devices in an IoT ecosystem. Understanding how to design for this may invoke the role smartphones as mediators of information and consent making processes. However, a background concern is that consent is not freely given because when a device costs a lot of money, the alternative of boxing it up and not using it is not viable. These findings add richness to the discussions above around redesigning consent mechanisms, where such elements as use of smartphone interfaces or standardising for more coherent consent mechanisms across devices could work.

Managing Flows of Personal Information

Moving beyond consent, IoT ecosystems involve **flows of information** between different devices, users and services. **The complexity and diversity of these interactions can make it hard to understand the flows and the rationales behind them**. As Iain puts it "*Across the IoT then we will have to deal with a whole host of transactions, and some of those will be incredibly small, and involve small forms of currency, not just economic, but data, if a kettle talks to the fridge, or the toothbrush to the toothpaste, or the door to the car, will many of those things, how will they want to be private, how will they construct valuable experiences? Will be really really challenging.*" [**Iain, Professor**]

Nevertheless, from a compliance orientated perspective, there needs to be effective understanding of the personal data flows within these micro transactions to enable oversight and effective management. One challenge is **understanding who is responsible for the data, and mapping their obligations**. This requires asking practical questions like what is data being used for, by whom, where it is being stored and how long it is being kept, but as Innes argues, the breadth of stakeholders, platforms and applications make this a tricky exercise:

"*I think identifying who the data controller is, particularly when not just speaking about a single device but in an interconnected environment where you have all these providers of different tech hosted on different platforms maybe a building landlord who is responsible for a building then you have got tenants and service providers and it gets very complicated with all these different players who are maybe using this data for their own different purposes, you start seeing different levels of data controllers for different obligations. It's going to get very complicated*". [**Innes, Associate**]

Both technologists and lawyers are concerned about flows of data to third parties. Whilst **interactions between users and primary service providers may be apparent, and legitimate, protecting rights with third parties is harder**. As Allan argues, "*you have a right to know that a third party has data about you and that right is kind of implied by the right to see that data, and to correct it and so on, if you simply don't know or you don't know who the third party is or how to get in touch with them, then your ability to exercise that right is completely undermined*" [**Allan, Director**]

Indeed, end users have a range of DP rights, but the challenges in establishing who is responsible for them can impact how they are protected and realised in practice. One reason these rights are so important is the **control** they afford the end user over their personal data. **Control in this context is not just about the data itself, but also controlling the inferences that can be drawn from the data, in particular any second order prejudicial impacts**. Blair's example captures this dynamic well, depicting a hypothetical scenario where insurers use wearables to monitor user activity to vary premium rates:

"*the idea of automated decision taking, and making, based on the data acquired from IoT… take for example, private health insurance and they say here you go, we will send you one of our smart pedometers or our smart fitness trackers, you wear it, as part of your contract of health insurance, and we will price your premium based on the level of activity that we see you doing, if we see you sitting in your chair all day you will get a higher premium because you're inactive, if we sense you play rugby you will get a higher premium because you will hurt yourself...*" [**Blair, Managing Director**]

With the flows of information, establishing responsibility for data is complicated by the complexity of the data flows in the IoT. As discussed in Part II, control is key and designers have a responsibility to ensure users can control impacts of their data being shared, for example with the inferences or prejudices that stem from information processing.

End User Rights and System Designer Responsibilities Around Data Handling

System designers owe many responsibilities to end users, such as only using their data for defined purposes, **not keeping it longer than necessary and only storing it in adequately protected conditions**. However, IoT business models challenge many of these rights, as we discuss in more detail below, but taking the example of data storage, Innes unpacks the compliance challenges designers face: "…*location of the data, where is it being stored, is it getting transferred overseas, where is it being hosted, we deal with a lot of issues that arise around transfer of the data outside of Europe. So a lot of the big cloud providers, people like AWS or Microsoft are based in the US, and so*

compliance can become quite tricky where data is flying all around the world which is often the case for these kinds of IoT type technologies." [**Innes, Associate]**

Some experts state IoT does not always have a negative impact on user rights, and has the capacity to offer more transparency to the end user about data processing. **If IoT could provide better information about data processing for the end user, it may even reduce the need to rely on existing legal rights like subject access rights**. As Blair highlights: "*in the context of the IoT it would be nice to think that subject access rights isn't required, that enough companies will simply make this data available for download as a matter of standard business practice. When you look from a privacy by design perspective, subject access right are really quite an abomination, why do you have to go and specifically request these [data], and pay your ten quid for the pleasure, when this kind of thing could be made available for download quite easily.*" [**Blair, Managing Director**]

To conclude, whilst from one perspective IoT poses challenges for compliance, such as with international data transfer and storage in the cloud, on another, the IoT can increase transparency of data processing, reducing the need to rely on legal rights like subject access requests. Systematic consideration of the risks and implications of data processing can help map how IoT enables or challenges rights, hence privacy by design comes to the fore again, as Blair introduces. Following our critical analysis in Part II we now present practical experiences of **doing privacy by design for** the Internet of Things from our experts.

2. Realising Privacy by Design in Practice

What is PbD?

Ideologically, the lawyers view PbD positively because it exposes privacy risks earlier in the design process, allowing them to be addressed and avoiding 'back-pedalling down the line'. However, experts argue PbD requires greater critique and reflection, including both communities sharing what works and what does not. At the abstract level, even the terms 'privacy' and 'by design' are disputed. For example, **with privacy, technologists question how to design for such a contested social value**. As Iain frames it:

"*My problem with privacy by design is I don't know what people mean by privacy anymore because all of the practices we carry out contradict the values…you can't expect people to recover values, and when they do recover values, they go back to really old school values like Christian values or family values, or I don't think they know what privacy values are, I think they contradict them all the time, through the value propositions of which ubiquity in networked data offer them***." [Iain, Professor]**

Whilst, some technologists questioned what PbD actually means, like Kenneth "*I don't really think industry understand what headline PbD actually means, I don't think there has been a communication that has turned it into what does this mean?*" he argues it is better **to understand how PbD will play out differently for specific application sectors and solutions,** e.g. with cars, cities and the home, **as opposed to a generalised approach.**

There are also **parallels between privacy by design and security by design**. Security is often not considered until later in the development cycle, retrospectively looked at after the device been rushed to market, and there are minimal motivations to thinking about security or skills gaps. Technologist Hamish **[Director and Managing Consultant, 30 years, Cybersecurity and Identity Management]** captures this within start-ups, a sector we return to below, explaining:

"…I think for start-ups and SMES unless security is critical to their project, it largely gets overlooked because they are working on a limited budget, they have got to start producing revenue as soon as they can, and therefore it is a race to get your component to market as quickly as you possibly can, and it is very much seen, well there might be some security things, but we'll fix those in version 2…sadly, it never happens in version 2 and what does happen in v2.0 is a bit too late, because of some of the design decisions made in version 1" **[Hamish, Director and Managing Consultant]**

Similarly, the lawyers are concerned how PbD is framed as a solution. Whilst PbD may involve building in privacy enhancing tools like encryption into a system, more fundamentally it is important to **reflect on if PbD is meant to support existing legal approaches to privacy, or to replace them with technical measures**. The latter did not work well with copyright and digital rights management; hence Campbell warns:

"*The idea that you can substitute legal protections and balances with technological protections or workaround… I think that will be trickier…if it's [IPbD] seen as part of a broader approach, as in one of the ways in which agreed legal standards can be implemented, so it doesn't add anything new in legal terms, it just takes, what I inelegantly call prevention instead of cure response, that has some potential"* **[Campbell, Reader]**

To conclude, more critical reflection on PbD in practice is important. Understanding privacy as a value is an issue for designers, as it is a contested term and looking to users may not provide much clarity. Learning from similarities with security by design may be useful, as can questioning what PbD is. Is it aimed at augmenting or replacing traditional legal approaches? The former is preferable, but importantly, like with IoT, PbD cannot be understood in the abstract, and focusing on how it manifests in specific sectors is important, instead of at a general level.

Doing PbD

Following these initial definitional points, we want to get into the detail on how the communities foresee actually doing PbD. Critical to understanding PbD in practice is unpacking the **commercial reality of the emerging IoT market, and how**

business models are shaped (or not) by regulation. Firstly, we turn **to business models** and the **motivations of organisations** for thinking about privacy.

Motivations for Engagement with Compliance and Dominant Business Models

On the one hand, our experts argue many organisations focus on **providing a cheaper product, knowing the value derives from the monetisation of the users' personal data**. This model is not exclusive to the IoT sector, and mirrors the approach of many web based services. As Allan states "*Fitbit is probably a good example – you buy the device, nominally you own it, but you might get it at a price that is based on an assumption that the device is partly subsided by the monetisation of your personal data, and you may have more or less control about that aspect of the bargain, in other words it might be buried in the small print or the privacy and security settings that you have to dig your way through to turn it off, and it's on by default.*" **[Allan, Director]**

Against this backdrop, the lawyers argue **many businesses are collecting more data than is strictly necessary and stockpiling it for later use because the technology lets them**. Collecting too much data, without good justification or oversight, **means effective protection of end user rights and prudent data handling can be lacking**. Ewan captures this tension well drawing on the context of subject access rights.

"…we work with clients, not just in the tech community but all kinds of sectors where they hold a lot more data than they probably need to, [client's say] 'you give me a subject access request, we have this data here, do we need to disclose it? No, we don't disclose it' …well we ask you –'have you got it' and they can't answer the question of why they have retained it in the first place because no-one knows about it… the technologies provide the abilities to do a huge amount, and people will just collect data, well because it might be useful. What we are trying to say to clients is that is not how you approach this, yes your system may allow you to collect all this stuff, but you need to think why you're retaining that, why you're collecting that." [**Ewan, Partner**]

In contrast, some technologists argue that collecting more data makes good business sense, for example more open access to data enabling discoveries and innovations in the health sector. Within the IoT industry, some experts suggested

there is a desire for more data, to learn more about the product use, to find interesting data-points and refine the business strategy. Clearly, this may contradict many tenets of data protection law (eg data minimisation, purpose limitation), yet any goals of operationalising PbD for the IoT needs to recognise these business models and this business culture. Accordingly, as Magnus argues:

"I would say is the industry wants as much data as it can get as opposed to restriction. The other thing I see in products is good products will be flexible so you can change the data that it captures, because a lot of the time you start off you don't know what data is valuable. To me the IoT gets interesting when the cost of connecting a device and getting the data back becomes so low that you just say "I collect the data because I can, don't know what I'll do with it but chances are there is something valuable. If you don't know what is valuable you'll start off by pulling as much data as you can, but you'll be limited as to what it is because of cost of connection, as you start to see things you'll want to adjust your sensor to say "let's ignore that but I want a lot more of this" so you'll get an evolution of the data you will want to pull back through the life of the product. That means you want to make your product flexible and capable of generating as much data as you possibly can. Any regulation that tries to say no I've got to anonymise or limit or pre-process that, pushes against the rationale of why you want to get that data back."

In light of this, **any appropriate regulatory responses, like PbD, needs to understand the motivations of different actors in IoT to adapt their practices and business models** to thinking about law and compliance during design. Interestingly, more than legal compliance, **damage to brand reputation from hacks or scandals and end user disquiet** are discussed by experts as prompting action, yet they have to be balanced against other factors such as **costs or lack of likelihood of enforcement**. Indeed, whilst many technologists are keen on the concept of compliance by design, either as privacy or security by design, they recognise the **practical motivations for doing it are lacking**. Allan, summarises the balancing that is necessary and factors organisations will consider. He states "*I think PbD is a good aspiration, the question is first, how do you motivate organisations to have that aspiration and second what is the pay-off for them if they do. Is it a negative pay off, we are not going to get silly questions from the regulator, or is it a more positive pay off, like customers in the long run will actually perceive us as a better company to do business with…"* [**Allan, Director**]

Beyond branding, technologists cite the motivation being building a **good product**, not just compliance. As Magnus states, "*you need to believe in what they are doing needs to be done because that makes a good product, rather than just saying, here are some hoops, jump through them"*. Some technologists also highlight that they are not driven to behave accordingly due to law but because of an **internal code of ethics and their own business values**. Kenneth captures this explaining his companies approach to trials with driverless cars:

"*I can assure you that all our trials this month and next six will be pro safety based innovation. we need to make sure a driverless car does not crash into people, or dogs or old ladies, and it is not the law that has made us do that, it is our code of ethics, it's the way in which we've been told the research has to be run… [asked about source of this code of ethics] I think the source stems from the fact that if you're building big networks as we do, we don't want to suddenly disappear overnight because somebody says you've stepped over the mark. So I think it's inbuilt personal values, but it's linked toward the fact that we're a licensed entity, licensed by the regulator, an entity called Ofcom, with links to the government…*" **[Kenneth, Vice President]**

Linked to this, as part of **being a better company**, an interesting motivation as the **lawyers cite pitching privacy and ethical data handling as a form of branding.** Responding to compliance can be made into **a viable selling point**, and frame compliance in a more positive way, not as stifling the market, but instead as a business opportunity. As Innes puts it *"…privacy compliance can be seen as a kind of barrier to innovation, this kind of idea that having to tick these boxes we can't develop the technology that we want to develop, but I think you can flip it over and say, well if you're a trusted organisation that can demonstrate really good privacy compliance, the end user is going to be more comfortable giving you their data and saying actually I don't mind you using my data for all these different purposes because I know you're going to look after it, so I think there is a flip side that if you are very compliant and you can demonstrate that…"* [**Innes, Associate**]

Experts also state that in fostering a trust relationship, consumer demands have to be considered, as we see with fair trade and ethical standards shaping other markets. Indeed, encryption, as a **privacy enhancing technology, is one which carries brand values**, and customer desire can motivate companies to adopt such

technologies. Campbell argues "*Does the tech company really care about encryption or does it recognise that consumers seem to feel comforted by it? Where if they hear the name of the product with high grade encryption in the same sentence, that is a signal of quality and security and reliability…it seems to have possible brand values...*" **[Campbell, Reader]**

Another element is both technologists and lawyers recognise businesses may take a **risk by trying to foster more privacy compliant practices.** They could face a **competitive disadvantage** because becoming compliant adds costs, yet without greater transparency in the market, it is hard for them to know if competitors are doing the same.

To conclude, the **commercial reality of the emerging IoT market is key to understanding how business models are shaped (or not) by regulation, and how PbD might work in practice.**

As our experts show, the dominant IoT business models and culture are to create a cheaper product but monetise the personal data. This involves collecting as much data as possible, partly because technology allows them to, but also to stockpile it for later use and to find new applications. This really challenges DP compliance because within the IoT industry **there is a desire for more data, to learn more about the product use, to find interesting data and refine the business strategy.**

The motivations for organisations to engage with compliance and PbD are lacking in practice. The drive is not to be compliant but protecting brand and reputation due to fear of hacks, scandals and user disquiet around practices. Any change needs to be balanced against monetary costs, lack of enforcement and competitive disadvantage (i.e. increased costs by being compliant when competitors are not). Internal code of ethics and brand values may be a motivating factor, as is the desire to become a better company and build a better product.

In responding to such motivations, lawyers pitch PbD and compliance to technologists as a type of branding that can be a viable selling point. Within this, consumer interests need to be considered by designers, and moving towards a

relationship of trust can prompt adoption of privacy enhancing technologies, like encryption. To understand these elements in more detail, we need to consider the range of actors involved in the IoT market, from multinational companies to start-ups and SMEs.

Differentiated Resources

Even if the motivation to act exists, any response requires companies to have adequate resources. Here we see a challenge as the lawyers' outline responses to compliance are shaped by the differentiated resources available to smaller firms (start-ups, SMEs) and larger ones (multinationals).

Perhaps obviously, start-ups lack the financial resources to obtain legal advice. **Instead they are focusing on getting more investment to stay in business, not compliance**. Accordingly, their relationship with regulation is not on good terms, and ironically, by neglecting compliance short term, they are exposed to legal risk, which makes future investors wary of getting involved. As Ewan puts it "*the people that I speak to who are in [tech incubators], a lot of them all they are interested in really is raising money from investors, because that is what they need to live on, because they are living pretty much hand to mouth, so their interest is in winning business and getting investment…things like Privacy by Design and Privacy by Default, how they are anonymising data, what their data retention policies are, how they communicate with customers, that's just not on their radar…"* [**Ewan, Partner**] Similarly, technologist Gordon explains that "*there is so much going on that the innovators are probably blissfully unaware, I think there is a bit of don't ask don't tell. They are so desperate to get product to market, to get revenue and investment, I think the legal and security side as well isn't being thought about"* **[Gordon, Principal Consultant]**

If we contrast this with large firms, they may have greater awareness of the regulatory issues in the first place. Their **familiarity with regulation in the market** puts them ahead of market entrants, like start-ups, who lack resources to get up to speed with regulation in that sector. Blair gives the example of the communications sector and telecoms where he states: "*So I suspect one challenge is networks, to my mind at least, were traditionally the preserve of large companies and often large companies with reasonable sized legal teams capable of understanding a complex and quite sophisticated regulatory framework, so I think the one challenge will be the fact that a lot more*

companies are working in this space, and they are not the traditional telecoms companies, how readily can they analyse and understand complexity of the regulatory framework and apply it to their products and services, does that remain a reasonable expectation."[**Blair, Managing Director**]

Secondly, larger firms have **greater financial and organisational resources to address compliance requirements systematically and comprehensively**. They can put in place processes that harmonise their approach on **a global scale,** for example, dictating when designers need to engage with in-house legal teams for advice. As Innes puts it *"…we are seeing more … organisations are consulting us not in relation to a specific technology but in relation to their compliance more generally. So if they are putting in a regime for an entire organisation globally, they cover off all of their privacy compliance, relevant documents, then they will have a privacy design policy that applies to all the developers that work for them, so there will be six steps that have to be followed, and they have to engage legal at a particular stage, and often they will have in house legal and won't be coming back to us…"* [**Innes, Associate**]

Clearly, privacy by design does not exist in a legal vacuum, and any practical implementation needs to reflect the commercial landscape and the motivations of those actors. Hence, even if motivation exists, resources may preclude engagement with compliance. SMEs are focused on investment, not compliance. In contrast, bigger firms have greater familiarity with regulation in a particular market, than start-ups, with financial and organisational resources to address compliance in a systematic, comprehensive manner, globally if necessary.

Another important consideration raised by experts, before moving to practical approaches to achieving PbD implementation, is the impact of **legal language.**

Legal Language

Even if both **motivation and resources** exist, another key practical barrier for designers engaging with law is the **inaccessibility and uncertainty of both legal terminology and the underlying legal concepts**. At one level, the nature of legal language is framed by the subject matter. As DP law expert Ewan argues, topics

like data protection are quite inaccessible, "*I think data protection law is pretty obscure to most people, I mean even as [a] practitioner it is not the friendliest thing in the world*" **[Ewan, Partner].** However, for the lawyers, greater crossover may be achieved by agreeing **a common language** to help both communities move forward. Part of this may be engaging in **cross community dialogue earlier**, during disciplinary education, for example in computer science degrees or in university research. Importantly, they do not view language as an insurmountable barrier, and Blair goes as far as arguing "*I suppose in my view, lawyers are nothing special, they just tend to be trained in a particular way of thinking, and because it is often lawyers on the other end enforcing things, you're likely to be thinking in a similar framework, but there is no reason why an engineer couldn't think like a lawyer*." **[Blair, Managing Director]**

For technologists engaging with law, complications vary from the complexities of the EU legislative process, like recent EU information privacy law reforms, to questions about jurisdiction where US designers may assume Californian law applies everywhere or struggle with regional legislative differences. As Jess [**Senior Level Researcher, 28 years, Cybersecurity & big data, ethics of Data Science]** put it "*it is really tough when there are 7 different interpretations within Europe alone, and we are going to produce something that conforms to the spirit and the letter of the law, even with lawyers to help it is hard to translate that into technical guidelines, and it's hard because the actual detail is complicated but also the languages have different grammar, vocabularies and types of common sense.*" **[Jess, Senior Level Researcher]**

A key issue raised by both technologists and lawyers is the **uncertainty** inherent in law. **Legal concepts, like consent, can pose challenges for designers, as they want clear design requirements to work with.** As Findlay explains from his experience with designers *"…the techies, the engineers, said to me [Findlay], I can't deal with unambiguous consent what does it mean, I'm an engineer I need precision..."* **[Findlay, Consultant]**

However, law does not provide clear requirements as it is not a binary entity, and even if the abstract language can be understood, in practice, **interpretative factors like likelihood of enforcement by the regulator** need to be factored in. This causes problems for designers, as both communities argue. Lawyer Blair explains

"…*actually the geekier clients sometimes struggle with law, because as lawyers, while we might like to think law is black and white, actually the law is a big shade of grey.*" Similarly, technologist Jess discusses the language of law and challenges of precision **"***well, the main problem is law, like technology, is written in a completely impenetrable language, and more than that it has a different type of precision from technology language…so in law, common sense does really help, whereas it doesn't help in technology, you take things as literally as possible, it's not the case in law, you can apply your common sense and judgement.***" [Blair, Managing Director]**

Whilst common sense can be useful, unpacking what the law requires needs a more **systematic process.** Interpretation, clarification and practical action necessitate further investigation and legal inquiry. The lawyers recognise that incorporating such an **exploratory process into an already saturated design process will pose practical challenges**. Whilst precise legal requirements may become just another design requirement, like usability, sustainability or low monetary cost, getting to that point takes some time. As Campbell explains:

"…*when a design process already has many steps and there is a desire to introduce a new step, if that new step creates a whole range of sub questions to which experts will say, 'I don't know it depends', that's a different type of step. If you have a design process that involves concept beta testing, security testing, these are all fairly self-contained, you know what is going on with them. If one of the things is make it privacy friendly and you say, what do I have to say, 'well there has been this case and there is this law under revision' that is not just a step, that is a whole series of steps, that's a whole literature, I think that is one of the biggest challenges*." **[Campbell, Reader]**

To conclude, there is uncertainty around both legal terminology and the underlying legal concepts for example legislative process, jurisdiction or designing for consent. Designers want to build technologies with certainty, but legal concepts do not provide this and the uncertainty around regulatory enforcement complicates matters further. Whilst greater cross community dialogue can help, designers need more systematic understanding of what the law requires, but such exploration cannot be complex and long as it has to fit within existing design processes, often constrained by time or cost.

Fundamentally, **addressing the requirements of privacy by design requires practical steps and approaches**. Whilst we explore one approach in detail in part IV, information privacy by design cards, for now we focus on approaches both communities raise during our interviews. For now, we present findings from our experts, classified into two areas: **developing effective communication and engagement around law.**

In part this requires looking at:

- how to communicate the relevance of law to designers;
- how to get effective engagement with compliance (where resources might be tight) and
- recognising that designers are often having to balance many competing commercial interests.

Effective Communication and Engagement

Participants state one challenge for law is getting past it being seen as a tick box exercise or a hurdle to be crossed and *effectively communicating the relevance to designers.* Technologists are keen on education, as opposed to regulation on the importance of compliance. However, even if knowledge exists, and is out there, for example with building secure websites, **the motivation may still be lacking to act on this knowledge.** As Hamish argues:

"*There are some very well defined best practice designs from government and industry bodies. If you follow those guides, it's perfectly possible to build a secure website but for some reason we still see website hacks every week. So for some reason, although knowledge exists on how to build a secure website, there are still businesses not doing it, and I think that is the challenge the IoT has to get over is, even if you get to the situation where there is knowledge how to build IoT, how do you make sure people do it, because the motivation isn't there on websites, now hopefully the GDPR will start to change that, but time will tell.*" **[Hamish, Managing Consultant]**

Doing this requires **developing strategies to translate and frame the relevance of law to the work of technologists**. Approaches need to engage engineers with law, such as framing privacy as an important value and an opportunity to help the end user not just a compliance requirement. As Findlay puts it *"…if you put it in the context of their own lives, they get on board very quickly, if you put it in the context of a dry legal requirement they switch off within 10 minutes…*" **[Findlay, Consultant]**

Furthermore, ensuring there is engagement beyond the technologists in an organisation is also key. Senior actors, like **board of directors** of companies, can foster a **culture of risk awareness** within the organisation through their leadership. Based on his experience in security consultancy, Hamish explains this often requires assessing values in a company and then presenting risks to that value:

"*…the board of directors are largely detached from the product set, because there are so many products, so the only way the board of directors can manage the business is by looking at risk, so that builds a risk culture into a business that propagates all the way down, so when it comes to the technologists at the end developing the tech, they need to understand risks because they have to report into the management chain…you have to get the board of directors of the business, and then you have to translate the security issue into language that they understand, which is about investment and risk. You can't just do it from, "there is a risk this system will be hacked", you have to turn it into something they really understand…so that is the skill you need, security people that are able to go in and understand where the value is in the business. Look at the risks to that value and inform the board of those risks, so the board can then take an informed choice as to how seriously they take security*." **[Hamish, Managing Consultant]**

Most interestingly, both communities recognise the need for a **process of translation from law into something actionable by engineers**. Documents, like **codes of practice**, are artefacts that bring abstracted legal requirements down to grounded, **actionable guidelines** such as 'install these patches' or 'use this software to secure your system'**.** These are invaluable, as Jess explains:

"*I'm used to reading the law, but it is like saying 'here is something is in Portuguese go and read it in Portuguese', you get an idea, but really it is much easier with a code of practice…so if you say, do you have adequate security safeguards on your machine, people will say, "I think so"…*

for very good reasons, the laws cannot be precise about the technologies because if they were, they'd be out of date by the time they were passed. This is good, but it does mean that the translation into the specific things that you have to do is something that has to be done, you can't get it just from the law." **[Jess, Senior Researcher]**

Beyond these codes, **annual training or support websites** may exist, especially in larger organisations. Again, Jess explains how training works in her multinational organisation, but raises the practical challenge of how to translate law into a more accessible form, a point we return to in part four. As she argues:

"*every employee for compliance purposes has to go through training, where some things are part of company policy, some are required by law and some things that it would just be a good idea to tell us and that is in all sorts of areas like export control, data privacy, competitive law, anti-corruption stuff…some of which are really well done, some of which seem to be written too closely to the legalese. You can understand why that happens, when translate something from the law you are inevitably reducing it in some way and you don't want to reduce it too much*" **[Jess, Senior Researcher]**

Understanding where to pitch the tone of any guidance is a key part of effective engagement. Knowing your audience is important, and **keeping legal processes as simple and lightweight as possible** is a good start. Technologists may have little time for red tape, and just want to get to work. As Jess puts it, "*researchers and engineers, we can't wait to get our hands on making something, we just love doing it, and the idea that you will have lawyers holding you back just really goes against the grain… if you are a geeky experimental type, anything that gets in the way of doing good work is just such a pain, you hate it.*" [**Jess, Senior Researcher**]

Furthermore, recognising that designers are often getting pulled in many competing directions within their organisation is important. Any engagement with law needs to **reflect they will be subject to pressures from different stakeholders who want designers to create systems in ways that address their interests**, be that legal, business or security, for example. Blair summarises this tension explaining:

"*I probably come from a world where you have the people who write the code, aren't necessarily the people who decide what that code needs to do, you've probably got a range of people all saying what it needs to do…people saying what the customers want and others saying what the business is willing to deliver and what are the trade-offs, and lawyers saying what needs to be done legally, the information security team saying what needs to be done technically, and you've probably got a business analyst frantically scurrying around trying to write all these down and then you've got some poor sod sitting in front of a computer trying to program something that meets all these objectives.*" **[Blair, Managing Director]**

However, some technologists argue it is **not the role of the designers to deal with these tensions**. Instead, they should be given requirements to work with, and it is up to the others in the supply chain to deal with these competing requirements beforehand. As Hamish puts it:

"*I'm not necessarily sure it's the engineer's responsibility. If you think about the technology or software development cycle, engineers or technologists build something to a set of requirements, what usually happens more that need to make sure the privacy and security requirements are defined and handed to them. If they've got those requirements, engineers and technologists are very good at controlling that. At the moment I think it's a weakness of business requirements defining what they will implement, I'm not sure it's technologists that need better understanding of it, it's probably the product managers and owners that are commissioning the technology…*" **[Hamish, Managing Consultant]**

The range of actors involved in design will differ depending on the organisation. As we discussed earlier, the differentiated resources available to smaller and larger businesses shape their capacity to deal with compliance. One implication from less internal resources for compliance the lawyers raised was relationships with state regulators. Smaller organisations are still subject to the same laws, yet they may lack the support channels from regulatory agencies that larger organisations have. **Engagement with regulation needs awareness raising, and practical support** and Ewan questions how this will be done by the Information Commissioner Office for start-ups and SMEs dealing with data protection compliance. As he argues:

"*…SMEs, and people who are not on the radar, and how you actively engage with them on what they are doing with data, and what they should and shouldn't be doing. That is a big challenge, because these are the people who may not have the money to take legal advice or employ a privacy expert within the organisation but they do need to understand this, particularly in the start-up community. I don't know how the ICO gets that message across, and if there is a lead person there, but I think there is a role for some sort of industry body… who can try and hold the hands of the people who are otherwise going to fall between the cracks and are going to really struggle.*" [**Ewan, Partner**]

Technologist Gordon reflects this point, explaining that **within the start-up community there is little awareness of legal obligations:** *"no no I don't think the innovators have any problem [with legal concepts] at all because they have no clue what they are supposed to be doing. The impact of regulatory stuff has no impact on a 5-man start-up"* **[Gordon, Principal Consultant]**

To conclude, developing effective communication and engagement around law and compliance can involve a number of strategies to make law more relevant to designers. These can include, putting law in the context of their own lives and work; promoting a culture of risk awareness through leadership and understanding how legal risks might endanger values held by that company.

A key area of support is through translation of law into more accessible form for designers. This includes translation into tailored codes of practice and actionable guidelines, training or support websites, and keeping the legal processes engineers need to follow as simple as possible.

These approaches need to reflect that designers will be subject to pressures from different stakeholders who want them to design the system in ways that address their interests.

A specific area of support is awareness raising, and practical support for SMEs who lack resources of larger organisations because within the start-up community there is little awareness of legal obligations.

In unpacking this discussion further, we now turn to discussion **about how state regulation and enforcement play out in practice**. Understanding the processes underpinning compliance provides us insight to then think about the changing roles of technologists, lawyers, their interactions and solutions going forward.

3. The Compliance Process

Within this thesis we focus on privacy by design, and data protection law but user centric regulation is broader. Within IoT, there are a range of other regulatory frameworks beyond DP law, which our experts discuss. The lawyers explain the range of factors that dictate the applicable regulatory frameworks. As IoT involves physical products, product law may have much to offer, such as with safety standards, but equally, distinctions in the type of physical product or networking (e.g. public or home network) can shape the regulatory forum. Taking the smart phone example, as a mediating technology in IoT, Findlay explains the breadth and complexity of regulation surrounding this device. **This reiterates that even if steps are made to address DP law, there are many other laws of the land, licenses and regulations to consider.** As he argues:

"*…we are taught about the central role the mobile phone plays in people's lives, it's the medium by which we connect to everything, so we have 109 DP laws, but we have over 200 telecoms laws, over 200 secondary codes of conduct and regulations, we have over 800 license conditions that regulate what mobile operators can do, imposing security obligations that place restrictions and restrictions on use of traffic, location, subscriber, account data that may stop some of this data going overseas, so it's not just about the DP laws. So when we look globally, the unique thing about the IoT is it is a global interconnected ecosystem, you've got the UK that connects to X to Y. But you've got this patchwork of laws that is a fabric, but it's a fabric that constrains and restricts the ability of the IoT to flourish, even regionally*." **[Findlay, Consultant]**

Similarly, in some industries, like telecoms, licenses to operate have significant regulatory effect, both as they are enforced by the state regulator, Ofcom, but also because consumers trust the brand. As Kenneth puts it: "*[with IPbD] what will happen in practice is there will be trusted parties, and people will use and work with trusted parties. So telcos are licensed, and in effect they will say, you are licensed don't mess with my data. People will turn to trusted brands as much as the law, people they know.*" The technologists discussed

regulation being framed not by the technology, but by the outcomes. Partly, this requires regulation to reflect the economic landscape of the dominant business models of monetising personal data. As Allan stresses:

"*So from the product manufacturers point of view, it's predominantly a matter of economics and they will continue to develop products in that way, either until the [oil] well runs dry or until regulation obliges them to stop or do things differently***" [Allan, Director]**

In moving towards regulating in terms of outcomes, not technology, again Allan discusses how this shift in focus by regulators could bring end user interests to the fore:

"*if you try and frame the regulation in terms of all those possible mechanisms [technologies for tracking user behaviour] you end up in a mess, if you frame it in terms of outcomes, to say look we don't really care how you are tracking the user but if your tracking of the user results in a loss of their rights, a loss of their self-determination or a violation of their privacy then you shouldn't be doing it. And if you are found to be doing it there should be a penalty*" **[Allan, Director]**

With such a breadth of potentially applicable regulations, understanding how state regulators will act and actually **enforce** these is essential. Within an emerging market like IoT, the lawyers expressed the importance of **engagement** by the regulators with technologists, to avoid knee jerk reactions and develop mutual solutions. Examples can be learned from past experiences in other sectors, as Duncan argues with crowdsourcing in the financial services sector:

"I think engaging with the regulators, if you look at the analogies within things like crowdsourcing in the financial services sector – when crowdsourcing first came along, the UK Financial Services Authority [FSA – former state regulator] went oooh, this is very difficult and could be dangerous and not sure if this should be allowed, and this is not going to be given regulatory approval to a process of actually engaging, the crowdsourcing companies engaging with what was then the FSA" **[Duncan, Partner]**

Beyond just engagement, the lawyers argue there needs to be regulatory pragmatism from state regulators. A more commercial mind-set from state

regulators can help emerging markets grow, as opposed to being more absolute when interpreting regulatory provisions. **As Magnus argues,** where regulation of an emerging market is too heavy, there is a risk technologies develop in alternative routes to avoid regulation "… *[if] you try and regulate hard, technology, it is like water, it flows around stuff, it will find a way. You need to be careful on the balance*." The UK Information Commissioner Office is often cited as a key example in this regard, unlike stricter regulators in other parts of Europe like Germany or Spain. As Innes argues:

"…whilst the techie developers have got to try and develop products with privacy in mind, at the same time, I think the regulators have also got to be quite commercial and pragmatic in their interpretation of the law and think, so how is this technology going to work if we are this stringent with our application of the law, and they've got to kind of keep applying it in a way that is commercial and doesn't completely stifle innovation. So I think it kind of works both ways, and it is going to be something that needs to be quite collaborative and continually develop as the tech develops" **[Innes, Associate].**

Recognising the challenges of effectively regulating an emerging market, we want to uncover what **solutions** our experts foresee as being useful in the IoT domain. **Greater interaction between technologists and regulators is a key requirement, either in terms of forums for discussion, or involvement in formation of laws and guidance.**

IoT crosses different sectors, hence we see desire from both communities for a forum, like EDPS IPEN[200] or AIOTI[201], that brings together actors, like technologists from different regulatory frameworks and levels of regulation (national, regional, international) to work through challenges of IoT. Findlay captures this point well, arguing:

"*A key challenge is identify what the key international forums are, bring together the constitutes stakeholders to have a meaningful discussion on it, establish things like the IPEN to work at a practical level, how do you design the solutions for identified risks. So I think that is part of it to*

[200] European Data Protection Supervisor Internet Privacy Engineering Network
[201] Alliance for Internet of Things Innovation

be honest, if you look at the connected car, ETSI[202]… IEEE[203], IETF[204], W3C[205] all setting standards on the connected car, there isn't a forum where they all come together, we have to have a way where we bring these constituent bodies together, with some extremely interested people in them, and sometimes we can't get them to agree so W3C and IETF couldn't agree on location privacy for example…but I'm afraid they have to alright…so I think that IoT exacerbates." **[Findlay, Consultant]**

Beyond actually getting stakeholders in the same room, another challenge the lawyers raise is how **official guidance lags behind the pace of technological change.** For practicing lawyers' official guidance, such as opinions of the Information Commissioner Office and Article 29 Working Party, are invaluable for advising clients. For technology designers, involvement in drafting guidance, for example with the ICO or A29 WP, can lead to guidance being a more responsive and agile mechanism for addressing regulatory change. **Even if the guidance is not specific to every technology, it can provide a sense of the issues and principles that need to be considered**. As Innes explains:

"*Certainly, if the Working Party [Article 29] or the ICO have said something is okay we are not worried about a client doing it (chuckles), so I think that kind of collaborative exercise is very important, that the regulators do work with people who are developing these technologies so that they can understand them and produce guidance and opinions that can then be followed so that people have a better idea of they need to be doing practically. If the legislation is so dated and so general, it's very difficult to interpret it without that kind of more specific regulatory guidance…*"

Both communities discuss the need for ways of sharing best practice, even relying on industry evangelists who will **raise awareness about what should and should not be done**. As Ewan states, "*it's not just sharing what the law is, but good design techniques, people would benefit from that a lot, how do you effectively anonymise data, at what point do you do that, when do you actually need to know, or be able to link the data to the customer or the user of the service*".

[202] European Telecoms Institute
[203] Institute of Electrical and Electronic Engineer
[204] Internet Engineering Task Force
[205] World Wide Web Consortium

From the technologists, we see a broad range of proposed solutions from **naming and shaming** of companies with poor security practices to **education** as opposed to regulation. Large scale IoT implementation **test beds** are a useful tool, as an opportunity of obtaining better understanding of problems, say in a city wide technology deployment, to help outline what to do, or what not to do. Other approaches include: **labelling products** with better information and a traffic light type warning, akin to food packaging, to help prompt user awareness; **open standards** that enable smaller players to gain market share; and **kite marks and certification** to show compliance with set security, safety, and financial standards. As Gordon argues, the kite mark and certification does not need to be complex, but just set a minimum level, like we already see with electrical safety marks:

"*Basically, a very simple checklist, would enable you to get a very rudimentary kite mark, that is not going to catch everything, but it may mean the people are engaged in that process, and the education that comes along with just realising they have to do that, might mean they might read the leaflet that you need to have an active CE mark, and anti-slavery mark as policy, and you don't do this or that. That feels like a way, but it could be a way to get more of this done quicker." [Gordon, Principal Consultant]*

To conclude, whilst we consider PbD, there are many other relevant regulatory frameworks for IoT, where compliance needs to be considered. In terms of enforcement, the commercial reality is a desire for regulatory pragmatism from state regulators. Experts argue a commercial, as opposed to absolutist, mind-set to enforcement may be necessary to help emergent markets grow.

That being said, in finding solutions to PbD compliance, experts argue for greater interaction between technologists and regulators, either through forums for discussion, or involvement in formation of laws and guidance. More approaches are needed to raise awareness of best practice, perhaps through evangelists or leaders in the industry. In terms of compliance for IoT, whilst law lags behind the pace of technological change, official guidance from the state is still useful for lawyers advising on compliance with new technologies, as it gives a sense of the issues and principles that need to be considered. Lastly, the technologists have a range of solutions to doing PbD, including, naming and shaming companies with

bad practices, tests bed for exposing problems in large scale IoT projects, product labelling, open standards, kite marks and certification for compliance**.**

Working towards solutions for 'user centric regulation', whatever they may be, requires understanding of the respective roles that lawyers and designers play in this domain, and how they might come to interact. In this final section we consider their **respective roles, relationships and their interactions**.

4. The Relationship Between Lawyers and Designers

Role of Lawyers in User Centric Regulation

Beyond the respective roles lawyers and designers play in realising user centric regulation, the relationship between them is also important to unpack. Accordingly, our structure in this section follows those three elements, and we begin by looking at the role of lawyers in user centric regulation.

Firstly, one role of practicing lawyers is **reminding their clients of their compliance obligations.** A key element of this is raising awareness as **early as possible**, but again, this can be a challenge for smaller business lacking financial resources. As Ewan argues: "*I think the most practical issue [of doing PbD] is actually getting in front of those people. Actually getting them to be aware of that issue, that is a big challenge about how you reach out, how you get those people thinking about it*". [Ewan, Partner]

Many compliance issues arise because privacy was not considered early enough, and the lawyers stressed compliance is easier when privacy is considered **before something has actually been built**, instead of retrofitting a solution. However, deciding the precise moment at which legal advice should be sought is tricky, and sometimes advice is being sought 'too early', (although this is good as it shows a growing awareness of the importance of thinking about privacy early on). **Lawyers need designers to provide key information about how the technology will work, what data it will collect and so forth to be able to advice effectively.** As Innes shares from her practical experience:

"*I think once they've got to a point that they have a good understanding about how the proposed tech is going to work and how it is going to use data, if they can explain this is the data we are going to collect, this is what we want to do with it, this is where it is going to be stored, this is going to be who can access it, if they can answer all these kinds of questions, then we can start advising them. If they haven't gotten to the stage of thinking about data collection and what they are going to do with it, it is more difficult. They need to have a basic prototype of what they are looking to do, in order for us to be able to start advising them at a practical level.*"

Secondly, **lawyers have to balance compliance against creativity**. **They cannot take an absolutist approach by saying the risks of a new technology are too great.** Instead, like the state regulators described above, they may need to take a more market orientated perspective, where some risk is tolerable in the short term. As Innes states "*It can be quite tricky because we can be the kind of no guys…but we have to find ways of addressing it so that it is more of a yes, but you need to do this, or yes, but you're only going to be achieving a 7 out of 10 in compliance for your level of risk.*". That being said, the type of data and context of collection can shape no-go areas in terms of compliance. Sensitive health data from medical devices would require a higher level of compliance than less sensitive or detailed data about office heating obtained from a smart thermostat.

Such an exercise of defining red flags highlights another element of a lawyers' role: the **risk advisor.** They need to advise clients on what level of risk they face in satisfying (or not) compliance requirements. Ultimately the end decision is down to the client. In particular, they need to factor in **interpretation** of the law and the likelihood of the state regulators actually **enforcing** it. As technologist Allan put it, design responses to legal requirements will turn on risk of enforcement, but often regulators will be unlikely to challenge business practices:

"*So if the developer comes to you and says well write me the functional requirements for the IPbD aspect of this [a personal data driven app]… that is pretty tough to do. You might say data minimisation, or you might say limited data retention periods, but I have yet to encounter an organisation that does limited retention periods… [but] what are the chances of the regulator actually showing up and saying, 'how long have you had that piece of data, do you really still need it…oh okay then'…even if the regulator did turn up and audit you and you said, 'yes we do*

legitimately do need that because we use that to manage the ongoing customer relationship', it would be a pretty brave regulator who said that is an unacceptable reason." **[Allan, Director]**

Furthermore, the experts recognised state regulators may lack resources to take action, like the ICO, even if they wanted to. This has to be factored into the risk. Beyond lawyers reminding of compliance requirements and acting as risk advisors, they provide a **legal process** for working through the issues a new technology poses. Often lawyers support designers by asking very practical and quite traditional questions. This is to ensure the correct documents and processes are in place for compliance. Despite novelty of technologies, this may involve mapping and understanding the impact of different regulatory environments like safety legislation, intellectual property law and contracts defining ownership over outputs and licensing agreements for market control.

With data protection, for example, many of the practical questions raised by lawyers included: What personal data is being collected? Should it be collected? Are users being informed about this? What information should they be given? What is being done with the data (eg marketing)? What information needs to go into contracts and consent mechanisms to reflect this? If new data is being collected, how are users consenting and being notified about this eg with location data? If data breaches occur, what has gone wrong, and how can they respond to complaints from the ICO properly?

These questions become complicated for multinationals who have to deal with multiple jurisdictions in **achieving compliance for a technology globally**. Again, absolute compliance may not be possible and there often have to be lawyers working in different jurisdictions, with technologies being tweaked to become compliant. As Innes states:

"*a lot of the issues we come across is a lot of these technologies are being released around the world and we tend to work with local lawyers in different jurisdictions so we usually work with someone in the US, people in Asia, people in all different parts of Europe, and the problem is obviously that the law isn't the same everywhere and it is not commercial for these developers to develop tech that could comply everywhere …these big tech companies might have to have a specific feature for*

a specific country because they just can't get around a particular law in that country that maybe doesn't matter anywhere else. And it is a balancing exercise, often we talk about achieving 7 out of 10 everywhere, rather than 10/10 in some countries and 2/10 in others..." **[Innes, Associate]**

Similarly, designers in multinationals cannot be expected to know how the law differs globally, as Jess expressed **"**I was *called in to advise on what the legal position would be on one proposed product, they were all ready to go with that product, there were no problems with that in the US, but I said, you can't do this in Europe at all… the product research and development had been done in the US, and you know, you can't expect US engineers to think about Turkish law.***" [Jess, Senior Researcher]**

To conclude, the role of lawyers is largely as risk advisers. They need to remind technologists as early as possible of compliance obligations, but a key challenge is getting in front of them especially SMEs/start-ups. Determining when is early enough in the development process is a challenge. The lawyers state that to advise appropriately, they need designers to be at a stage of development where they can provide key information about how the technology will work and what data it will collect.

Lawyers have to balance compliance against creativity by not stifling innovation by being too risk averse, but equally, having parameters where non-compliance is not tolerable. This threshold is often guided by the type of data and context of collecting.

As risk advisers, lawyers inform clients of the level of risk they face based on interpretation of law and likelihood of state enforcement, but ultimately leave decisions to designers. This involves systematically working through practical questions around the technology to understand to what extent it differs from existing systems and to put in place compliance mechanisms, often globally.

Role of Designers in User Centric Regulation

We now turn to the role of designers in user centric regulation. The lawyers feel designers have a **critical role to play in compliance**, as they are central to protection of fundamental rights. They can actually **instantiate the legal principles in practice**, through technology and mediate an end user's actions, perhaps even more so than law, as Blair explains:

"*Law in itself, other than as a conceptual or philosophical level is fundamentally useless when it comes to preserving rights, it's use is acting as a behavioural nudge in my view, into encouraging people to develop technologies and systems and processes that operate in a way that protects either fundamental rights, or non-fundamental but still important rights.*" **[Blair, Managing Director]**

Similarly, other lawyers argued **designers already have a role as regulators**, and even where law is not involved, regulation is still ongoing, because design decisions are consciously being made that have regulatory impacts. As Campbell argues:

"*it's not a case whether they'll have a role in the future [in regulation], they are already doing it… it is happening. These design choices are being made already, so the question is what influence should be brought to bear on these design choices, but if no legal influences are brought to bear, there will still be acts of regulation, minor acts of regulation taking place all the time… The other is the thing of the designer actually as a regulatory actor in terms of their relationship with the user, whether there is a legal requirement to or not, designers will face choices as to for instance, their data that is collected, whatever about the security under which it's held, how its transmitted, how it's used, things don't necessarily collect data by accident. Someone has made a call as to what data is to be collected or what is to be maintained even if it is just captured as part of a stream, you will face a design choice, plenty of devices will collect data in the course of use….*" **[Campbell, Reader]**

In terms of how technologists feel about interacting with law, there are broad variations in perception. Some argued **law is a useful stick to help prompt action**, as Jess captures "*as a technologist, if you are trying to persuade another part of the company that they need to do something, you can give them all sorts of technological arguments, but if you can say, 'it's the law' then they will suddenly start listening to you so it's a very powerful tool to have in your armoury.*" **[Jess, Senior Researcher].** Others raised the

importance of going beyond just legal compliance, towards thinking about **ethics** too, however, unlike with law, motivating to do this was reflected as a problem. Scepticism emerged about the grasp policymakers have of IoT, and the huge gap **between law and technology resulting in lawyers lagging behind technologists by some time.** Gordon shares his experience:

"The legal profession feels like it is behind the curve, but at least it is on their radar now. That would be a fair summary for me. The technologists and product guys right at the bleeding edge, you've got the service provider guys slightly behind them, then you've got consumer stuff behind that and then in 4th place you've got that (law) and I think the timescale from front to back is that the innovators are probably I would say 5 years ahead of where the regulatory side is. Legal side is 5 years behind cutting edge, that is what it feels like to me." **[Gordon, Principal Consultant]**

Some technologists respond to **legal values in a more provocative manner**. Legal values are not absolute, and accordingly need to be understood in different contexts. The design prerogative of transgression is interesting as an approach to surfacing legal values, not in order to do compliance, but instead to have a discussion about legal values and their impacts. This more reflective, critical approach is discussed by Iain who states:

"*if I don't expose it [transgressions], then we can't have a conversation about it, so there is a design imperative to explore transgressive activities or design approaches… My interest as a designer isn't to lock these [behaviours] down based on an old model, but more to reveal and understand what type of animals we are dealing with. We like to exploit, we are designers, we want to build things that help understand the condition of ubiquity.*" [Iain, Professor]

This point leads us nicely into discussions about **variations in the design process**. For some designers, it is about provocation and reflection, but for others, as we see with lawyers, the process involves asking very practical questions about the **requirements, constraints and needs of a system.** Gordon clearly lays out some of the requirements to think about when building a new technology: "…*how much is it going to cost to build this thing and how much will people pay for it, what is my power budget, my data budget, how much processing do I do, have I got external connectivity, can I send the data to the cloud to be processed a lot cheaper than having processing online, what is my comms, have I*

got battery life, am I launching it where there is a particular network coverage for this technology (say in the home) …" **[Gordon, Lead Consultant]**

Importantly, there needs to be questions about **where in the design process legal responsibilities emerge**, and the design methodology being used can impact this. Often the design model is to keep **system design and compliance separate**, where legal issues are considered after the product is already built or designed. Added to this, within global multinationals, the nature of the IoT supply chain adds an extra layer of complication where work is distributed across many departments and countries. As Jess explains,

*"…you can have a really really long supply chain because you start from the basic hardware to slightly more involved hardware to firmware to generic software to specialised software and networking in that. All of those may be done by different teams in different continents, maybe not continents but you'll have one part of the product that is done a small team in China, and then the next part done by a small team in Indonesia, and the next by a small team in California. It may be that they will have lawyers they can speak to, but they will be company lawyers as opposed to specialists in those elements that might be relevant. [with] these teams one problem with security and safety of IoT is that it is quite common to find, when you find a security issue, it is because of a misunderstanding or mismatch between two of the teams, and I can quite see that happening with law…that is a difference in the production process for the IoT compared to traditional computing products.***"**

Similarly, within the supply chain, the diversity of technical actors, each with their respective disciplines and languages poses challenges, especially for security. This is interesting as it shows even on the technology side there are big challenges to be overcome, before even thinking about how to get technologists and lawyers to work together. Magnus explains the big disciplinary gaps within technical communities in the IoT supply chain:

"*so the people doing the firmware for the device, engineers putting in the cellular modems for the connection, the ones working out how to do the web service and the protocols that send stuff back, the ones who are designing the databases and security for the databases are all trained in totally different disciplines and you get them in a room together and they don't speak the same language*

and that is one of the biggest challenges we've got to face going forward, we are training people who are very specialised and nobody or hardly anybody understands that end to end experience."

To conclude, lawyers perceive the role of designers as key as they can instantiate legal principles in practice, and they argue designers already have a role as regulators, because design decisions they make have regulatory impacts

How designers perceive law shapes their interaction with lawyers. On one side, they see law as valuable because it prompts action, unlike ethics where aspirations exist but action may not follow. However, on the other side, technologists feel the lawyers are quite far behind the bleeding edge of technology. Beyond these, practically, differences in how technology is built and various approaches of designers' shape how legal concerns manifest in practice. Some focus on practical questions about the technology, like lawyers, others focus on using technology to provoke reflection on legal values, not for compliance but to create a societal conversation around them.

Often legal compliance and design are kept separate, especially in larger companies where the development of new products is spread globally across different departments and countries. Even within the technical community, there can be very wide gaps between the language and approaches of different specialists, an additional factor to consider in the interaction of lawyers and designers.

We now turn to more detail on the interactions between technologists and lawyers below.

Interactions Between Lawyers and Designers

Lastly, we reflect on the nature of interactions between lawyers and designers as discussed by our experts. We start by considering the experience of practicing lawyer Blair as he explains how he finds lawyers and designers interact in practice. The interactions during advice giving can be broken down into the following steps:

- **Process of understanding the goals of designers** – for example making a product more usable by using data analytics to interaction with the interfaces - *"how can I make this product the most usable it can be, and at some point you're going to have to say I actually need user data, I need to know how a user is navigating through and app, and what screens they spend the most time on, or if they miss a screen and need to tap back, I need that volume of data to analyse'"*

- **Lawyers presenting responses and advising about risks** – for example the need to inform users of this analytics, put in place opt in consent mechanisms, and how to communicate benefits to user -*"talk to them and say, that is a secondary use of their data, how are you going to be talking to users about it, and how are you going to persuade them that they probably need to opt in to give their consent, to be tracked like that, and you know what, realistically most people aren't going to do so because they will feel that somehow they are being spied on.*"

- **Lawyers proposing solutions that balance goal and risks** – for example opt in consent, little data but low risk, opt out consent, more data and risk, no consent, lots of data, high risk – "*you go for opt in consent, or consent, quite bluntly, and rely on the fact that you're not going to get much data, or you go for an opt out approach, and you take the risk of not being compliant, but getting some data, but you know what some people might complain it's opt out not opt in, or you don't talk to people at all and you just go on and do it, because, you know if you don't tell them perhaps they won't find out, and if they don't find out, they don't complain***"**'

- **Designers and lawyers negotiating an outcome** – for example negotiation between lawyer who aims to ensure compliance and designer who just wants to make a better app – "*But either of those last 2 options are*

unlikely to be legally compliant and carry a degree of risk, and you've probably got people going, 'what the hell do you mean, all I want to do is make a better app, why are they going to complain about making it better' – that is a difficult kind of situation to explain to someone so engrossed in making things better, they don't see the bigger privacy picture. Or is that just a lawyer being a pain in the arse, pointing out legally what is wrong, when in fact the vast majority of consumers will not care."

Whilst this interaction shows a degree of conflict, interactions between technology law and design communities may not be as strained as might first appear, and indeed, there could be significant crossover in their respective mind-sets. Blair, argues they both try to work in a very procedural, consistent and logical manner. As he puts it:

With the "*issue of Engineers vs lawyers if I can put it that way, in some senses I think there is a great deal of similarity between the way a good engineer thinks and the way a good lawyer thinks. To take a very simplistic example, when you look at a contract, it should very much be like a computer program – it should be readable, it should have a series of definitions that can only do one thing to you, but avoid you repeating yourself, like a library of routines, and then it sets out a process for doing things with a series of actions of what happens if the processes are not followed. It should make sense, what happens is that programmers have it a lot easier because you run it through your compiler and it will hopefully tell you which bits are not going to work or are erroneous, where in the legal system the compiler sense is the judge, which is a far more expensive way of dealing with things*" **[Blair, Managing Director]**

Importantly, for our lawyers, there has to be a **complementary approach between both technologists and lawyers**. The nature of privacy by design is such that **the role of designers is growing, but lawyers will always be necessary**. As EU DP law turns to designers through PbD, the relationship between legal practice and technology designers may shift, with greater responsibility for designers to engage with legal issues, and even take a leading role. Ewan unpacks how the interaction between the two might play out in practice:

"[*under the GDPR approach] system designers, product architect type people, have a much greater role to firstly when they're designing technology, in particular IoT, to actually understand at the*

outset the privacy issues so they can adhere to things like PbD when they are building the system, and secondly they are the ones who are probably best placed to take the lead when drafting the process or privacy notice that actually explains what is being done and how that data is going to be used. I don't think that is something a lawyer can lead on so much anymore" **[Ewan, Partner]**

A barrier that needs to be overcome is **upskilling of both communities** around the respective disciplines so that they can interact more effectively. There is a need for better skills from both sides so they can interact more effectively. As Blair puts it:

"*what I think we are going to need to see is either there a rise of lawyers who are more skilled at dealing with technical people or a rise of technical people who are more skilled at dealing with lawyers, whichever way round you want to look at it, but there is going to have to be an interaction between the two. Because, law remains the vehicle by which we regulate, and technology is the output, that consumers are buying… so the lawyers may be able to advise on what the regulatory framework says and might be able to help those drafting the law to say what the law should be but at the end of the day the law in my head can only have a practical impact if it is enacted through the technology, and the technology is built in a way which complies with those legal principles*" **[Blair, Managing Director]**

To conclude, by looking at examples of interaction we get insight into the different elements i.e. understanding the goals, investigating what designers are aiming to do; how lawyers respond to this goal with advice; the options designers can choose to follow, and lastly, negotiation of an outcome. In summarising how the roles may change in these interactions, we see a shift to a greater role for designers in leading on compliance issues. Partly led by changes in the law, there is always an important role for lawyers in advising, but we see the emergence of a complementary role between both parties. Increased engagement between their respective fields can help develop strategies for supporting their corresponding roles.

5. Aligning the Perspectives

Having analysed various practicalities of doing privacy by design for the internet of things, we now position our findings within the narrative of the overall thesis. This provides us with a richer understanding of **how** to align these two communities in the practice of **doing** 'user centric regulation'. It also informs our final Part, which looks at how to support designers engaging with data protection law, by using information privacy by design cards. For clarity, we cluster our analysis under the banners of different perspectives:

- Business perspectives;
- Regulatory perspectives;
- Technological perspectives.

Business Perspectives

The first range of perspectives stem from business realities of doing PbD for the IoT, and we present three positions to be considered in order to do user centric regulation.

Perspective 1: Recognising the impact of differentiated resources on technologists' ability to engage with regulation.

The business reality is SMEs and start-ups are focused on investment, not compliance. Even if the motivation exists to consider law, lack of resources prevent meaningful engagement. In contrast, bigger firms have financial and organisational resources to address compliance in a systematic, comprehensive manner, globally if necessary. They also have greater familiarity with regulation in a particular market, for example telecoms, than start-ups or SMEs. Accordingly, doing privacy by design needs to reflect the differentiated resources available for technologists to act and engage with the law in the first place. Under Article 25 GDPR (2016), demonstration of compliance includes use of accreditation, internal policies and various technical and organisational measures. Without resources providing stability to even think about legal compliance, never mind putting in place measures, PbD for SMEs and start-ups is a significant challenge.

Perspective 2: Understanding the business models and motivations for engaging with compliance in the emerging IoT market.

Our data shows the dominant IoT business models are to create a cheaper product but to raise revenue from monetising the personal data. This involves collecting as much data as possible, partly because technology allows this, but also to stockpile it for later use and to find new applications. Within the industry, there is a desire for more data, to learn more about the product use, to find interesting data and refine the business strategy accordingly. This is in direct conflict with many provisions of DP compliance, for example, Article 25 explicitly states data controllers should minimise data collection, avoid keeping unnecessary data and provide means for the data subject to monitor processing of data. Such business models are at odds with these measures, and any goal of moving PbD from rhetoric into practice needs to engage with this commercial reality. Turning to motivations within the industry for change are one way of doing this.

Currently, the practical motivations for organisations to engage with compliance and PbD are lacking. Rather than the drive being compliant as an end in itself, protecting brand and reputation due to fear of hacks, scandals and user disquiet around practices are more compelling. However, any change needs to be balanced against monetary costs, lack of enforcement and competitive disadvantage stemming from increased costs by being compliant when competitors are not. Other drivers include an internal code of ethics, brand values, desire to become a better company and build a better product.

Within UCR, structuring reflection and action by designers on the nature of their legal and ethical responsibilities to users is key, and what quantifies a better product may be part of this. If a better product is a more privacy compliant, ethically sound product, developed in response to consumer interests, then this is a route to prompting change. Practicing lawyers already take this tact, as they pitch PbD and compliance to technologists as a type of branding that can be a viable selling point. In any case, PbD in practice needs engagement with how business models are

shaped (or not) by regulation, and how to utilise motivations for technologists to interact with compliance.

Perspective 3. Supporting the Changing Role and Interactions Between Lawyers and Technologists in Regulation

As we argue in Part I, UCR involves an explicit alignment of technology law and design communities, where there has been a turn in technology regulation to design, and a turn in design to social concerns. How this manifests in practice depends on how IT law and HCI communities understand their respective roles. This requires critical reflection and development of practical means to support each other as they move forward together.

Despite the new role of designers as regulators, the role of lawyers is not going away. They act as risk advisers, reminding technologists of compliance obligations as early as possible. How early is key, and in order to advise effectively, the lawyers need designers at minimum to provide key information about how the technology will work, what data it will collect and so forth. Differences in the role of designers and how technologies are built will shape how legal concerns manifest in practice. With the former, some designers' role is to address practical questions about the technology, like lawyers, others focus on using technology to provoke reflection on legal values, not for compliance but to create a societal conversation around them.

With the latter, legal compliance and design are often kept separate, especially in larger companies where the development of new IoT products is spread globally across different departments and countries. With SMEs and start-ups, again resources are tight hence even getting in front of them to provide legal advice is not practical. Lawyers and designers may have differing goals where the latter want to build a better system and the former to ensure legal compliance. Such debates need to be resolved by negotiation between the two to find optimal solutions, and doing this as early as possible is ideal.

When they do interact, lawyers have to balance compliance and creativity, taking care not to stifle innovation by being too risk averse. Equally, they need parameters

where non-compliance is not tolerable, often guided by type of data and context of collecting. Lawyers as risk advisers determine risk through legal interpretation and assessing the possibility of state enforcement. They present this to designers, who make the final decision on acceptable levels of risk.

A complementary role between both is emerging, where the role of lawyers continues to be risk advisers, but designers increasingly have a bigger role in thinking about technological compliance, and lawyers advising accordingly. In terms of mutual attitudes, lawyers value designers because they can instantiate legal principles in practice and feel they already have a regulatory role due to regulatory impacts of design decisions. Designers perceive law in a more mixed manner, where on one side, law is valuable because it prompts action, unlike ethics where aspirations exist but action may not follow, but lawyers are often seen as being quite far behind the bleeding edge of technology.

UCR needs greater critical reflection of the mutual roles designers and lawyers play, and a shift past the current separation of compliance and design. Whilst lawyers seek earlier consideration of legal issues, we argue there needs to be practical strategies to support increased engagement between these two communities, especially for SMEs and start-ups.

Accordingly, building on these business perspectives, we propose our system for supporting PbD in practice using privacy by design cards, which are considered in detail in Part IV. This tool looks to support SMEs lacking in house resources, and helping designers engage with legal concepts in a more accessible way. Furthermore, we use the cards to explore how technologists respond to data protection law and compliance requirements in the context of their own work, building a system with various constraints and users to consider. They help us understand in more detail how PbD can manifest in practice, how legal issues impact different sized organisations and their engagement with law.

Regulatory Perspectives

The second range of perspectives stem from regulatory realities of doing PbD for the IoT, and we present three positions to be considered in order to do user centric regulation.

Perspective 1: Contextualising Privacy by Design and Legal Values

We find that whilst lawyers support PbD, in practice, technologists are uncertain of what it entails. Critical reflection on PbD is important, considering how it complements existing legal mechanisms, but practically, legal language poses a barrier to designers. This can be uncertainty around both legal terminology and the underlying legal concepts for example legislative process, jurisdiction or designing for values like consent or privacy. It can also be because designers want to build technologies with certainty, but legal concepts do not lend themselves to this. Uncertainty around regulatory enforcement complicates matters further. Whilst greater cross community dialogue can help, designers need more systematic understanding of what the law requires, but such exploration cannot be complex and long as it has to fit within existing design processes, often constrained by time or cost. Furthermore, **even within the technical community, there can be very wide gaps between the language and approaches of different specialists.**

Like with IoT, PbD cannot be understood in the abstract, and instead focusing on how it manifests for specific sectors, contexts and technologies is important, instead of trying to frame it at a general level. This aligns with a key argument of UCR which is need for a turn to the context of technology use to give meaning to regulation in practice. For designers and lawyers to move forward together, a situated understanding of how regulation through user rights and designer responsibilities materialise in practice is key. The proximity of HCI designers to users, and the range of tools and approaches they possess to understand user interactions with technology in context, are one way they can obtain legitimacy as regulators. However, firstly law has to be made more accessible to non-lawyers, in order to sensitise them to its goals and values. Again, our cards are a response to this need.

Perspective 2: Finding the Richer Picture of Regulatory Challenges

As we saw in Part II, IoT poses a range of challenges for end user DP rights, particularly around controlling flows of personal data, and from inadequacies of existing notice and choice consent mechanisms. A turn to practical experience uncovers deeper concerns around the IoT, providing a richer picture of the regulatory challenges in situ. This helps situate how designers can respond in doing UCR too. Some challenges mirror existing understanding of why IoT is problematic to regulate. These include, device and interface heterogeneity complicating consent mechanisms in IoT ecosystems, or complexity of IoT data flows frustrating establishment of responsibility for providing users control over inferences and prejudices of data sharing. Other findings add new dimensions to our understanding of the regulatory context. These include, the role smart phones as mediating devices in IoT ecosystems for obtaining consent, and the fiction of freely given consent where the alternative to agreeing to a new contract is for a user to box up a costly IoT device. Furthermore, a turn to practice shows that whilst IoT poses challenges for compliance, such as with international data transfer and storage in the cloud, on another, the IoT can increase help compliance, for example increasing transparency of data processing, reducing the need to rely on legal rights like subject access requests. This informs the context of UCR, and how designers can respond to regulatory challenges, for example, redesigning consent mechanisms involving smartphones, or other mediating devices to increase transparency in the user experience trajectory.

Perspective 3: Managing Risk and the Realities of Enforcement

Our experts express a desire for state regulators to be commercially minded, avoiding absolutist interpretations of law in order to give room for an emerging market to grow. There are a range of challenges for IoT compliance partly due the embryonic nature of the IoT market, the heterogeneity of devices and the lack of industry standards. In practice, technologists are engaging with many other regulatory frameworks beyond DP law such as product safety, information security or intellectual property laws. Assessing likelihood of regulatory enforcement and

risk of sanctions is an important consideration. However, as the law lags behind the pace of technological change, this is a tricky analysis. Mechanisms are needed to help understand risks, with a key role for awareness raising. At a high level, greater interaction between technologists and regulators is necessary, and this can be achieved through more cross-sector forums for discussion, and greater involvement of technologists in formation of laws and guidance. At a practical level, state guidance can assist with new technologies, flagging key issues and principles to be considered. Education, sharing best practice, and leadership from evangelists or senior figures in the industry are other important elements.

Again, PbD expressly calls on designers to be involved in regulation so they need to be supported and to engage with law in a structured, accessible manner. Our cards are a response to these regulatory perspectives, a tool to help designers that translates law into a more comprehensible medium, to help designers engage with the nature of the law, build understanding and respond, with user centric interests at the fore.

Technological Perspectives

The third range of perspectives stem from technological realities of doing PbD for the IoT, and we present three positions to be considered in order to do user centric regulation.

Perspective 1: Communicating the Relevance of Law to Designers

Whilst PbD may involve designers in regulation formally, the relevance of law to their work needs to be contextualised. A key support mechanism for engagement is translating law into more accessible form for designers, such as creating tailored codes of practice and actionable guidelines, training or support websites, and keeping the legal processes engineers need to follow as simple as possible. Other strategies include promoting a culture of risk awareness through leadership in organisations; getting designers on board by putting law in the context of their own lives and work; and by thinking about how legal risks might endanger company values. A specific area of support is awareness raising, and practical guidance for SMEs who lack resources of larger organisations. Within the start-up community

there is little awareness of legal obligations. Again, this drives our approach in part four, to better understand how to translate law to designers, and the challenges SMEs face in practice, and how best to communicate relevance of law and engage them.

Perspective 2: Appreciating Conflicting Agendas

PbD in practice needs to incorporate an appreciation of the conflicting agendas designers may be subject to. Designers will face pressures from different stakeholders who will want them to design the system in ways that address their interests, for example business strategists. They have to balance these agendas, hence determining the organisational or technical safeguards required for compliance involves a range of stakeholders

Perspective 3: Application Led Framings of Technology

Instead of arguments about where the margins of IoT lie, or what networking approaches define the technology, the **applications** are key. This moves away from a vision led approach, committed to principles of what is or is not IoT, instead focusing on specific applications.

Importantly, with applications come contexts of use and importantly, end users who have various needs and interests. By considering this level, a richer, situated vision of IoT, can emerge, looking at the practices, interactions and relationships end users have with technology. A key element of user centric regulation is reflecting on the societal implications of technology, considering ethical responsibilities, and as we argue, considering the legal implications. Accordingly, these applications and contexts provide framing for how regulatory issues impact users, and responding accordingly.

Again, these perspectives highlight the need to help support designers to understand regulation and their role therein. In part IV, we use our cards as a design tool to see **how** designers navigate around legal concepts. Building awareness of the conceptual barriers and strengths designers have with regulation and law allows

us to develop a richer picture of what is needed to do PbD, and UCR more broadly, in practice.To begin this process, we now move to Part IV where we introduce the information privacy by design cards.

Part IV Design Perspectives: Information Privacy by Design Cards

Overview

As we have explored, PbD explicitly involves technology designers in regulation. They need to consider information privacy risks of a technology as early as possible in the design process, ideally before anything is built or comes to market. However, doing PbD in practice is complex, as we see in Part III. There are a range of motivations for these cards, but a key driver is to create a tool that supports designers doing PbD. Our response, we call '**information privacy by design cards**'. These have been developed to translate the new GDPR into a more accessible form, to engage designers with law in a structured manner. We have tested these cards within a range of industry organisations, in order to better understand the practicalities of PbD in different settings. We also investigate the utility of the tool, asking those who will use it for feedback. Before delving into the detailed findings, we outline some background on physical playing cards in research and the methodological approach.

Whilst we present cards as an instrument, the **underlying driver is to find tools to communicate legal principles, concepts and values to technology designers in a more accessible manner**. Accordingly, cards are just one medium and approach. They are appealing due to their established lineage within the HCI community. They also have an aesthetic novelty due to being a tangible artefact. Nevertheless, depending on needs of the design community, other mediums will develop. The requirements of such tools needs to emerge between legal and design communities. We also want our tool to contribute to that process, understanding the challenges designers face in doing PbD. Indeed, there is further work beyond this thesis to be done on critically investigating other mediums to effectively communicate law to the design community. Accordingly, the motivations are around finding tools that help designers engagement with law, not just through cards per se. To summarise our motivations, we wanted to create a tool that does the following:

- Supports designers' engagement with data protection law in practice.

- Makes legalese less complex and more accessible to non-lawyers. This is necessary to help inform designers of legal requirements in order to inform and shape their design responses.

- Helps raise awareness of why law is relevant to designers in a structured manner.

- Helps us explore the conceptual and practical challenges designers face in doing PbD.

- Builds our understanding of where designer strengths exist in PbD, and where greater support is needed.

- Investigates how designers engage with and navigate around legal concepts in practice, especially in different organisational settings.

- Prompts reflection by designers on their legal and ethical responsibilities to users.

We now turn to the development of the information privacy by design cards in Chapter 8.

Chapter 8. Developing the Information Privacy by Design Cards

Physical cards were chosen as they have an established lineage in HCI as a tool for sensitising designers to new, complex ideas in a structured way.[206] Card based approaches go by a range of names like 'envisioning' (Friedman and Hendry, 2012), 'pattern; (Wetzel, 2014), 'ideation' (Golembewski and Selby, 2010) or 'methods' cards (IDEO, 2002), but broadly they all aim to help structure thinking around complex themes in the design process. The approaches for using cards vary and crossover greatly. Some examples include, playful game mechanics to raise awareness or to educate (Denning et al, 2013b; Barnard Wills, 2012), more reflective, critical approaches (Belman et al, 2011; Friedman and Hendry, 2012; Denning et al, 2013a) and for enabling creativity (Wetzel, 2014, Know Cards, 2016, Golembewski and Selby, 2010). They have been used in a variety of contexts including:

- General creativity in design (Golembewski and Selby, 2010);
- Computer security threats (Denning et al, 2013b);
- Computer security education (Denning et al, 2013a);
- Use of methods (IDEO, 2002; Mackay, 2002)[207];
- Mixed reality game design (Wetzel, 2014);
- Human values in games (Belman et al, 2011)
- Privacy (Barnard Wills, 2012);
- Programming language education (Varianto 25, 2015);
- Sustainability (Innovate UK, 2016);[208]
- Internet of Things device design (Know Cards, 2016);[209] and lastly,
- policy design methods (Silk, 2007).[210]

Conceptually, our cards are primarily inspired by Friedman and Hendry (2012) and their work on value sensitive design envisioning cards. Their cards aimed to bring

[206] See Emergent by Design website for a list of current card based design approaches - https://emergentbydesign.com/2012/10/25/21-card-decks-for-creative-problem-solving-effective-communication-strategic-foresight/
[207] IDEO 51 Method Cards Website https://www.ideo.com/work/method-cards
[208] See Innovate UK Horizons Website http://horizons.innovateuk.org/about
[209] See Know Cards Website https://know-cards.myshopify.com/
[210] See SILK Website - http://socialinnovation.typepad.com/silk/silk-method-deck.html

specific human values into design, like sustainability or psychological well-being, through a set of physical cards. Used in workshops with groups of designers, the cards prompt discussion around human values in the design process. As they found, "*robust like a pencil, the envisioning cards were designed to be a versatile tool, useful for many design processes: ideation, co-design, heuristic evaluation, critique, and more*" (p1148). Our goal was to create a deck of cards to bring legal values into design, namely around information privacy law (DP).

The cards have been through a number of different iterations, with the first prototypes being designed, tested and results presented in 2015 (Luger, Urquhart, Golembewski and Rodden, 2015, hereinafter - CHI, 2015).[211] We discuss how they were created and sketch findings from the exploratory studies with the prototype below.

However, within this Part, we focus in much greater depth on the most recent iteration. As the GDPR will be enforced across the EU from May 2018, strategies need to be developed to respond to compliance requirements like PbD. The new deck is more comprehensive, focusing on the full GDPR, instead of the narrow set of issues we considered with the prototype. We reflect on the challenges of translating complex legalese from the GDPR into 'bite size' chunks of law for a more comprehensive deck of cards. We present detailed findings from a range of workshops conducted with technology designers from three different organisations:

- A large global media firm ("MOZ");
- A small technology businesses trade association ("SBA"); and
- An innovation network centre for SMEs/start-ups ("INC").[212]

---

[211] E. Luger, L. Urquhart T. Rodden, M. Golembewski (2015) Playing the Legal Card: Using Ideation Cards to Raise Data Protection Issues within the Design Process, *Proceedings of ACM SIGCHI 2015*, p457-466. See press coverage in D Pauli (2015) Hey devs! Confused by EU privacy law? Pull out the FLASH CARDS, *The Register* at http://www.theregister.co.uk/2015/05/06/devs_confused_by_eu_privacy_law_pull_out_the_flash_cards/. This work led to a US National Science Foundation EAGER Grant of $175,000 to replicate our work in the US. A project involving Microsoft Research, Intel, University of California, University of Nottingham and Tandon School of Engineering, New York University was setup to do this.

[212] Our new cards reflect the entire GDPR, and the extension of the deck from the original version. The work has been funded by a joint project between Horizon Digital Economy Research Institute, University of Nottingham and Microsoft Research, Cambridge. For details of how the project has

These workshops provide us rich insights into how designers engage with legal concepts in practice, and what is necessary to do PbD, and consequently UCR, in different types of organisations.

A range of methods have been utilised in the development and testing of the different iterations of these cards. Questionnaires, focus groups, practical workshops, card sorting exercises and informal discussions have all played a part. In the interests of space, we focus on key elements here. All empirical studies have been conducted following approval from the University of Nottingham Computer Science Ethics Board. All participants have been given information about the study and have provided their written consent. Below, we provide more detail on the prototype cards.

Prototype Cards

The **scope and language** of the initial prototype deck (CHI, 2015) was informed by **a small, detailed legal questionnaire** run in summer 2014. It was conducted with **seven** academic legal experts (professors, lecturers and PhD researchers), selected due to their specialism in data protection law. The questionnaire was highly targeted, distributed to participants selected from our academic network, who completed it on digital survey service Qualtrics. The short questionnaire used a combination of 10 point Likert scales and open-ended questions to question experts about the **role of technology designers in DP regulation**. To frame the questionnaire, we used four key areas from the draft GDPR (Smith, 2013): 24 hour data breach notification, the right to be forgotten, privacy by design and explicit, informed consent.[213] These are linked to regulatory challenges of ensuring end user

progressed see the Horizon Project page at http://www.horizon.ac.uk/project/privacy-by-design-cards/ and Lachlan's Research Blog at https://lachlansresearch.wordpress.com/. Reflecting on my role, I've primarily led the project, with oversight from Prof Tom Rodden. Neha Gupta has assisted me in the project, particularly with practicalities of running workshops and transcribing data. Ewa Luger and Michael Golembewski provided initial guidance, and Michael produced the graphic design of the cards (selecting images, colours, general aesthetics, and incorporating my legal text). My role has included translating the GDPR law into card text; negotiating access to participants (with support from Prof Steve Benford), particularly through gatekeepers either in industry or education; designing and leading workshops; running focus groups; designing surveys; transcribing, coding and analysing the data; and raising awareness of the project and obtaining community feedback through conferences and workshops.

[213] These provisions have since changed, for example it is now a 72 hour not 24-hour data breach notification period, consent to data processing is not explicit for all data. These four areas were

autonomy for ubicomp type systems (see questions in Appendix 7). We focus on the more qualitative responses here from the open ended questions.

The participating legal experts raise a number of challenges designers will face in addressing the four key areas of GDPR. With privacy by design, they argue it is a valuable concept but worry about lack of guidance on practical implementation, and warn that PbD responses to regulatory challenges need to ensure the social/legal debate, and not just turn privacy into a technical question. With data breach notification, experts cite the need for designers to prioritise accuracy over speed of response, where they may face challenges in notifying users effectively when breaches occur, and fear of reputational damage may prompt better security measures in the first place. For the right to be forgotten, it needs to be balanced against the right to memories, where designers can create more-subtle less binary solutions to enable forgetting. With consent, experts were worried about user apathy to consent mechanisms. They cited the importance of retaining control but the need to find alternatives to consent to let users have self-determination of data. These insights informed our text on the regulation cards. We ensured text flagged key concerns raised, for example, with data breach notification, mentioning the importance of notification mechanisms and accuracy of breach information.

Figure 8 Original Prototype Cards from CHI (2015)

The overall cards design followed other card based studies (Friedman and Hendry, 2012; Golembewski and Selby, 2010). We incorporated four suits in the deck, each with ostensibly 'evocative' images, and designed to be used by the group for a targeted activity that prompts discussion i.e. building a hypothetical system. The initial card deck was composed of 35 cards, including 5 'regulation' cards (drawn from the legal questionnaire) and a number of cards to support discussion around

based on a UK Information Commissioner Report suggesting areas businesses should start thinking about to ensure GDPR compliance see Smith (2013)

these cards. These included 10 'constraint' and 'user' cards that were developed from informal conversations with designers about elements they consider when creating a new technology, e.g. constraints like low cost and environmental sustainability or needs of specific user groups like children, elderly or visually impaired. To situate the discussion, 10 data driven system cards were created e.g. a smart energy system or platform to trade personal data in the home.

Following Friedman and Hendry (2012) the structure of the workshop for using the cards was a timed card turning exercise. The cards are there to structure discussion between participants around the various aspects of the system, particularly the regulation. Over 30 minutes, participants discuss how they would build a hypothetical system based on the cards they turn. Each group had 5 minutes of discussion after randomly turning one 'system' card, one 'user' card and two 'constraint' cards.[214] The last 15 minutes of the exercise was used to discuss two 'regulation' cards, with the goal of shifting discussion towards data protection.

Feedback on the cards was provided through a card ordering exercise, where participants reflect on the workshop by ranking cards, as a group, in terms of importance to their discussions (eg one most important, six least). The workshop and card sorting exercise with the prototype involved **twenty-one participants[215] split into four groups**. Their specialisms included systems architects, HCI designers, and programmers, with experience ranging from one to sixteen years. Prior awareness of data protection varied, where eleven had basic workplace/university training, three from media reporting, two had passing knowledge, and five a working knowledge. The workshops were video recorded and thematically coded. Through these exploratory workshops a number of initial findings emerged, and we briefly present a few here.

Firstly, unlike HCI designers who are closer to user interests and more amenable to involvement in regulation, more technically orientated system architects and programmers did not see regulation as their role, instead focusing on functionality.

[214] The full deck is available in downloadable format on www.designingforprivacy.co.uk
[215] 16 male and 5 female

Secondly, when engaging with regulation cards, designers saw protection of user interests and engagement with regulation as distinct issues, where the former was central concern, and the latter an afterthought. Lastly, designers were concerned at the level of DP knowledge necessary to engage with regulation effectively. Designers often held limited, needs driven awareness of DP (e.g. from a particular project) and frequently felt more knowledge was needed to act competently. This initial study provided encouraging insights, and helped focus our deeper inquiry. We already see the cards helping with reflection by different designers on the role they have in regulation, in particular, the knowledge gaps where they need greater support, and their prevalent focus on user centric interests.

However, whilst useful for initial exploration, the initial deck and studies are limited, and a broader deck and studies have been developed for a number of reasons. We outline the reasons, and how the new cards build on these below:

- The initial cards have a narrow regulatory scope, focusing on just five elements of the GDPR but we wanted them to become more of a resource for evaluation or creativity with design of new systems. The new deck was broadened to reflect the entire GDPR.

- The initial findings are based on fairly short, tightly timed workshops (30 mins). Longer, less prescriptive workshops provide scope for richer discussion, reflection and more natural use of cards by participants.

- Participant feedback is limited. Whilst card ordering provides interesting initial results, more detailed reflection from designers is necessary. Accordingly, focus groups plus pre and post workshop questionnaires provide more comprehensive feedback from designers.

- The initial workshops do not look at how the cards work in different organisations. Accordingly, we tested the redesigned deck with a range of designers in three different settings to get greater detail on PbD in practice.

We now turn to detail on the GDPR cards.

Figure 10 Sample Information Privacy By Design Cards

Introducing the Information Privacy by Design Cards

In turn we consider the four elements highlighted above: broadening the scope of the deck; revised approach for richer, more detailed workshops; obtaining increased feedback from participants; and understanding PbD in practice for a broader range of settings.

1. The Broadening of the Deck

We wanted to develop the deck into a resource to support designers that raises their awareness of DP compliance; supports reflection on legal values and their role in regulation; prompts creative responses to DP law, and helps evaluation of compliance of their systems.

Unlike the initial cards where the text was derived from a questionnaire with legal experts, the new cards were translated directly from the GDPR. This required an extensive period of translation, analysing the recitals and articles of the GDPR. The cards are based on the 'final post trilogue' GDPR draft released in Winter 2015/6, which then passed into the final law and EU Official Journal in May 2016.[216]

Translation of a 200-page document into a deck of around 100 cards is an interpretative but also structural challenge. It requires distilling the intent behind the different provisions whilst balancing aesthetic requirements of developing segments that can fit into a few lines of text on a physical playing card around 9cm x 6cm. The text of the cards is documented in Appendix 3 and images of the cards in Appendix 1. As an example, the Right to Erasure/To Be Forgotten in Article 17 GDPR (2016) is 421 words long, and this was translated into 37 words, trying to capture the intent of the law and present a key message to the designers. The

[216] Timeline of GDPR at http://ec.europa.eu/justice/data-protection/reform/index_en.htm

translation in the card is "*Users have a right to data deletion without delay. If user consent is withdrawn or data is no longer necessary, controllers must delete that data. This right must be balanced with other rights, like freedom of expression.*"

Translating text from the legal to design communities involves a degree of reductionism. The process of translation was a balancing act. One approach we adopted to help manage the size of the GDPR was clustering the provisions into distinct suits within the cards. Broadly, we divided the GDPR into 'Action' (i.e. those prompting action) and 'Background' cards (i.e. those providing explanatory detail). We focused resources on developing the Action cards as they had direct relevance on the designers' legal responsibilities and the rights of users. Some background cards were necessary, particularly definitions of legal terminology (the definitions cluster) but others contained background detail that was too rich, technical and arguably of less relevance to designers too (i.e. operational requirements of supervisory authorities).[217] In future work, we will find methods to communicate these background elements too. Below we provide detail on how the cards are classified based on clustering and sub clustering of the GDPR:

- Cluster 1: Ch. 2 GDPR (Art 5-11) – **Principles of DP and Consent**
- Sub Clusters
    - DP Principles
    - Lawful Processing
    - Consent
    - Children
    - Special Categories of Data and Exceptions

- Cluster 2: Ch. 3 GDPR (Art 12-23) – **End User Rights**
- Sub Clusters
    - Transparency
    - Information and Access to Data
    - Rectification and Erasure

[217] e.g. Cluster 8: Ch. 1 GDPR – General (Definitions, Territorial Scope); Cluster 5: Ch, 6 and 7 GDPR; Oversight; Cluster 6: Ch. 9, 10, 11; – Misc; Cluster 7: Ch. 8 GDPR sanctions, remedies, liabilities

        - Rights to Object and Profiling
        - Restrictions

- Cluster 3: Ch. 4 GDPR (Art 35 - 43) – **System Designer Responsibilities**
- Sub Clusters
        - General Obligations
        - Data Security
        - DP Impact Assessments and Prior Authorisation
        - DP Officer
        - Code of Conduct
- Cluster 4: Ch. 5 GDPR (Art 44 - 50) – **International Considerations**
- Sub Clusters
        - Third Countries
        - Equivalence
        - Safe Harbour
- Cluster 5: Ch 1 GDPR (Art 1 - 4) – Definitions
    - Selected Definitions – data controller; personal data; data processing

Figure 11 Clusters of Cards

To provide a bit more detail on the process of developing text and translating the GDPR into cards, we highlight a few key considerations. **Accessibility** was a crucial concern, keeping language sufficiently lightweight for non DP experts to understand. Capturing intent and essence of legal terms involved interpretation and judgment based on experience in the field of DP law. Equally, maintaining **legal robustness** was another concern, ensuring there was enough detail for the cards to be a useful resource, accurately reflecting the law but avoiding being too **reductionist**. We sought to find a middle ground. **Clarity** was key, removing jargon and legalese where possible, for example referring to users and designers instead of controllers and subjects. At other times legal terminology was necessary, so we created definition cards to help designers understand key terms.

An area of further work is that the cards are based on new legislation, but do not incorporate elements like case law interpreting the legislation (as none exists yet), expert opinion and state regulatory guidance (eg likelihood of enforcement, prosecutions under these provisions etc). Accordingly, keeping the text reflective of changes and up to date is a key issue for this tool. Supplementing each card with an augmented reality overlay is one proposed solution, to provide additional, up to

date information, readable through a smartphone or tablet. However, this requires constant oversight, updating and maintaining the information, hence further work is necessary to work out how best to do this, in order to protect the longevity of the cards as a reliable resource for designers.

A pertinent example of an area of emerging uncertainty for GDPR is the UK Referendum result to leave the EU. Following this, the UK Information Commissioner Office indicated implementation of GDPR in UK is still likely to happen.[218] Nevertheless, the position is not settled. If the UK leaves before May 2018 when GDPR is enforced, whilst the Regulation will be the same in all 27 member states, the UK may need to pass equivalent domestic legislation too. Even if GDPR 'light' is passed in the UK, the cards will remain useful as a standard of DP compliance in the rest of the EU Single Market. Furthermore, under Article 3 (2) GDPR (2016), non-EU actors processing data whilst targeting products and services at EU citizens, or monitoring their behaviour, are subject to GDPR compliance. The cards need to reflect shifts in the regulatory landscape, for example, if a EU-US Privacy Shield[219] type agreement or Article 45 GDPR equivalence is necessary for data transfers from EU to UK.

Having considered the broadening of the deck, we now turn to the revised approach within the workshops.

[218] https://iconewsblog.wordpress.com/2016/07/07/gdpr-still-relevant-for-the-uk/
[219] See EU-US Privacy Shield Agreement

Figure 12 Turning Process for Cards

2. A Revised Approach

The prototypes were tested through a strictly timed workshop with reflection through a card sorting exercise, as detailed above. We wanted to provide participants more space to discuss issues posed by the cards in greater depth and in a more flexible manner. We made iterative changes to the approach for the GDPR version, based on observing, designing and running the workshops.

We kept the outline of the sessions quite open, explaining we wanted participants to discuss how they would build a hypothetical system, thinking about a specific user group, according to two constraints, and two legal issues. For each group this differed, and we provide a list of them here.

Table 9 Cards Selections from Groups

Group	System Card	User Card	Constraints Cards	Legal Cards	Variations
Group 1	Smart Energy	Second Language	- Low Cost - Careful Collection	- Children and Consent - Giving User Consent - New Seals, Marks and Certificates	Selected extra Legal card
Group 2	Personal Data Trading System	Second language	- Low Energy - Careful collection	- Right against profiling - The USA (Safe Harbor)	
Group 3 [220]	Smart energy management	Country of residence;	-Careful collection -Default sharing - Data minimalisation	-Joint controllers	NB – group went through all legal cards
Group 4	Connected Home	Children	- Default sharing - Privacy	- New seals cards and certificates - Right to Be Forgotten	Looked at extra cards: Children and consent Data portability Purpose limitation

[220] This group used the cards in a very different way, went through nearly all other cards briefly eg Scott – "*so we got low-cost, low-energy, limited connection, data minimalisation which was a resounding – yes, these are the constraints we need to think about. Data maximization, privacy, careful collection and default sharing – were .. yeaahhh, yes but not quite so strong. Minimal distraction, social sharing and user control didn't appear to have any impact whatsoever.*"

Group 5	Intelligent Public Display	Second Language	- low cost - data maximisation	- Right to Be Forgotten - Purpose Limitation	Looked at extra cards – Quantified Self Data breach notification Data portability Restrictions
Group 6	Augmented Reality Glasses	Mental Health	- Low cost - Minimal distraction	- Purpose limitation - Giving user consent	

Timing

During the MOZ workshop, we observed participant discussion was impacted by following the same strict timing approach for card turning taken during the prototype workshops. For some participants, 5 minutes of discussion for each card was not enough, and we needed to intervene in their discussion to prompt them to pick up of another card. This sometimes curtailed ongoing conversation and debate. For others, 5 minutes was too long, and they had covered key issues as a group in 2 minutes. They would run out of topics to discuss or force discussion to fill the allocated time.

After the first MOZ workshop, we revised our approach moving away from strictly timing card turning, to letting participants determine the pacing of turning, how long they spent discussing each card, or whether they wanted all cards upfront (as some did. Accordingly, we still observed time but adopted a less prescriptive approach, letting them progress in a more natural manner. In terms of content in card selection, some groups wanted to read through all cards upfront, to select cards they felt most relevant and interesting to their own experience or collective interests. Others relied on randomly generated selections of cards, determined by picking whatever cards were on the top of each physical suit. We allowed groups to change cards if they did not like the ones they had selected, and in general, tried to allow greater freedom to decide how they wanted to navigate around the legal cards.

We had longer workshops too,[221] where total sessions (including session briefing, pre/post questionnaire, card workshop, and focus groups) lasted from around 1.5 hours for MOZ; 2.25 hours for SBA and 3 hours for INC. The combination of these elements enabled richer discussion and reflection by participants, as we see in the results below.The detailed structure to the sessions is provided in Appendix 2, but in the summary below we provide the process.

Before the workshop, participants read information sheets, sign consent forms and then we arrange them into groups of four or five. A briefing is provided, explaining the purpose and nature of the workshop. They fill in the pre-study questionnaire, and then the process for the cards workshop is explained, highlighting the process for card turning, and the purpose of discussing the various elements at play in designing their selected system. We observe and provide guidance as necessary throughout the sessions. Following this, both groups are brought back together for a focus group discussion about the cards, their role in regulation, and general reflection. This acts as a debriefing too. Finally, participants are asked to fill out the post workshop questionnaire which provides us further data on their attitude to the cards, regulation and their role.

We digitally recorded video and audio from each group. Audio data was transcribed verbatim, coded in the same manner as the interviews in Part III, using a thematic analytical approach, developing clusters of codes into themes and sub themes.

3. Increased Feedback Through Questionnaires and Focus Groups

Whilst the card sorting exercise provided useful initial insights in the prototype workshops, we wanted to obtain much richer discussion and reflection by designers on the legal concepts, their engagement with regulation, and roles therein. Accordingly, we have moved away from card sorting[222] and designed a focus group

[221] In the thesis we just focus on the industry settings, as they are well developed, but we have been running pilot workshops with MSc and PhD level computer science students using the cards too.

[222] Although we did conduct this with MOZ after the focus group, but found after a longer cards session working with the cards, the focus group already

and questionnaires. We have a pre workshop questionnaire (provided in Appendix 6) to provide us a baseline level of prior engagement with DP law, existing attitudes and understanding. We also created a post workshop questionnaire to gauge attitudes towards the cards, DP law in general, and their role in regulatory issues. In this section we unpack findings from conducting our pre and post workshop questionnaires. The full questionnaires are provided in the appendix, and we used a mixture of 5 point Likert scales coupled with open ended questions to justify their answers. The pre questionnaire has 14 primary questions, and the post 20 questions. These were handed out to at the beginning and end of the workshop, respectively. Not every participant completed a post questionnaire, and we have more complete data for the pre-questionnaires, so we focus more heavily on this data. They were designed to give us a baseline understanding of our participants' pre-existing awareness of data protection law and to paint a richer picture of their backgrounds. The questionnaires were input to Bristol Online Surveys, the data exported to Excel and then analysed and visualised within both Excel and Word. For the Likert scales findings, we present these descriptively in graphs, with a mixture of percentages and number of participants. For the more open ended answers, we've coded and classified the different responses into categories, and present these below in tables or descriptions. We go into more detail on the results from these questionnaires below.

Figure 13 Example 2 of GDPR Cards

covered the issues in depth, and the card sorting contained an element of repetition the participants were less keen on.

We also conducted post workshop focus groups to get detailed reflection by participants on the tool and workshop as a whole. A list of semi-structured focus group questions is provided in Appendix 2, but in coordinating the session, we kept the approach quite adaptive, responding to discussion points of the group, prompting reflection on key areas of interest through the questions, but aiming to maintain an open, respectful forum for group discussion.

Questions for the focus group included: did they like the cards? were they useful? challenges they see in using them in their work? did they want more information? Were the concepts in the cards relevant to them? were they comfortable dealing with DP issues? What barriers do they see to engaging with DP law? Does it impact their creativity (stifles or enables)? What are their motivations for engaging with law? What are their current strategies for dealing with legal issues in their work? We provide greater detail in our findings from the focus groups below too.

4. Broader Participation

As Part III highlights, PbD in practice will manifest differently depending on the organisational settings. Whilst the prototype cards provide us initial insights, we need more cross organisational findings, hence we extend the cards to look at how a range of designers, in different industry settings deal with PbD (or not) in reality.

We have **twenty-four** participants split into six groups in total across three different organisations: a large global media firm ("MOZ"); a small technology businesses trade association ("SBA"); and an innovation network centre for SMEs/start-ups ("INC")). MOZ are involved in a range of traditional broadcast and digital media, SBA members work in many areas including, biological and life sciences, pharmaceuticals, precision engineering, energy, and IT; the INC network brings together stakeholders like start-ups, SMEs and researchers working with data driven services.

We classify our participants as coming from three overall groups: business strategy and management; technology, design and creative; and research.

Table 10 Overview of Workshop Participants

Job Cluster	Example Jobs	Percentage of Overall Participants
1. Business Strategy and Management	e.g. Managing Director; Facilitator; International Development; Auditor/Accountant; Marketing; Patent Attorney	33% (8)
2. Technology, Design and Creative	e.g. Software Engineer; IT Consultant; Programmer; Cyber Security and Privacy Consultant; Producer; Graphic Designer; UX Designer;	50% (12)
3. Research	e.g. Industry Research Scientist; Senior Lecturer; PhD Student	17% (4)

The range of participants shows the diversity of actors involved in the creation of new technologies. The workshops are pitched as for those involved in the creation/design of new technologies, where there was self-selection within organisations. It shows that design does not occur in isolation and there are a range of actors shaping the design process. This goes from those most proximate to users (interaction designers), and those focused on functionality (programmers) to a range of other creatives, business strategists and managers.

The overall gender split is **nineteen** males to **five** females, as shown in percentages below.

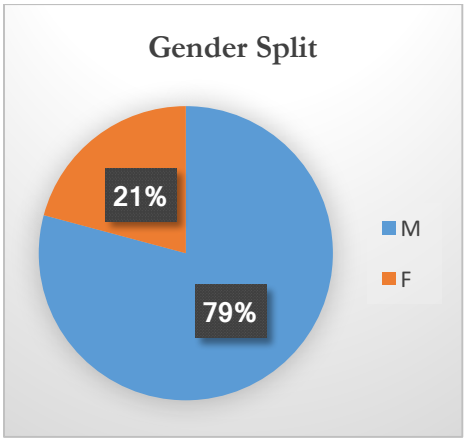


Figure 14 Workshop Participants - Gender Split

With overall years of experience, **42%** have between **11 and 20** years in their profession/industry, **25% from 0 -10 years**, **13%** each for **21-30** years and **31-40** years, and lastly, **4%** for **Nil** and **41-50 years**.

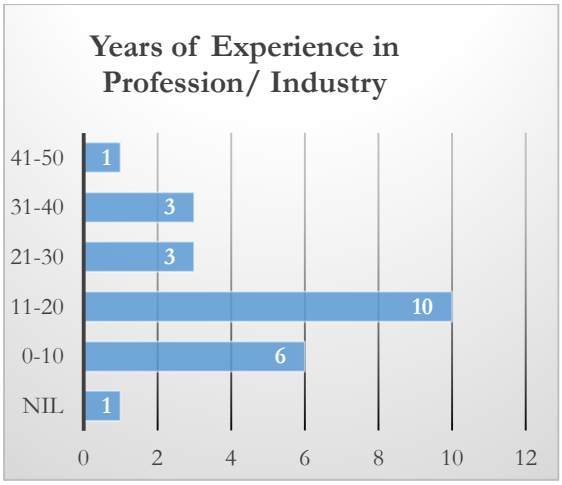


Figure 15 Workshop Participants - Years of Experience in Profession/Industry

For age range, we have quite broad representation. We have **five** aged between **20-30** and another **five** between **31-40**. **Six** participants are between **41-50**, **seven** from **51-60** and lastly, **one** aged **61-70.**

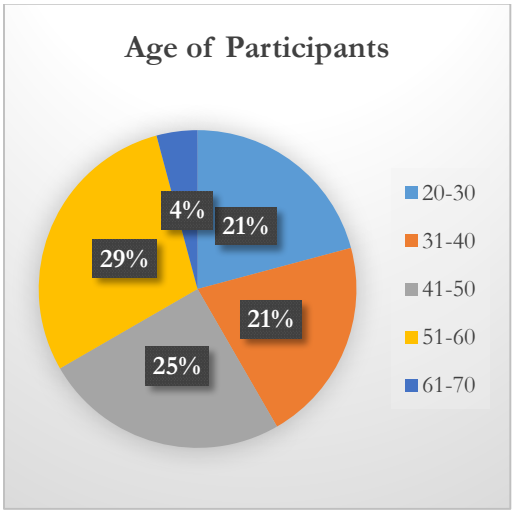


Figure 16 Workshop Participants - Age

We now present our findings from the questionnaires. For clarity, at this stage we provide an overview of **all** participants who completed the questionnaires and their responses. Later, we unpack the more detailed responses from the focus groups and workshops. Those responses draw on wider perspectives, as a couple of participants did not complete the questionnaires but were participating in the focus groups. We keep these discussions split up into the three organisational settings, to focus on the impact of organisations on engagement and understanding of regulation.

Chapter 9. Exploring the Data

In this chapter we present our findings from the workshops, firstly introducing the findings from the pre and post questionnaires, before turning to the workshop and focus group data.

1. Pre and Post Study Questionnaires

Participants Prior Contact with DP

We ask about what ***level of knowledge*** they feel they have about DP/information privacy on a Likert scale from 1 (limited) to 3 (some) to 5 (expert). Only **4%** say they are expert, **17%** between expert and some, **38%** have some knowledge, **21%** between some and limited, and **21%** have limited knowledge of DP/information privacy.

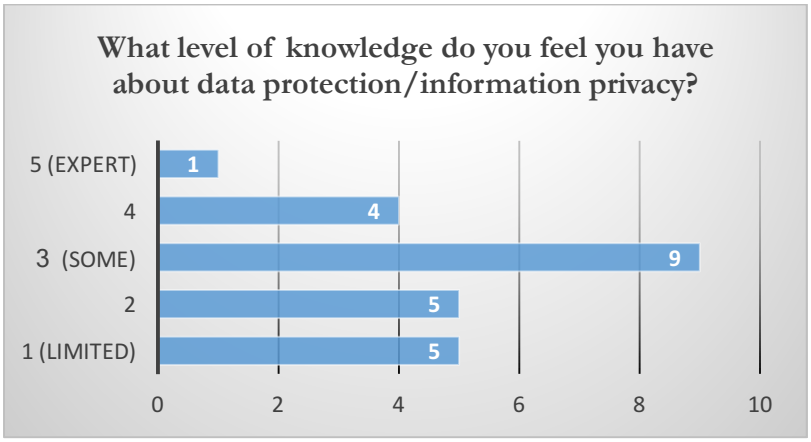


Figure 17 Prior Participant Knowledge about Data Protection

When questioned about their ***contact with data protection/information privacy in the past for professional purposes*** many participants list they have experience either from **working on projects or as part of their role** (listed below). A number have no experience with DP and information privacy, and others have interaction via in house experts e.g. data protection officers.

- **Working on Projects**: academic research, user testing, going through ethics process, for non-disclosure agreements (NDAs), developing personal data driven software, designing privacy policies

- **As Part of Their Role:** as managing director, providing taxation information, managing marketing databases, designing DP policies for websites, Freedom of Information requests, training videos on job.

Participants Sources for Finding out About Data Protection/Privacy

1. Organisations	1. Trade bodies, activist groups (Electronic Frontier Foundation), regulatory body (Information Commissioners Office).
2. Internet	2. Internet e.g. blogs, search engines(Google), websites especially from government and legal, specialist forums e.g. info security, mainstream media and news stories, Wikipedia.
3. Experts	3. In house legal and general advisors, conferences, academic writing, law firms
4. Training	4. Professional Qualifications, taught seminars, attending events, training videos, guidelines.
5. Informal Channels	5. Colleagues, peers, word of mouth, Twitter Friends and Followers.
6. Experience	6. Project work, legislation.

Table 11 Participant Sources for Data Protection Information

We then ask about different **sources** they use to find out about DP/information privacy. We have clustered their responses as follows: organisations; internet; experts; training and informal channels (as detailed above).

We are particularly interested to learn more about their **motivations** for learning about DP/privacy in the first place. The reasons vary greatly, but we'd frame them as following. A number just note a **general interest** in the area, but **legislative change, risk and compliance** reasons are concerns, from the upcoming General Data Protection Regulation to company reputation. Many are driven by its **relevance to their own roles**, for example IT consultant stating they need to know, and avoiding issues running experiments and user testing. Others see their role to **educate and protect their users**, seeking to build trust and a good relationship,

particularly ensuring they do not harm user interests. For example, a Graphic Designer states "…*thinking about systems and how my own work may encourage people to protect their privacy, respecting ethics.*" To this end, a number cite *ethics* and allude to their own *personal values*, for example a University Projects Officer states "*I believe data privacy is of fundamental importance to society and personal wellbeing*".

We push for a bit more detail around these motivations, particularly, if it is their **responsibility,** if they feel it was **important,** and if they are **comfortable** dealing with information privacy of users in their work. We present findings from our Likert scale, and also open ended answers here.

Motivations: Responsibility

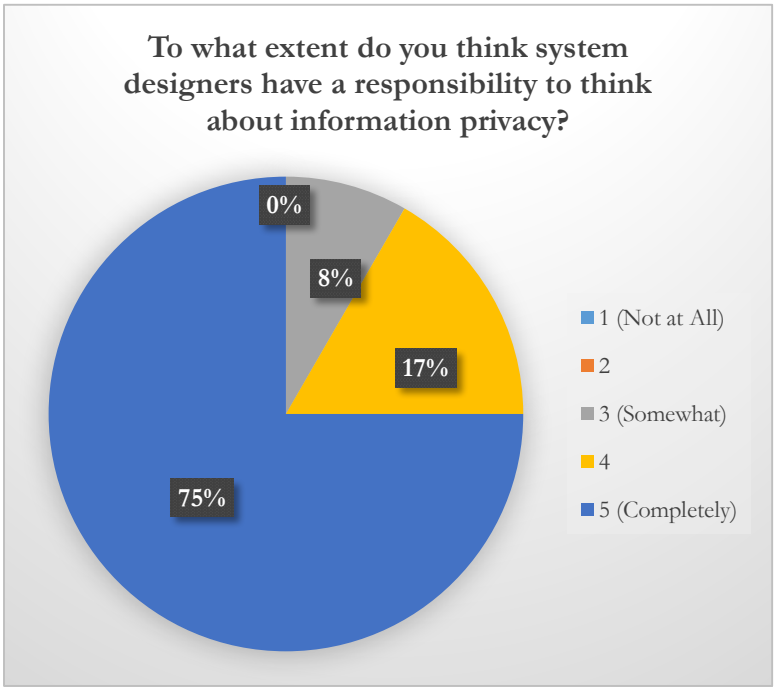


Figure 18 Motivations - Responsibility

Overall, the vast majority of our participants think system designers have a responsibility to think about information privacy. No participants think it is not their responsibility. **Two** think it is somewhat, **four** between somewhat and completely, and **eighteen** it is completely their responsibility.

The rationale behind their feelings of responsibility are rich. Some suggest **security and privacy are key social values**, noting the practical importance of keeping data safe and secure. Data protection and security should be built into systems, as one participant argued: "*the system should be watertight... can't say the same for humans!*". Their users should be able to expect security of data, and whilst legal requirements

may mandate this, ethically they feel designers should do more. As one participant states there is a "*Legal requirement of minimum, ethical imperative to do better.*" They may merely be following orders from superiors in the workplace, yet many suggest it is part of their **professional obligations.** The following comments suggest different dimensions of this professionalism, from **necessity** ("*who else would do it? Very important.*") to **responsibility for their outputs** ("*everyone has to interact with what they have created*") and **users** ("*because they are the front line of designing privacy*") to a **general duty** ("*we all have to learn about ethics regardless of our profession; shouldn't be a choice*").

Motivations: Importance

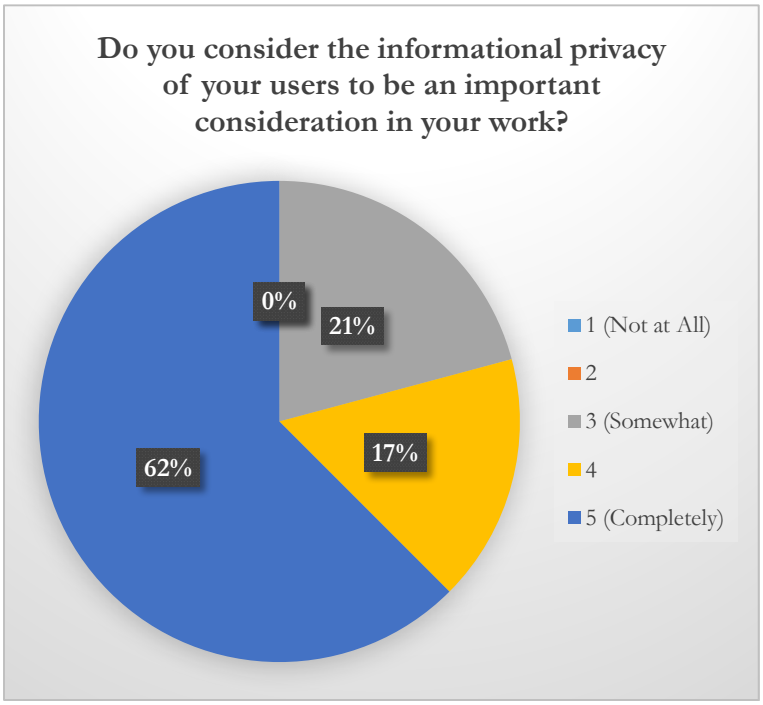


Figure 19 Motivations - Importance

The vast majority, **nineteen**, think information privacy of users is an important consideration in their work. **Fifteen** think completely, **four** between somewhat and completely. No one feels it is not important at all and **five** feel it is somewhat.

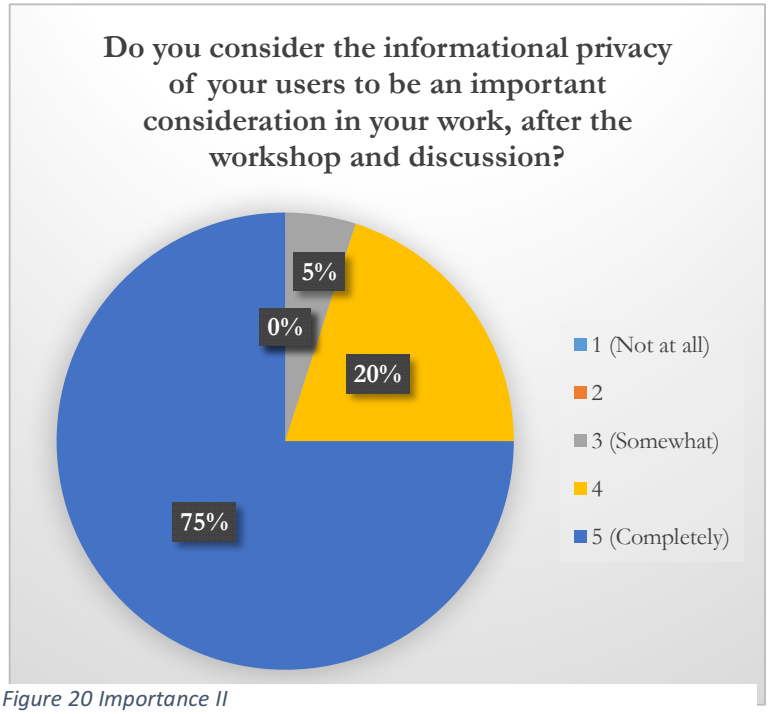


Figure 20 Importance II

In the post workshop we have 20 responses (4 missing), hence the figures are not directly comparable, so we present the percentages as opposed to number of participants. **Nearly all of our participants see privacy as very important in their work, after doing the cards exercise. 95%**

see privacy as between somewhat and completely important, **5%** somewhat, and 0% for the other two.

The answers in both questionnaires are broadly similar, so we group them together. Broadly, we would frame the responses around **designer responsibilities** and **end user rights**. With the latter, participants recognise users have an interest in how data is used, "because they care about it! Or at least, if it goes wrong". With the former, the **value of data** is cited, specifically a greater need to share how it is used, and the importance of establishing trust and reputation. As one argues, *"trust is important: people have a right to know what happens with their data"*. Indeed, some developers acknowledge they are in a relationship with clients/users, and accordingly need the user data, but equally, they have a role in creating "…*informed choices, empowering, facilitating new experiences*…". Moral and legal obligations may drive this, as one put it "*It's the law*!!" but similarly it can be operationally desirable to create a **culture of awareness from the top down**: "*it has to be put at high level protect to allow smooth operation*". Indeed, **institutional trust** is key, as one argued "*without privacy no trust can exist and therefore MOZ would lose its faith across shareholders*". **This has to be balanced, as some feel DP/privacy is less important to their roles as they are not handling particularly sensitive information.**

Motivations: Comfort

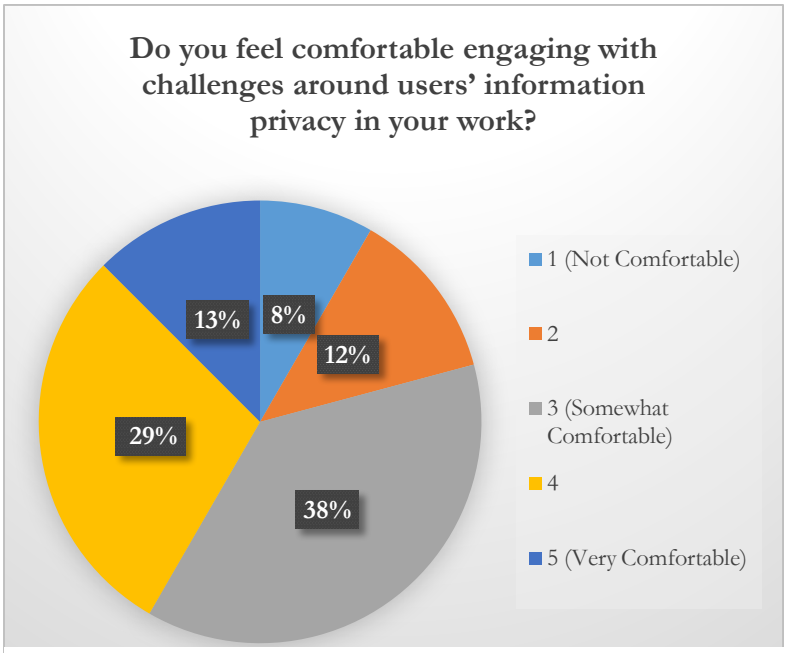


Figure 21 Motivations - Comfort

Around half of our participants feel comfortable dealing with challenges of information privacy in their work. Two participants are not comfortable dealing with user

information privacy challenges in their work, **three** between not and somewhat comfortable, **nine** somewhat comfortable, **seven** between somewhat and very comfortable, and **three** very comfortable.

Matching this fairly even split in the figures, in pulling out the detail we see variations in experience from those who are familiar with privacy and feel they have a good understanding of the issues, to those with very limited engagement and understanding of the law. A few mention amendments might be needed in practice to accommodate privacy requirements, as one Graphic Designer states "*having to make alternate plans can be more difficult but more private would be more ethical*" and similarly, *professional values or protocols* of an organisation are important, as one UX Designer states, they need "*to ensure we are adhering to MOZ policy and data protection laws in our daily working practices*". They also recognise the challenge, as one senior lecturer puts it "…*they're really important to get right. it can be challenging, but I'd rather engage with users about it*…" Others recognise training exists, or they would know where to go if necessary for information.

Participant Reflections on the Cards

Having unpacked participant attitudes to the underlying concepts of the cards, we now turn to the cards themselves. Accordingly, we present feedback about the cards as a medium for communicating legal principles, reflecting on the method and practical utility of the tool. This data is based on the post workshop questionnaire, where there were consistently 20 participants returning forms, unless otherwise stated. We proceed by considering the following elements:

- *Practicality and Ease of Use;*
- *Design;*
- *Symbols;*
- *Language;*
- *Reflection (thinking differently and desire to know more).*

Cards: Practicality of Use

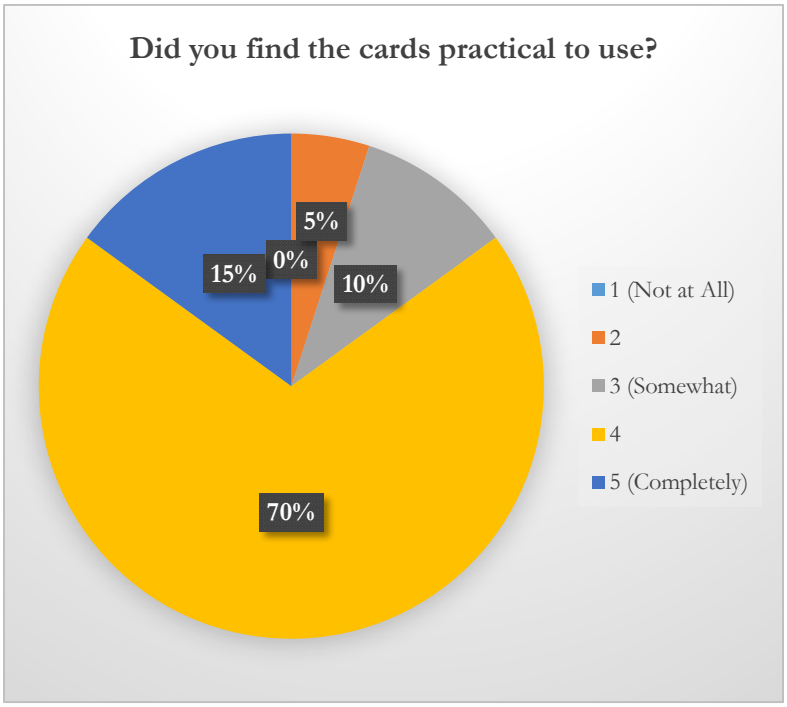


Figure 22 Practicality of Use

The vast majority, seventeen, think the cards were practical to use. None of our participants think the cards are not practical to use, **one** between not at all and somewhat, and **two** for somewhat. **Seventeen** are between somewhat and completely.

As the figures show, participants are largely positive about the practicality of the cards. They particularly like that it prompts reflection and sharing of opinions, that they are clear and easy to look through, and how they prompt thinking about new aspects they would not otherwise consider. In particular, the participants like the structure of providing channels for debate in a focused direction. As one states "*The categories forced consideration of relationships between different types of factor.*" Alongside this, they provide a number of recommendations to make the cards more practical, like provision of more guidance of "*how to play*", more linking of discussions during sessions to possible impacts and solutions. Some want more cards, and others less.

We ask them separately about what things they would change about the cards. Mainly they are points already covered, but other points raised are more information on different types of data (eg inventory of data types); examples of what to do next to overcome issues raised by DP and a mechanic where they can work through more cards and scenarios.

Cards: Ease of Use

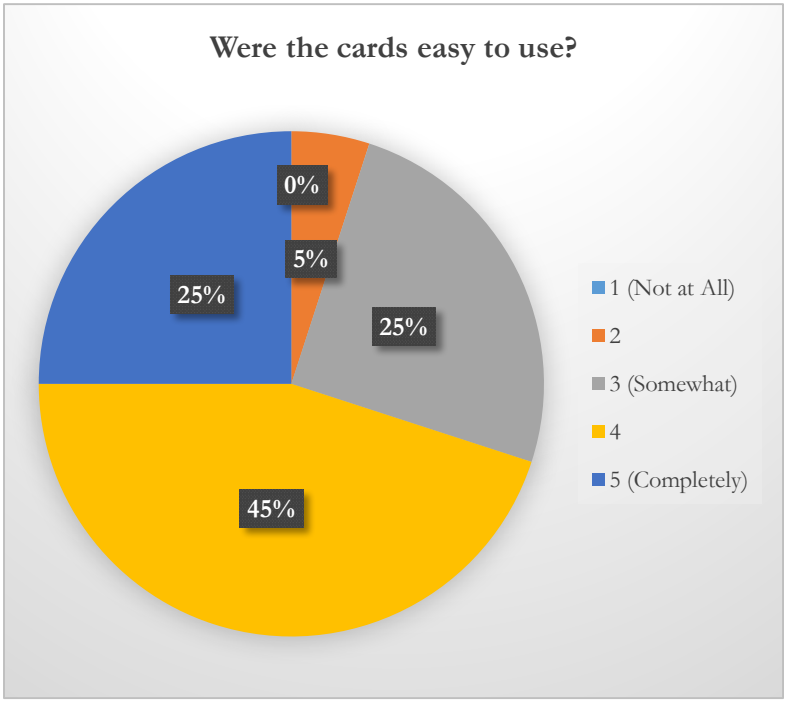


Figure 23 Cards - Ease of Use

Overall, the majority, fourteen, think the cards are easy to one. No-one finds them too difficult, **one** is between not at all and somewhat, **five** at somewhat, **fourteen** between somewhat and completely.

Similarly, with ease of use, we have some who like the concept, size of cards, clarity, explanation of use, and balance of detail with brevity. One states they are "*really intuitive, and easy for starting the conversation*". Others want more scene setting around tasks, structure around relationship between different cards and there is a bit of confusion from the workshop format, when to turn over new cards and meanings on the cards.

Cards: Design

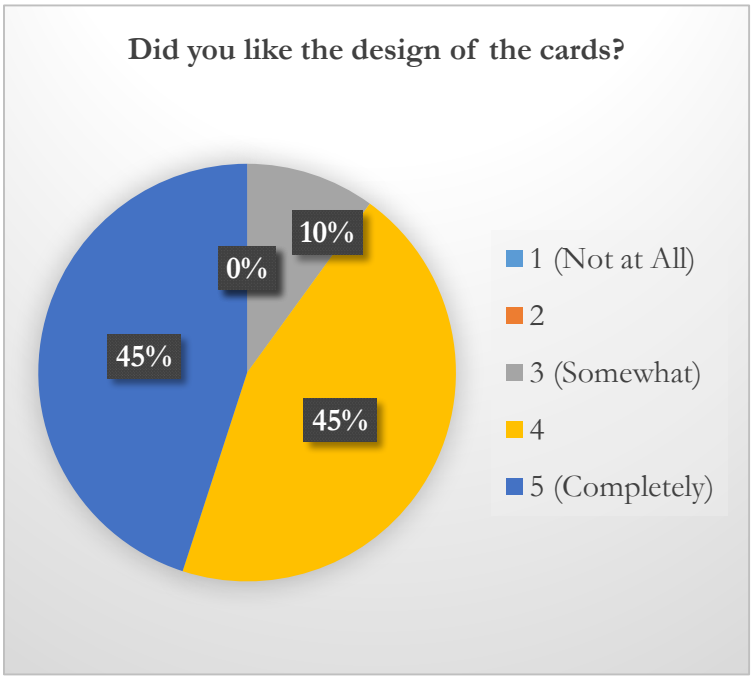


Figure 24 Cards - Design

Nearly all participants, eighteen, like the design of the cards. None are between not at all and somewhat**, two** at somewhat and, **eighteen** between somewhat and completely.

Given the largely positive feedback to the design, the comments match this. The overall feel is high quality and aesthetically pleasing, as one states "*Clear, simple, well-structured physically robust.*" Some want more linking to the background material, for example "*User rights were interesting particularly. Would like the link to source of the data for each card*". Another states, "*they were attractive but didn't give enough insight into the core idea I felt*" and on the more critical front some are concerned about low colour contrasts and justification of text.

Cards: Symbols

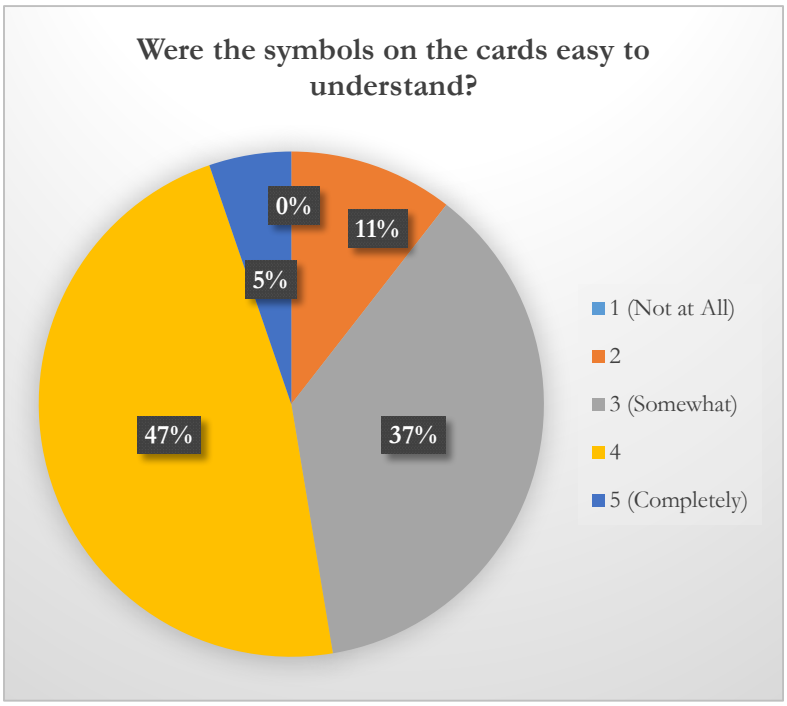


Figure 25 Cards - Symbols

We only have **nineteen** answers for this question, with one missing, and have more mixed results here. Overall, **ten** think the symbols are from somewhat to completely understandable, **seven** somewhat, and **two** between somewhat and not at all. Icons are praised as logical and simple, however, primarily participants feel they will not make sense without the legal text, but when combined they work. Many others do not even pay any attention to the icons.

Cards: Language

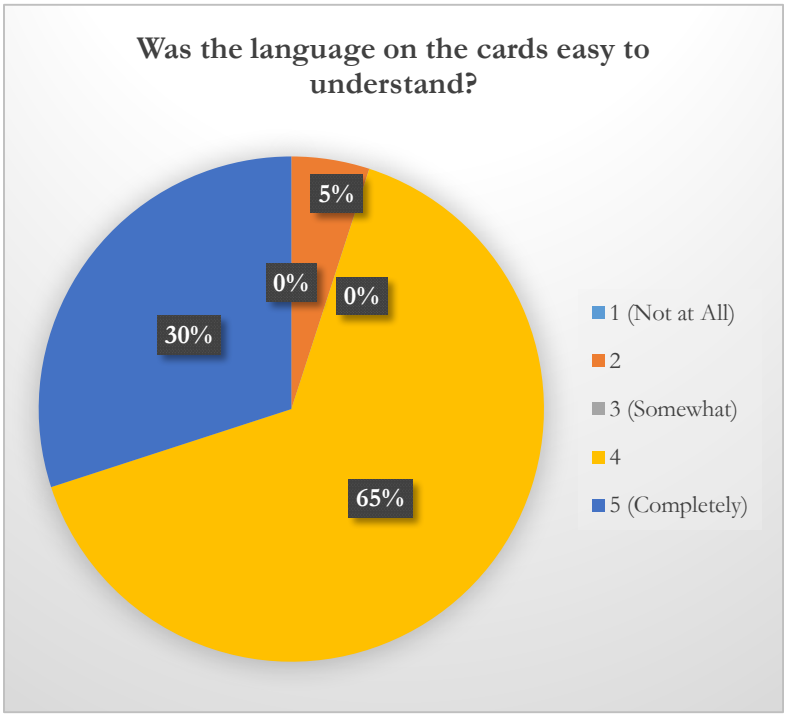


Figure 26 Cards - Language

Nearly every single participant, **nineteen out of twenty,** find the language on the cards easy to understand. **One** is between not at all and somewhat; **none** are somewhat; and **nineteen** are between somewhat and completely.

Feedback is very positive, with the majority of participants noting the technical complexity of the language yet find it very clear and legible as plain English. As one says '*I'm not British and / or expert on it, and I could understand*'. The core definition helper cards are valuable, but they would like more examples, and some find legal terms confusingly ambiguous.

Separately, we also ask them if they have heard of the legal concepts on the cards before. Most who have good knowledge are due to working with data protection in their profession and through reading terms and conditions. Whilst one has not at all, others are aware of some concepts through passing conversations, teaching and project work and discussions with colleagues.

Cards Reflection: More Knowledge?

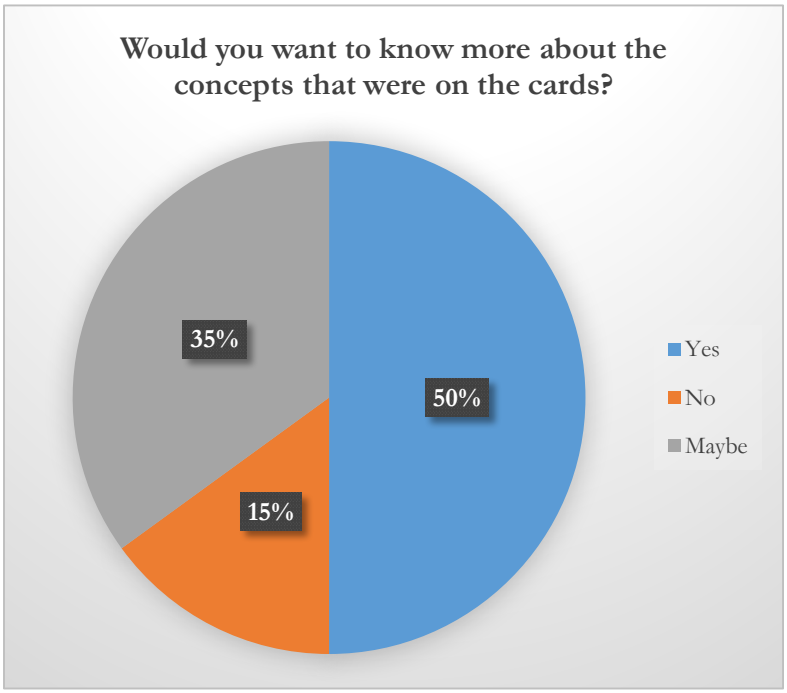


Figure 27 Cards Reflection - More Knowledge?

This result is split, primarily by those unsure if they want to know more about the concepts. Ten want to know more about the cards, **three** do not, and **seven** are not sure.

Many are keen to know more, particularly in relation to their work. One participant argues "*I'd like to have a better understanding to aid my design process and thinking*" and another sees value "*to be able to share knowledge and improve working practices*". One notices that the level of information is tailored to the tool, stating "*generally yes, but in the context of the method it would have slowed things down.*" Others feel they do not see enough cards to know, or they already have enough knowledge from their background, or feel they obtain sufficient insight from the core definition cards.

Cards Reflection: Different Thinking?

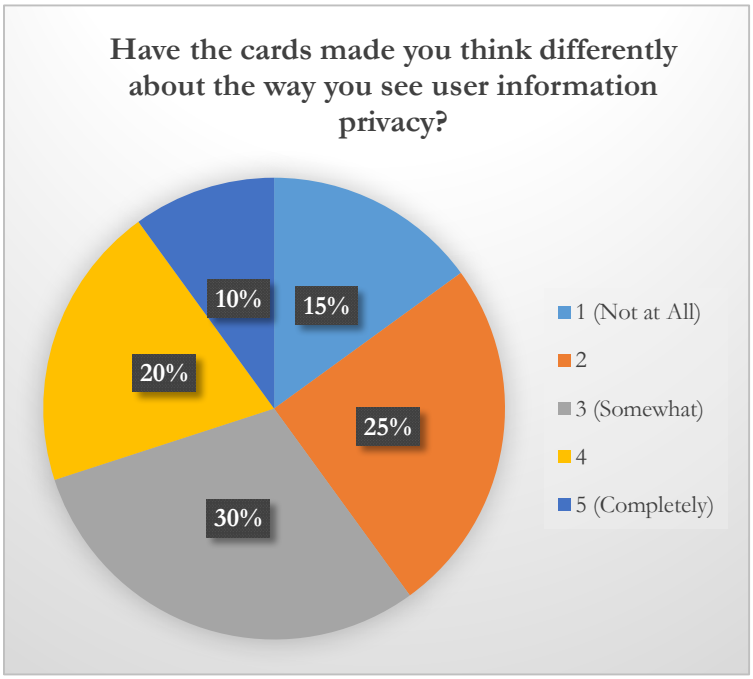


Figure 28 Cards Reflection - Different Thinking?

On the whole, it seems participants do not think differently about information privacy after using the cards.

These results are very interesting as they have quite a spread of responses. **Eight** are between not at all and somewhat; **six** are somewhat; and **six** are between somewhat and completely.

Some state it makes them more reflective, for example, the cards prompt them to question, and raise awareness of new complex issues, often from different perspectives. As one says "*yes I know not to assume anything*!". Others, often those with most experience feel it does not really change anything for them, as they already know it is a big issue.

Separately, we ask participants about their current approaches for engaging with privacy requirements at work, and if these are effective. Some have support within the organisation, for example in MOZ they have an **internal advisory authority** which works well. Others mention speaking to other **staff, lawyers or project managers**. This has mixed results, from being useful with managers to slow and time consuming with legal, to being last minute and low priority with other staff. Some note they either have no methods, or fairly ad hoc approaches, which need more structure. Training exists, for example video tutorials or training courses which participants are not convinced with. Researchers mention they have a standardised process, but most interestingly is the more technical approaches from

encryption to access limitation and standard enterprise resource processes. This extends to approaches for understanding the social context, as one puts with "*co-design, focus groups, interview, questionnaires, local expertise*" which works well but "*more techniques would be useful*".

When we ask about other forms for conveying the card information, whilst they like the physicality, participants also largely want **digital support**, ranging from a website linking to sources, available for offsite use, or providing a primer to the cards. An **interactive app** is also a popular idea, with more background and extra activities e.g. a game/story; and an online version of the cards**. Written guidance** in a book or briefing might also be useful, as would **additional resources** like e-learning materials, Wikipedia pages, flow charts, examples of applications or a [learning] pathway. Others feel nothing else is necessary.

We ask if participants would recommend the cards to anyone else. Quite a number say no, for example "*they're good, but I don't know people I'd recommend them to*" but others see utility for universities, teaching staff, small businesses, start-ups, UX designers and basically, "*anyone designing systems involving data*".

Many feel the cards may be useful in their professional and personal lives. One captures a range of uses like "*Explain about privacy; useful for projects; raise awareness of users rights; use with developers, improving their own systems, in consultancy, facilitation*". Others would use them whilst developing new software and systems, during testing and work with users and importantly to take a different point of view or spot data concerns earlier in the process.

2. Focus Groups and Workshops

We used video and audio devices to record the workshops with participants using the cards and the focus groups of their feedback. Our study went through University of Nottingham ethics process, and all participants read information sheets and signed consent forms. The format of the workshop, ethics and other relevant documents are contained in the appendices. We transcribed our recordings verbatim to enable systematic thematic analysis and coding, following the same approach as we did for the interviews in Part III (Braun and Clarke, 2006). Our

findings are based on six card workshops across three organisations. There are four focus groups, as the MOZ workshop involved two separate focus groups. The make-up of our groups are provided below.

- **Large Global Media Organisation (MOZ)**

Group 1	Details
Pseudonyms	**Amy; Adam; Barry; Christopher; Derek**
Average Age	**32 years**
Average Years overall Experience	**10 years**
Average Years in Current Role	**2 years**
Gender Split	**4 male; 1 female**
Job Types	**Producer; Software Engineer; UX Designer; Technologist; PhD Researcher**

Table 12 Media Organisation Z (MOZ) - Group 1 Participants

Group 2	Details
Pseudonyms	**Randy; Irvin; Mark; Alan; Rita (did not provide details on age, experience etc – data below based on male participants only)**
Average Male Participant Age	**41 years**
Average Years Overall Experience	**17 years**
Average Years in Current Role	**6 years**
Gender Split	**4 male; 1 female**
Job Types	**Research Scientist; UX Engineer; Programmer; Producer**

Table 13 Media Organisation Z (MOZ) - Group 2 Participants

- **Small Technology Businesses Trade Association (SBA)**

Both Groups	Details
Pseudonyms	**Ted; Stuart; Scott; James; Andrew; Barry; Christine; David**
Average Age	**53 years**
Average Years overall Experience	**28 years**
Average Years in Current Role	**10 years**

Gender Split	**7 male; 1 female**
Job Types	**Facilitator; Hardware and Software Design; Application Specialist/Managing Director; IT Consultant; Marketing; Director; Patent Attorney; Managing Director**

Table 14 Small Business Association (SBA) – All Participants

- **Start-up/SME Innovation Network Centre [223] (INC)**

Both Groups	Details
Pseudonyms	**Oliver; Patrick; Robert; Susan; Tina; Casey; Matias; Ivan; Sam**
Average Age	**37 years**
Average Years overall Experience	**Insufficient data**
Average Years in Current Role	**3 years**
Gender Split	**4 male; 3 female**
Job Types	**Information and Cyber Security Consultant; University Project Office Worker; Senior Lecturer; Privacy Services Manager; International Business Development; Graphic Design; Audit/Accountancy**

Table 15 Innovation Network Centre (INC) - All Participants

[223] (based on 7 returned questionnaires, instead of 9, hence not full reflection of attendance)

A Model of Regulatory Literacy

We conceptualise our findings from the workshops under the concept of **regulatory literacy.** User centric regulation requires actors to possess a range of skills, knowledge and strategies for engaging with regulation. As in other domains, literacy is knowledge in a specific area to enable competent action. The workshops help unpack the strengths, weaknesses and challenges for designers engaging with law. Put simply, **regulatory literacy** is key to any notion of user centric regulation, and we use our findings from the six workshops and focus groups to understand what that may require in practice. Our conceptual framing shows how designers understand legal issues through the medium of cards. It highlights where competency exists and where greater support is needed. Our model, as detailed in figure 29 below, breaks down our concept into three main elements: **regulatory interaction; sense-making strategies and managing complexity**. We explore each of these in detail in turn, beginning with **regulatory interaction.** Figure 29 below also visually portrays our model:

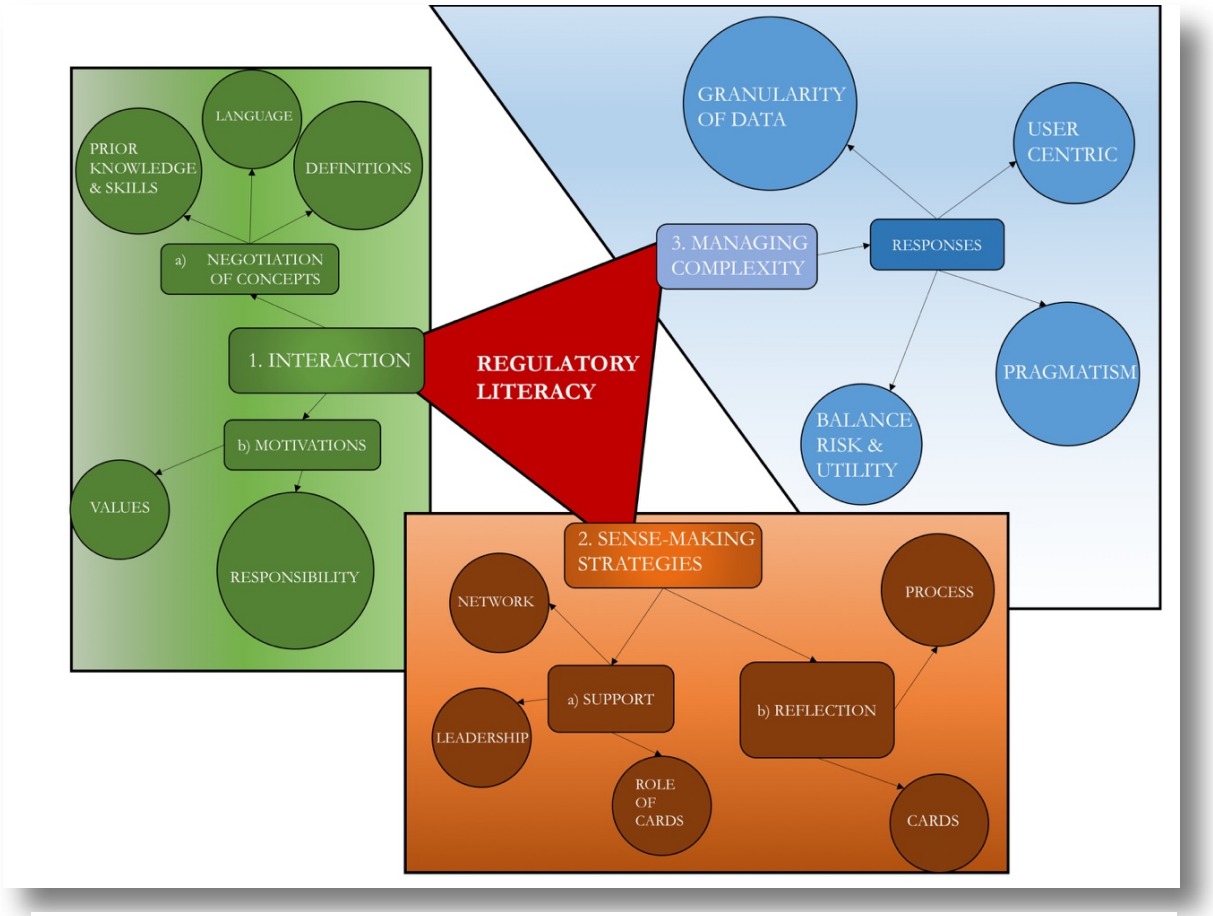


Figure 29 Proposal For Regulatory Literacy Model

1. Regulatory Interaction

In understanding how designers interact with regulation, we consider their motivations and then how they negotiate around these concepts. We find there are particular personal and organisational values, and a spectrum of responsibilities motivating designers to engage with law. However, once they do engage, they have both strengths and weaknesses in negotiating around the legal language and concepts.

Motivations: A Spectrum of Values and Responsibilities

We have already mentioned many of the motivations above, so we keep this section brief. Nevertheless, within MOZ, **protection of reputation** is a factor, particularly any consequences from possible data breaches like risk of being sued, bad media coverage, or resulting loss of public trust in the institution. With stark honesty around such **organisational values**, Barry put it: "*my motivation was a) covering my own ass and b) covering MOZ's ass*". Beyond protection of reputation, some see their role as going beyond just legal compliance, to seek a higher **ethical** standard of conduct, avoiding profiling or use of data for advertising where possible. As MOZ Group 2 Mark argues, "*I think in the general case, our kind of aspirations in terms of ethics probably exceed what is legally required anyway."*

Distinctions between what is personally ethical, and professionally compliant, emerge during discussion of the new GDPR privacy compliance certification process[224] by MOZ group 2:

> "*Mark - oh so we can get a rubber stamp…*
>
> *Irvine - …so you basically hide behind the certification…hiding behind the certification… just saying it as it is…*
>
> *Mark - ...oh that's quite good though. That might be reassuring to our users... simple way of saying …, certainly we as a company, we as systems designer or whatever don't*

[224] Law - Art 42, GDPR, 2016; Card Text – "**New Seals, Marks and Certification:** New data protection certifications, seals and marks showing compliance with regulations are being developed and will be granted for maximum of three years."

have to make sure that everything is internationalised …credentials… suddenly you know… we got this way of ... if we comply to that."

With **personal values**, designers often tacitly empathise with their end users, discussing their own personal preferences, like avoiding systems that collect data in morally questionable ways or their practices for avoiding linking their data across different services. These values manifest in the design discussions as they seek to create systems consistent with their own ethics. Whilst considering their augmented reality glasses for users with mental health conditions to navigate the supermarket, INC Group 6 reflect on ethical risks to vulnerable users, taking a paternalistic stance to protect them:

"*Oliver - There is also the fundamental thing, if the system is targeting people with mental health issues, these glasses are effectively going to be tacitly broadcasting the person has mental health issues, if that is the sole target market…*

Robert - Glasses related to the health…

Patrick - I would think we are talking about an application that would sit on these glasses, but it is a very valid point, because if you're saying this user needs extra protection and therefore shouldn't be having those kind of guided offers to try and influence them, then the glasses then can send some kind of signals to say, this kind of person needs extra protection.

Tina – Yeah I think they could be used in a positive way, tailored adverts is automatically a bad thing, but tailored not to advertise to a vulnerable person…

Patrick – it's a key thing not advertising to vulnerable people.

Susan – don't exploit this person."

When speaking to small businesses, **necessity** is a key motivation for engagement. Resources and company size shape the nature of their internal obligations. In very small companies, the managing director may be solely accountable, whereas, in

slightly bigger small businesses, heads of department in accounting, information technology or marketing may play a role too.

The need for oversight and control dictates one person has to take the lead yet this can be quite arduous and prompts a degree of fear about consequences of non-compliance too. Importantly, small companies do not just deal with data protection, but other areas too like environmental or financial regulations. **Necessity** pushes them to engage with this range of laws and they often hold hope that others are acting prudently too. As Ted, Group 3, SBA explains:

> "*for a lot of one man bands, particularly think about companies that are starting up, they wouldn't be able to consider a lot of this. If they were using proprietary software, say you had a software to do your accounts, you have a proprietary client management system, would that... providing you've made it clear to the people you put into those systems, would the kind of security and everything offered by that proprietary software be adequate, would you think? …*
>
> *Stuart: hmm... it doesn't stop the copying, does it - oh I'll just exploit this bit of data, you know.*
>
> *Ted: doesn't matter how big you are though … most of them are companies that have been breached...*"

For the very small businesses of SBA, they often argue **responsibility for data handling does not wholly reside with them**, and may be divided among others actors in the data supply chain. Security and data handling concerns, for example, would be 'downstream' from their influence, with those who buy their products, like utility companies, or with services they rely upon, like banks. Cloud storage, third country and US data transfers can further ameliorate their responsibility, as they feel they lack adequate control over these processes. As small businesses they are less well-resourced, and carving out a narrower range of responsibilities is pragmatic. In understanding the scope of their responsibilities, legal definitions

(data controller vs processor)[225] can confuse matters further, as the following SBA focus group discussion shows:

> *"Barry: … if the Bank breaches and you are stored on their system, the supplier information…*
>
> *James: oh, I see. Is it you…or is it them?*
>
> *Barry: an awkward one, isn't it?*
>
> *Stuart: but that's where the controller and processor issues are really gonna be a nightmare aren't they.*
> *Christine: critical…*"

Overall, the nature of law is key because whilst ethics are important, participants cite the **authority** of law as an important rationale for mandating action. This varies from having to re-establish consent with each new beta release of software, despite inconvenience, to finding ways of satisfying new GDPR requirements of having provable user consent[226]. As Christine, Group 4, SBA explains:

> "*Christine – reads [proving consent card] – so when we do [the] consent thing with people…*
>
> *Barry – Would you expect it to be written? Do we have to have a written part, to go along with digital consent?*
>
> *Christine – That is the law… (David echoes – 'new law') … that is the new law*"

As we see, interaction with regulation is motivated by a range of factors, primarily necessity, responsibility, personal ethical values and

[225] Law – Ch4, s1, GDPR, 2016; Card Text – "**Processor v Controller**: A controller may define the means and purposes of processing, and a separate processor may carry this out. Controllers need to strictly and contractually define their relationship with processors."
[226] Law - Article 7, GDPR, 2016; Card Text – "**User Consent 2**: Consent must be provable. It can be withdrawn by the user at any time, and when it is given as part of a written contract it must be flagged up in clear and plain language."

organisational values like protecting reputation or guarding against litigation.

Negotiation of Concepts

Whilst we see there are many reasons why designers engage with law and regulation, we need to better understand **what strengths and weaknesses they possess in negotiating around legal language and concepts**.

Definitions and Legal Language

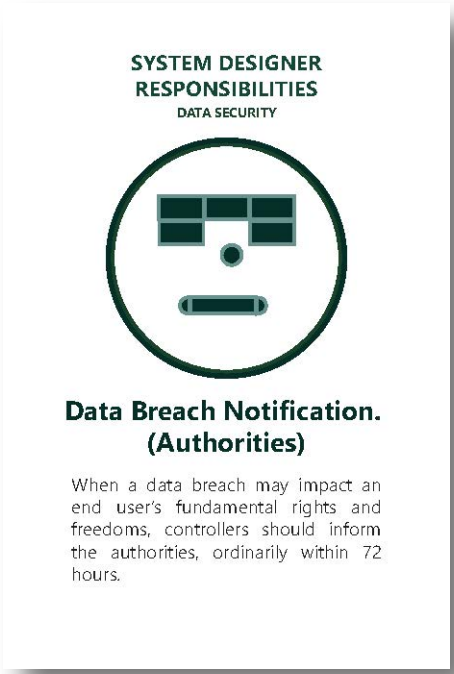


Figure 30 Data Breach Notification Card

The cards, by design, aim to **prompt reflection on legal terms**. This helps us learn how individuals not trained in law deal with these concepts. During the workshops, some express they feel like **they are becoming lawyers**, whilst others recognise the limits of their skills. As INC's Patrick puts it "*Unambiguous vs explicit consent – that relies on interpretation plus case law, and that is where as a non-lawyer you go, I have to stop now*". Whilst more **experienced participants show understanding of law and legal concepts**, referring explicitly to terms of art like duty of care, reasonable expectation of privacy, or even subject access requests, more often we see rich engagement around legal concepts, just not necessarily by name. **Overall, groups use the cards to delve into deep discussion of quite technical legal issues, often grasping concepts straight away, like purpose limitation or data portability**. They appreciate the **nuance**

and subtlety of legal language, as Group 5 INC display during discussion of the data breach notification card:[227]

> "Sam: '*Data Breach'. Oooh. 'Data Breach Notification' (Reads - "When a data breach may impact an end user's fundamental rights and freedoms, controllers should inform the authorities, ordinarily within 72 hours"). That is interesting.*
> …
> *Sam: so it's a data breach, should all be leaked somewhere*
> *Ivan: what does the word 'fundamental' mean?*
> *Sam: now you are really drilling down too... are you a lawyer?*
> *Ivan: sorry. no no. but this is what I am trying to do at the moment, work out what it means ... I've been caught out in the past. But it's a very good question. You either need some control internally within the company.*
> *Sam: … I am on a journey here.*
> *Ivan: I am on a journey ...*"

Where we see greater uncertainty or confusion around an abstract legal term,[228] participants **resort to definition cards** where possible,[229] but more often they **discuss their interpretations, drawing on real life analogies or experience to provide meaning.** A pertinent example is when MOZ Group 1 are unsure what a legal effect stemming from an algorithmic decision is.[230] During discussion, Amy realises it is decisions based on unfair profiling, stating "*so if I was automatically banned from buying knives because my profile had told that I was a knife criminal, I could then go, hang on a minute, I'm actually a chef…that kind of makes sense*".

Such discussions are useful for us as helps us to understand what mental model designers **have of the law, how they understand it and see how this differs from the legal definition.** To help explain this further, we briefly look at two

---

[227] Law- Article 33, GDPR, 2016; Card Text – "**Data Breach Notification (Authorities)**: When a data breach may impact an end user's fundamental rights and freedoms, controllers should inform the *authorities*, ordinarily within *72 hours*."
[228] Or any language on the cards
[229] Range of cards provided to help with legal terms - see Appendix
[230] Law - Article 22, GDPR, 2016; Card Text - "**Right against Profiling:** Users have the right not to be profiled or subject to algorithmic decisions with legal effects. They have a right to request such decisions get human oversight and review."

terms that prompted extensive discussion across the groups: **personal data and data controller vs data processor.**

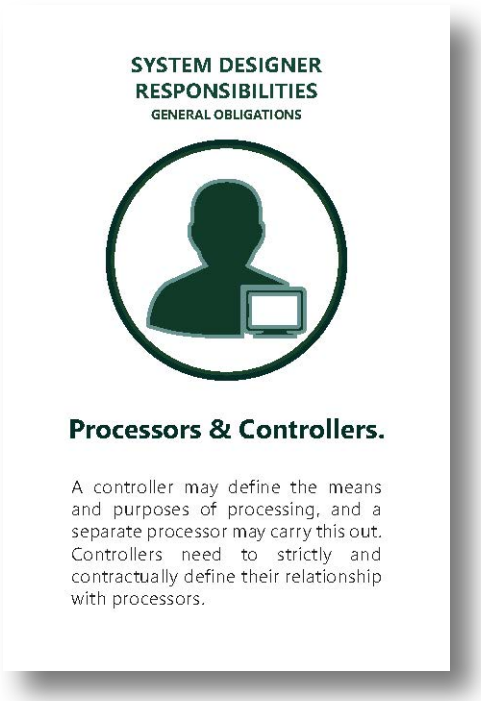


Figure 31 Processors and Controllers Card

Legally speaking, **personal data (PD)** is "*the information that directly or indirectly relates to the end user*". [231] Across the groups we see a range of definitions emerging for PD, often drawing on personal experience. These include PD as classes of information like names, home and email addresses, phone numbers, photographs, device data (GPS or metering), linked together non-personal data, behaviour profiles, and sets of numbers or facts related to individuals (eg user IDs or language preferences).

Participants cite specificities of culture, context and users need to be considered in addition to these types of information. They recognise expectations of what is personal vary and this is not static but changes over time. Personal data needs to be handled in a trustworthy manner to meet expectations of users. As we can see, these definitions capture the key elements of information being tied to individuals, even if this is indirectly. There is the additional focus on user interests, commensurate with the important nature of the information.

More legally complex is the distinction between a data controller and processor. **Data controllers are** "*those who determine the purposes of collection and means by personal data is processed*"; **data processors are** "*those who process personal data on behalf of others*"; and the **relationship between processor and controller** is "*a controller may define*

[231] Law- Article 4(1), GDPR, 2016

the means and purposes of processing, and a separate processor may carry this out. Controllers need to strictly and contractually define their relationship with processors."[232]

Despite a bit of confusion with participants, they fundamentally grasp the implication of risks around **how liability and responsibility is split between the two parties**. Responsibility may even be shared, inadvertently or deliberately, due to joint handling of data, hence what that means for each party is important to understand. INC Group 6 discussion captures the practical implications of shared responsibility, debating who needs to obtain consent from end users for data processing:

> "*Oliver - Would they count as the data controller or would we?*
>
> *Patrick –that is an interesting problem*
>
> *Oliver – now it's getting interesting isn't it– so if they are the data controller they are going to have to get consent as well. Or we are going to have to get consent to pass it off to someone else, our supermarket partners. We can't just pass it on - or are we going to give them [the users] pages and pages of stuff…which isn't really great*"

On the whole, participants **do not struggle greatly with legal language, finding ways to understand, often using definition cards, personal experience and group discussion**. Importantly, as indicated above, **nineteen out of twenty** who responded to the post-questionnaire, state **they** find the language on the cards easy to understand, indicating cards provide support in engaging with these concepts.

Empowerment and Prior Knowledge

The cards are a useful medium for sharing knowledge about data protection law. Importantly, they can provide **empowerment** to individuals by helping them to understand law and give them confidence to use their new found awareness. As a baseline, there are **differentiated levels of knowledge** between participants. Within MOZ, for example, some employees are quite comfortable with privacy and

[232]Law – Ch4, s1, GDPR, 2016;

data protection as they have to think about these issues regularly in their day jobs, in more strategic or user facing roles. In contrast, those new to or unfamiliar with the concepts **feel lost, unsure where to start, who to ask, and what they are allowed to do with data**. MOZ, as a larger organisation, has an internal service to raise awareness and give advice around security and data protection law. The service helps employees manage risks posed by their projects, advising how to proceed or not. Participants feel how they approach the service dictates likelihood of getting approval. Going in with too many questions is less successful. They need to ask for advice on implementation, not permission.[233] In any case, they foresee a role for cards in shaping their relationship with the service, where more knowledge of law could rebalance the power asymmetry.

As Barry, MOZ Group 2 states:

"*If I had these [the cards], I could clarify in my head what I actually need to do, so rather than saying I want to put out all this data and obviously they are gonna say no, but If I said we are trying to achieve this thing, then they might be more like, receptive if I already have a bit of background in what I'm trying to do.*"

In the smaller businesses of SBA, the situation is quite different as they lack such in house services. Accordingly, the cards can be a starting point towards **empowering their position**. Many SBA members rely on either reading the law themselves, or going on training courses. Courses are still expensive, and accordingly, they want to find out as much as possible in advance of deciding to go. **Cards can be a useful starting point to get a handle on what they need to know, but they would like more detail so they can investigate further.** Even finding the relevant law and documents can be a huge challenge, hence the support needed for small organisations is greater than for MOZ. As Ted, Group 3 SBA explains:

---

233 *"it's probably just my biases but I feel like if I've got a question I'm not sure about a question on data protection but if I ask IAGS if I'm allowed to do something they're definitely going to say no [Amy]…haha yeah their default answer is like no [Christopher]… yeah exactly to then I'm like maybe I shouldn't ask them and I should figure it out myself [Amy]"… "I tend to go to them and ask how can I do this not can I do this… tell them what you want to achieve rather than how you are going to do it" [Adam]*

"*…we've been try to comply with regulations and it often comes down to getting some great big, as you say, 200-page document: carriage of dangerous goods by road was one of the things we were interested in and it becomes an absolute nightmare to even find which document you are interested in, and then which section you are interested in. So one of things I would like to see on these cards, if I was seriously contemplating using them within my business would be references on the card, where to go to next…*"

2. Managing Complexity

Responses: Risk Management and Granularity

The cards sensitise participants to the breadth of compliance requirements around designing personal data driven systems. Like many areas of law, data protection uses highly technical language, making it difficult to fully understand what obligations are faced, by whom and how to manage them. Data subjects (end users) and data processors/controllers (system designers) have a range of rights and responsibilities. **The cards prompt participants to reflect on not just the law but the perceived risks from non-compliance, and it pushes them to consider how to respond accordingly.** In this section we look at examples of how they manage the complexity of compliance during the design process. We would typify their responses as falling into three categories:

Balancing Risk and Utility

Balancing the risks of data handling against the utility of the system they are designing is a tricky process for participants. A good example is how participants deal with data minimisation. It mandates processing should be kept to the minimum necessary for purposes of the system or service. Ostensibly this is appealing to them: **it simplifies their obligations because broadly speaking, less personal data equals less risk**. Some already have strategies to minimise the data they collect, as SBA participant James discusses in the focus group. He explains he relies on others, i.e. the banks, to store the personal data, not his organisation:

"*what's the barest minimum I actually hold, and you don't hold much information … you don't hold a supplier's bank account details, for example, they arrive on the invoice every time he sends*

it and maybe you've got it stored in your bank system, so you don't need to store those records at all."

This mind-set shows **awareness of risks, and management strategies to alleviate their responsibility**. However, collecting less data is not always the default. As we know, many prominent business models involve data mining, analytics, and profiling for advertising or third party access, hence more data is collected. Equally, with home energy management systems, end users may want to access their data, so they can understand their consumption habits, lower costs or share the information with others. **The challenge then is for designers finding the right balance between their compliance risks and ensuring systems have utility for end users**. The following excerpt from a SBA Group 3 shows how risk aversion and utility are balanced:

> *Scott: default sharing (reads aloud).*[234]
> *All: Definitely not.*
> …
> *Ted: Actually, possibly, that. That last one is possibly interesting.*
> *Scott: Default sharing?*
> *Ted: yeah, if you like, as a utility company installing meter they've got no interest in sharing that data with anyone else. As the homeowner, you might want to share that data with some helpful website that can tell you you're paying more for your electricity from your current supplier than you'd do with someone else…*

In this space, we see scope for user centric regulation, where **participants balance legal risks with end user needs**, in order to create innovative responses. However, they need to know the **legal risks in the first place to respond accordingly**. During the INC focus group, participants explicitly stated having **awareness of legal requirements upfront is better**, as they can factor them in during the design process, as opposed to at the end when it is too late. As Patrick puts it, "*it is just they [legal] are different sets of constraints, there are constraints in anything that is creative, it doesn't stop you being creative"*. Building on this, we see **creative**

[234] Not legal, but constraint card; Card Text "The system should allow for default sharing with third parties"

responses to legal requirements from across the groups, often changing how user/technology interactions are designed. One example is, control may be increased through addition of RTBF requests actioned by hand swipe functions on intelligent public displays, or creating more ephemeral experiences, removing the need for anonymisation or long term data storage.

The most detailed discussions are around managing **granularity of the data** in a system. **They recognise there may be legitimate reasons for more detailed information but these need to be balanced against the user rights**. SBA Group 3, for example, discuss balancing their need for detailed feedback from deployed utility meter prototypes against access to data by other stakeholders, and maintaining legally required records of processing: [235]

> *"Ted: We are interested in seeing the very detailed technical data, so that may well be, in prototypes data is being sent to [utility company] and is being also sent to us and there might well be a regulatory interest in that happening.*
>
> *Scott: so your consideration is the bit that you provide in actually understanding how they might use it even if you don't control it.*
>
> *Ted:* ***we are not really interested in what they are doing with the data we send to them.*** *Yeah, we have no interest in that, but we do have… I suppose it's like Rolls Royce have an interest in getting data back from aeroplanes about how their engines are performing,* ***we have interest in getting data back from our meters to see how our meters are performing, which long-term we don't want to have to collect because if there are thousands of meters out there, we don't want to…we just want them to work.*** *but in the prototyping stage, we would be interested in getting all sorts of health data back from… so to that extent we possibly do come under a lot of these things which we have been saying are utility companies' problem."*

[235] Law - Article 30, GDPR, 2016; Card Text- "**Record Keeping:** Comprehensive records of processing need to be maintained by controllers and processors eg categories of data, recipients, transfers abroad, security measures in place"

However, more often participants are worried about the privacy risks. **In particular, spotting patterns from plotting and correlating data from physical devices can detect details like house occupancy, lifestyle and routines**. As Christine, SBA Group 3 puts it "*with this system [smart home management], you'd be pinging the things, the IoT, data would be pinging real things, talking to or communicating constantly between real things, but things you'd interact with on a daily basis, things that actually tells a story about our life, time we go to bed, time we switch off lights, time we wake up, time we are in the bath, come in, time we cook…, time kids back from school*".

Controlling **legitimate and illegitimate access to this data is a key concern**, with the latter bringing security considerations to the fore. Whilst they offer solutions like cryptography, strong passwords and robust authentication processes, the **SBA participants in particular show fear about hacking and maintaining security against breaches, particularly for the IoT**.

In general, they recognise **inferences** are not commensurate with reality, and accordingly need to protect against overly literal interpretations based on the data. As SBA's Andrew states "*the trouble is that they get some data but they don't get the intentions behind the data, they suddenly realise you are buying lots of wine, is it because you're having a party or you're an alcoholic or something else, so they get part of the information.*" MOZ participants are particularly aware of the impacts of inferences being drawn, where linking of non-personal data points and entire datasets can reveal otherwise invisible information. **Looking beyond just external flows of data (i.e. to third parties) they focus on how this information is used internally within the domestic setting**. As discussed above, homes are contested social spaces with politics and hierarchies. As Alan and Mark, Group 1, MOZ discussing their smart energy management system show:

"*Alan – it become[s] more of sort of privacy between the members of the household. Actually, 'you are here on Saturday night, look how much energy you've used. what are you doing? you were supposed to be out this Saturday night, you told me you were going away for the weekend and what are you doing at home.' Data privacy within the family unit.*

Mark - you don't use [an] electric toothbrush dad?!"

As with external access to data, participants recognise the **need to adjust what level of detail users get about systems internally, to mitigate family conflict, relying on trends, or aggregates as opposed to more granular information**.

Pragmatism and User Centricity

In addition to risk based approaches to legal requirements, we also observe the **pragmatic, user centric nature** of participant responses. They consider a wide spectrum of **user interests during design like convenience, comfort, protection of vulnerability and against prejudice**. When faced with ensuring the system is 'low energy', for example,[236] MOZ Group 2 consider multiple angles. How device battery life is managed shapes the end user experience positively or negatively. For participants' this may sway whether to run analytics locally (using more power) or outsource to cloud backend (less power). More indirectly, poor battery management may impact data collection, leading to incomplete data profiles and incomplete reflection of the user. It can even shape what cloud provider they use, where most energy efficient provider (e.g. with 'green' server farms) might not be the most secure, exposing user data to risk. **This is not a legal requirement, yet brings a range of legal concerns to the fore, like data security or accuracy of profiling**.[237] Barry, Amy and Christopher debate the final point, tying back to our earlier discussion about values too:

"Christopher - does this low energy restriction somehow jeopardise the data security in the way that you have to think about infrastructure?

Amy - what if your lowest energy provider was outside of UK? – how do you then choose between? – then you can't go with your cheapest energy provider

Barry - because there is no alignment between the values of you and your energy provider potentially."

---

[236] Deliberately ambiguous

[237] Accuracy – Article 5(d), GDPR "Personal Data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay"

We see the combination of this pragmatism and user centricity in more detail through responses to two legal concepts: **consent and controls on international data transfer**. We explore these below:

Within the cards, consent appears in multiple guises. The three main consent cards state:

"User Consent 1: Consent must be freely given. The user must make a specific, informed and unambiguous agreement to data processing.[238]"

"User Consent 2: Consent must be provable. It can be withdrawn by the user at any time, and when it is given as part of a written contract it must be flagged up in clear and plain language.[239]"

"Children and Consent: Consent must be given or authorised by parents when children under 16 are using online shopping, social media and similar types of services and systems.[240]"

With the first two cards, both MOZ groups show particular concern around clear/plain language, and the informed element of consent. For them, non-native language users will face particular challenges as they will not understand the text or intent of a consent agreement. Pragmatically, this means ensuring consent documents are available in a user's native language too. The discussion by MOZ Group 1, shows this

"*Amy - it might mean that if you know that a certain proportion of your user base doesn't have great English you'd might make sure you really carefully word it so it doesn't use any…*
Adam - …yeah like no legal speak or jargon
Derek - or if you know what the first language is likely to be, then you could provide two different versions…
Amy - yeah, translations"

[238] Article 4(11), GDPR, 2016
[239] Article 7, GDPR, 2016
[240] Article 8, GDPR, 2016

However, MOZ Group 2 focus **not just on the need for clear, legible text, but the need for user's information comprehension**. This is harder to achieve, as informed consent needs more than just native language translations, **it requires communication of intent, irrespective of language,** as the following quote captures.

"R*andy - it's about what you're consenting to, if you're comprehension is out.*
Irvin - it's about the ambiguity of like the terms and how they are used.
Alan - well, there are two issues aren't there. 1) making it clear what you are doing. 2) making it clear for people who use different languages…"

Despite this aspirational commitment to user interests, both groups also recognise the commercial reality of consent where it is still seen as a silver bullet that legitimises processing, despite inadequacies in tick boxes, form contracts and opt in/opt out mechanisms. **Within their discussion they struggle to reconcile the realities of what consent is, with their more aspirational vision of what consent needs to be.**

With the **latter card on children and consent**, SBA Group 4 consider difficulties around obtaining **consent in the home.** Unsure if they are designing for consent from all occupants or relying on parents, the participants show sensitivity to how their design can shape the manifestation of under 16's rights in the home. Focusing on the rights of children **as users**, they **consider whilst parents have responsibilities, domestic hierarchies may be reinforced by the consent process they design**. Indeed, carrying this forward, they question how the transition will be managed when the child becomes seventeen and consents for her/himself. They need to consider **how to design opt out mechanisms so over 16 can withdraw their consent easily within the social dynamics of the home**.

> "*Christine – I just think that building this system, and you're building it for a house, and the number of inhabitants for the house, do we then have to build in consent that everyone in that house agrees, the end users all need to, can't just have the head of the household.*

Barry – I'd have thought so, but the head of household if you've got under 16s would have to agree on their behalf

Christine – agree on their behalf and when they are no longer 16 and consenting then they'd have to do it?

Barry – how would you opt out?

Christine – how do you manage data? on an individual basis or a household basis?"

Next we consider how the **pragmatism and user centricity factor into controls on international data transfer**, through our two cards:

"**Data Sent Outside Europe:** Ordinarily, data should not be transferred out of the European Economic Area. Sometimes, it can be sent to specific countries that guarantee data protection like Canada or New Zealand."[241]

"USA: The EU-US Safe Harbor Agreement is now invalid. A new framework is emerging, but currently legal transfer of data requires extra safeguards like special contract clauses"[242]

The global nature of the regulatory landscape adds complexity for participants. Whilst aware of the relevance of third country laws, **they also are aware enforcement varies, and they need to manage this in their roles**, as SBA discuss below:

"Ted - Possibly, the country of residence is one that's triggering thoughts of - we just don't have to worry about the law in this country you might have to worry about what's the law in Brazil or Africa or something.

James: most companies that are manufacturing anything, are bound to be global in some respect.

[241] Chapter 5, GDPR, 2016

[242] the *EU-US Data Shield* has since passed.

Stuart: … how people in some countries observe the law is interesting. Seeming that there might be a law written but the way they actually observe it might be quite different. So we get this bit even with France. You know, we talk about EU legislation… and the French office just say… 'Ahhhhh.. it's really a guideline. It's not really a law.'"

Nevertheless, in response to data transfer limitations, the MOZ and SBA participants opt **for pragmatic approaches, focusing on ways to avoid sending data outside the EU**. This often manifests in rethinking how they design the system, looking at how to store data locally or avoid storage in the 'cloud'. When using the cloud, they wanted to ensure they are using UK or EU providers. Again, with pragmatic focus, using **US servers may require involvement of legal teams to draft contract clauses, adding costs for their fees, so participants could use this as a basis for avoiding US cloud services**. As we see in the MOZ Group 2 discussion, they already use local storage to address these kinds of risks from international transfer:

"*Amy: basically just avoid at all costs – just don't put it in America… probably kind of design it so you avoid.*

- Christopher: but MOZ has to use their own analytics

- Barry: yeah that is why we don't use Google analytics because it is probably States based…

- Amy: so it basically means you'd have to design it in from the start that you're not going to rely on the USA

- Derek: yeah just avoid international or if you are going to, probably get a load of lawyers in"

3. Sense-Making Strategies

Support Mechanisms: Network, Community and Leadership

Lastly, we are interested in what **strategies designers use to make sense of their regulatory obligations.** Overwhelmingly, support networks and their professional community emerge as an invaluable mechanism for the SBA and INC participants. In MOZ, **leadership within the organisation and support from internal advice services** are more prominent.

For SBA groups, **self-help** is key as they lack financial resources to resort to a default of professional help. As Ted, SBA Group 3, explains in the context of training courses:

"- *Ted: being cost-conscious, lets put it that way, we would always try and find out how big an issue we are dealing with before we go off on a training course. There is always this feeling that we go off on a training course that costs £400 ... just to tell you stuff you already knew.*"

Importantly, there is a broad network of forums that they draw on for support. This includes industry trade associations/network, technical societies and professional bodies like the IEEE or Imech,[243]local Chamber of Commerce (CoC), service providers like accountants or website designers and the Federation of Small Businesses (FSB). How they **access support** in their community varies. More formally FSB and CoC, **offer legal advice** to members and seminars or meetings of trade associations provide forums to share advice and learn. More informally, they draw on their **social network, talking to other small business owners who understand the issues**, particularly trusted, well known individuals. Importantly, face to face contact is a key channel, so whilst online social networks like Twitter or LinkedIn Groups, websites or search engines play a supporting role (either at the initial stages or as a last resort), traditional human interaction in their community is central. The discussion in the SBA focus group shows this, as they discuss how to find an expert:

[243] Institute of Mechanical Engineers

"*Christine: how do you get…where do you go to... find the expert?*
Barry: find the expert, like you were saying, word of mouth at that point.
Christine: it is, it often is.
Barry: like with anything you don't know, if your business can't do that themselves then generally a word of mouth seems to be where you'd want to go isn't it, but you will look beforehand about...
James: yeah, you Google the basic problem but you wouldn't Google to find someone to do it.
Barry: no. no. I don't think I'll feel comfortable doing that.
Christine: no no. definitely…"

Participants state they look to the UK Data Protection Regulator, the ICO for support, but due to the vagueness of their guidance, it has limited utility. In contrast, within INC, they discuss the volume of useful, free advice being offered by big law firms, as Patrick states:

"*I go to a few trusted legal sources, there is actually quite a lot of free legal advice if you know the right forums to look at. Lawyers are giving all the information away, not specific, a lot of the publications from the big law firms, briefing documents tell you an awful lot, now they don't tell you about your specific situation, because that is what you pay them for, but if you've got the time and interest and knowledge in it. I've learned about the law in the last 5 years and become interested as a result, but only in this very specific area.*

Within MOZ, they have more internal support network, from the internal advice giving service discussed above and from management leadership. With the latter, project managers and team leaders may divide labour so they look at the relevant law instead of their team members. Barry, Group 1, explained his experience with this in a recent project:

"Barry - *we are starting to make a new tool…the first thing I thought of what are the rights relating to data and IP…we've got a really good director and she had gone through*

and looked at all the terms and conditions and privacy policies so I didn't have to and supported me in that way"

Cards as Awareness Raising: What Next?

Overall, participants like the cards and workshop as a medium for learning about these issues. They are concise, creative, fun, generate discussion by structuring thought around a specific system and bring in new elements that would not otherwise be considered. As INC's Patrick states "*I think what it's [the workshop] really shown is even if you take something very simple it quickly grows into something very complex.*" The groups need moderation to help keep them on track, and we observe their need for reassurance and further explanation about the tasks, workshop goals and their approach. The workshop model works well as we are on hand to advise.

In general, MOZ provide the most critical and detailed insight into the cards as a tool and scope for improvement, hence we consider their perspectives here briefly. The process of turning was commended as it helps keep discussion moving and working through the issues. They feel some cards are so important they should be mandatory, like user rights and designer responsibilities. Some cards initially appear irrelevant, but after pausing to reflect, they quickly link them into the discussions, as we saw above with low energy and user interests. With the process itself, they approach it as a challenge, perhaps drawing on the playing card aesthetic of the cards. With iconography and design, they note icons are not strong enough to standalone without text, but different types of participant may want different visual design:

"*Christopher - I didn't really pay much attention to the symbols actually – I was more reading, more of a text based person …well they do say that text is a lot better than icons or stuff just that you do read*
Amy - but that would look rubbish if that was just a wall of text – I think it depends what the point is…
Christopher - maybe it is because I'm a programmer and that is all I do"

They pick up on managing **translation** from law to cards too, an issue discussed above, where there is a tension between balancing legal detail and design of cards. As Mark puts it, "*so I think it's good. The only thing I thought about... had a quick squiz at some of the legal ones … I thought that... the rights ones (end user rights). I think, for me at least, just the couple I looked at, if any of them would benefit from having more explanation…because the legality, the precision of it is the issue, yeah?*"

As mentioned above, different participants have varying levels of experience with law, hence those more comfortable with law require less support. For SBA, the **cards can be integrated into their business if there is further supporting material**, such as providing the legal source of the cards, so they could go and look at it in more detail. As Ted puts it "*so it's giving you the headline, but I am thinking what is the legal standing of this statement which I've read on a playing card. I can't really hold this [the card] up in court…*". A primer is suggested to help with the learning curve and to build familiarity with the concepts. Support materials could include **booklets, checklists, websites, decision trees**, or just working through the deck or background key legal concepts for an hour before the workshop. In terms of use within their everyday work, with INC, Oliver saw how they could fit into his workflow "*the good thing about these things is I can imagine using this being useful in other contexts where you've got whiteboards, printed papers about the system you're designing or working on and these that sit together".* For MOZ, the cards should be used early during scoping work and used across teams involved in a project, as Irvin states "*I think it needs to be baked in right at the beginning… you have to actually actively go, you need to go, right from beginning, not like, oh now lets talk about that. It's like accessibility…".*

The approach groups take to using the cards is key too. One SBA group looks **through all cards, and the others quickly and randomly pick some**. With random choosing, they feel it keeps them focused but brings in different angles, whereas those that choose to systematically work through **all** the cards during their session run out of time. Indeed, the latter group appears overwhelmed by the end, as this telling quote at the end of the workshop shows:

"

Ted: … and 'Right of access' (Reads text & waits for responses). 'Rights to information' (Reads text). 'Information provision' (reads text). I don't fancy being someone who collects user data

James: well, this is pretty onerous stuff, isn't it?

Stuart: well it's a problem.

James: it is, yeah.

Stuart: it's a problem.

Stuart: yeah."

In contrast, with the turning **process** in the cards[244] both MOZ groups want to see more. Whilst appreciating the need to limit them due to risk of being overwhelmed, they show frustration they only got a small cross section of the cards:

"Adam - I'm just thinking what is in all the other cards though…

Amy- yeah, I'd want to know what is on these ones as well…

Adam - I feel like I'm getting a slice, but I can't design it on the basis of this…it's like its literally randomly thrown up stuff

Barry - yeah bite size stuff…

Adam - I'd want to go put every card out there and read through it. I'd want a big checklist of stuff"

In general, the cards **raise awareness about legal issues and prompt reflection**. Participants see the value in this, as SBA, Group 4 James puts it "*even if it brought forward one thing you hadn't thought of, it would be extremely useful. It's not a particularly onerous exercise.*" C**rucially, what to do next is not defined and they crave further guidance, because once sensitised to the issues, they want a roadmap for how to move forward.** This could vary from further training or seminars, or more self-help tools. They express desire for help prioritising what to handle first, and where to find answers. One example of a particular stumbling block is defining the

[244] See appendix of method; with MOZ they turned in sequence of 1 system card, 1 user card, 2 constraints and 2 legal cards. They had strictly moderated timeframes eg 5 minutes to discuss system card, 5 minutes for users and random turning. For subsequent groups we were less strict on time, letting them decide when they felt ready to pick up more cards. They still followed the same ordering (system, user, constraint, legal) but they may have picked up all cards early in the workshop, or they could look through all cards over 45 minutes. We wanted to see different ways cards would be used.

scope of personal data. Participants propose tackling this with a list of examples that differentiate personal/non-personal data so they can understand more easily. Another proposed tool is a repository of case studies of how other organisations have responded to legal issues, to develop examples of best practice for a particular sector, coupled with flow diagrams of precautions to take. This would need to be balanced against confidentiality and commercial sensitivity on sharing examples. Part of the discussion of SBA focus group states:

> *"Stuart: I think higher level is just … is there a business like mine? What challenges have they faced? What things have done to try to protect themselves, and then once you've got an appreciation ... then I think you've got some questions you can go and ask.*
> *Barry: next steps.*
> *Christine: case studies yeah.*
> *Stuart: you got a starting point."*

We now summarise the findings from our workshops.

Summary

In conclusion, our model of regulatory literacy unpacks the nature of the new role of designers as regulators doing user centric regulation. It provides richer insight into how and why designers engage with legal concepts in practice, highlighting where competencies exist and where greater support is needed. For clarity, we break our findings and model down into three main elements, **regulatory interaction; sense-making strategies and managing complexity**.

A. Regulatory Interaction

1. Motivations: A Spectrum of Values and Responsibilities: As we see, there are a range of motivations for why designers engage with law and compliance. These include values like protection of reputation, guarding against bad publicity, litigation or loss of public trust. Within this, there is a desire to uphold certain professional ethical standards beyond just legal compliance, and on a personal level, a moral standard of desirable/undesirable courses of action in design.

Necessity especially in SMEs, is another factor, where there may not be anyone else to look at compliance but managing directors or heads of departments (eg finance, accounting). Accordingly, SMEs often rationalise their responsibility for data handling as being shared with other bigger actors in the personal data supply chain, those with greater resources.

2. Negotiating with the Law: Authority of law is an important factor for prompting engagement, as it mandates action. However, designers possess various strengths and weaknesses when navigating around legal language and concepts**.** Experienced participants show greater understanding of law and legal concepts, but overall, groups delve into deep discussion of quite technical legal issues, often grasping concepts straight away. They do not struggle greatly with legal language, finding ways to understand terms they are unsure by drawing on personal experience, group discussion, analogies, and the definition cards. They formulate rich understanding of legal terms, often capturing the rationale and implications of technical legal terms aptly, as we see with personal data and data controllers/processors.

The knowledge provided by the cards has different implications in SMEs and larger organisations. Within MOZ, cards can empower employees to reshape the relationship they have with internal advice giving bodies by giving them greater awareness of risks to negotiate progression of their projects. Within SMEs, they may need to read law anyway, so cards can provide an easier starting point to understand issues. They look for even more detail from the cards, to be as well informed as possible, and they help them understand gaps in knowledge, and if they need to go on a training course.

B. Sense-making strategies

3. Support Mechanisms with Networks, Community and Leadership: Self-help is key for resource strapped SMEs/start-ups, hence support networks and their professional community are an invaluable mechanism to get a grasp on legal issues. These forums vary from industry trade associations/network, technical societies and professional bodies, local Chamber of Commerce (CoC), service

providers like accountants or website designers and the Federation of Small Businesses (FSB). They access support via legal advice from memberships of these types of organisations or seminars and meetings of trade associations. However, their social network is key, with face to face contact with other small businesses being preferred to online support (although it plays a role too). Free advice from big law firms can be useful, but state regulator the ICO does not provide much support.

In larger organisations, leadership within the organisation from managers and support from internal advice giving bodies is key to addressing legal concerns.

4. Cards as Awareness Raising, but what next? - The cards do their job of raising awareness about legal issues and prompting reflection**.** Participants feel they are useful concise, creative, fun, tool that generates discussion by structuring thought around a specific system and bring in new elements that would not otherwise be considered. With more critical feedback, additional supporting material is suggested like booklets, checklists, websites, decision trees, primer sessions. For some, the methodology of use needs refinement, where some participants want to see all cards at once, but struggle with timing. Others feel random turning gives too narrow a perspective on the issues (although pragmatically they understand why). The biggest critique is, whilst the cards raise awareness, they do not say what to do next. They want a roadmap of what to do next, with increased support in how to move forward. This varies from training and seminars, self-help tools, lists of examples of legal terms (eg personal data) and a repository of case studies to help develop best practice.

C. Managing Complexity

5. Designer Responses - Risk Management, Utility and Granularity of Data:

Participants consider the tension between risk and utility in handling personal data. Often this requires finding the right balance between their compliance risks, legitimate need for more detailed information and ensuring systems have utility for end users, and don't negatively impact their rights. They do this through different

creative strategies. Data minimisation is key, as it simplifies their obligations because broadly speaking, less personal data equals less risk. Redesigning user interactions is another approach, for example creating ephemerality or increasing control over data for the RTBF.

However, upfront awareness of risks in the first place is necessary so they can respond. Managing granularity is a key concern, as is protecting against overly literal interpretations based on the data because designers are aware inferences are not commensurate with reality.

Overall privacy risks are a key concern. Designers are aware of the risks for users posed by spotting patterns with plotting and correlating of data from different physical devices. This can detect details like house occupancy, lifestyle and routines. Accordingly, controlling legitimate and illegitimate access to this data is a key concern, where safeguards like passwords, encryption etc can be used. However, SBA participants in particular show fear about hacking and maintaining security against breaches, particularly for the IoT. This involves looking beyond just external flows of data (i.e. to third parties) and they focus on how this information is used internally within the domestic setting. Designers may need to adjust what level of detail users get about systems internally, in order to mitigate family conflict. This may shift to creating systems reliant on trends or aggregates as opposed to more granular information.

6. Pragmatism and User Centricity

We see user centricity and pragmatism manifest prominently in the context of two legal issues, consent and third country transfer. Designers have key concern for convenience, comfort, protection of vulnerability and guarding against prejudice from data with users.

With consent, there is a rich awareness of impact on users, where it is important not just for clear, legible text, perhaps in multiple languages, but the need for user's information comprehension. This requires communication of intent, irrespective of language. Despite this focus on user interests, participants struggle to reconcile

the commercial realities of how consent is used, with their more aspirational vision of what consent needs to be.

In the complex social space of the home, consent mechanisms need to ensure they protect interests of child users, which may mean designing approaches into the system that reflect the social dynamics and appreciate hierarchies within the home (eg where parents' consent on behalf of under 16s, but once they turn 17 they need to be able to consent for themselves).

The pragmatism and user centricity of designers' factor into how they design controls over international data transfer too. The global nature of the regulatory landscape adds complexity for participants, although they are aware enforcement varies in different countries and they need to manage this in their roles. Pragmatically, they respond by focusing on ways to avoid sending data outside the EU, primarily looking at how a system can store data locally and avoid storage in the 'cloud'. This can be tied to a business rationale too, where use of cloud, with US servers, involves legal teams to draft contract clauses, adding costs, it could be cheaper to store data locally. Following these findings, we now draw a set of conclusions to pull together the thesis as a whole.

Chapter 10. Thesis Conclusions

Overall this thesis posed the question: how we can understand the role of designers in regulation of emerging technologies? We have answered this from four primary perspectives: conceptual, legal, practical and design. Often, we have focused on the specific context of the domestic internet of things and information privacy by design to situate our investigation. In these conclusions, we briefly reaffirm our key arguments, where further work is necessary, and situate the implications of the research.

Within Part I we asked how to conceptually align IT law and HCI in order to situate the role of technology designers in regulation. To do this, we proposed the concept of 'user centric regulation'. This is based on a number of shifts within HCI and IT law.

The concept of regulation has broadened to the extent that the creators of technology, as mediators of user behaviour, are now regulators. The nature of designers as regulators is not settled, and they need to find ways to establish their legitimacy, as they lack the same authority as the state to regulate. Within technology regulation, the role of design is understood through abstract, social systems theory level models, where actual user interactions with technologies are not considered. This is in contrast to the interaction led approaches of HCI, where designers look at how technologies operate in context, reflecting the social dynamics of use and how the technology may mediate behaviour of users. We argue their user centric approach is a route to establishing legitimacy, hence, there needs to be a shift away from systems theory, towards interaction led models to situate the role of designers in regulation.

Whilst HCI designers can increase the attention paid to users, they are not currently explicitly orientated to regulatory concerns. However, we find there is a growing engagement with their broader social and ethical responsibilities, with attempts to situate these, particularly through the incorporation of human values in design. This has not yet extended to legal dimensions in design, but in order to align these two

communities, we argue it should be. We use our concept of user centric regulation to encapsulate these changes.

Having positioned the role of designers through conceptual alignment, Part II of the thesis provided insight into the legal dimensions of their responsibilities and how they can respond accordingly. Designers as regulators need support to understand their role, and we used two detailed case studies on doing PbD for the domestic IoT and smart metering to contextualise the regulatory questions they face. To delve into the detail, we critically evaluated what PbD is and challenges it faces in application. We then assessed the nature of these emerging technologies, regulatory dimensions and user experiences of living with these systems. To provide analysis orientated to designers, we mapped the personal data ecosystem, concentrating on the interactions, relationships and information flows between users, designers, technologies and third parties. To narrow our inquiry, we looked at how designers can respond to two specific regulatory challenges: user control over personal data flows in domestic IoT ecosystems, and regulating access to consumption data for smart metering.

We outlined how, through a user centric perspective, designers as regulators are able to respond to these two challenges. With increasing user control over information flows, we showed an approach to redesigning consent mechanisms by thinking about the holistic user experience and interactions with IoT devices, as opposed to existing contract based methods. With user management of access to smart meter consumption data, we considered techniques to increase transparency and control. Through provenance tracking and personal data containers, user awareness of who is accessing their data, when, why, and so forth can be raised. These detailed case studies provide valuable legal analysis of emerging technologies. More importantly, they unpack what designers can provide as regulators, by drawing on concepts from their own domain, and applying these in a user centric manner.

Building on these case studies, in Part III, we wanted to go beyond the conceptual and legal analysis, to understand the practical challenges designers as regulators face in doing privacy by design for the internet of things. Therefore, we turned to

practice, specifically the experience of thirteen leading UK experts in information technology law and design. Through analysis of semi structured interviews, we obtained greater insight into the contested terms of IoT and PbD, but also found overarching business, technological and regulatory perspectives that need to be reflected in the practice of doing PbD. Understanding dominant business models within the IoT market, and building on the limited motivations to engage with regulation and compliance is important. The differentiated resources to do PbD cannot be ignored. Even if motivations for PbD exist, SMEs and start-ups do not have the same stability, organisation, or financial means to engage with compliance as large multinationals do. Consequently, without greater support for SMEs and start-ups, PbD in practice is likely to be fragmented.

Bringing legal compliance into the design process early requires tools to support greater interaction between lawyers and designers. This is particularly around how lawyers, as risk advisers, align with goals of designers seeking to build better systems. Communicating the relevance of law to designers and supporting their engagement therein are two prominent aspects. Strategies for doing this vary, including translating law into simpler forms, like tailored codes of practice, actionable guidelines and prompting reflection on impacts of non-compliance within their own personal or professional lives.

PbD needs to reflect designers conflicted agendas within organisations, showing design does not occur in a vacuum, but instead is subject to interests of a range of different stakeholders from business strategy to information security departments and of course, legal. Designers want to build with certainty, but legal concepts do not provide this, and what PbD requires is often unclear to them.

Accordingly, PbD in practice needs clarity, and looking beyond the top level term, to how it manifests in specific sectors, contexts and technologies can help with this. Making legal language more accessible to designers coupled with greater interaction between technologists and state regulators are other approaches. With the latter, the range of regulatory challenges IoT pose mean risk assessment is hard and experts expressed desire for less strict, more commercially orientated enforcement of the law to enable growth of the emerging IoT market. However, uncertainty

persists as guidance on compliance does not keep pace with technological change. Awareness raising and engagement with state regulators can help management of compliance risk, and consequently, resources. To conclude, this part shows the range of elements that need to be considered in doing PbD in practice. To situate the role of designers therein, greater support is necessary to enable them to engage with law.

Therefore, in Part 4 we develop an approach that does this. We show how we can support technology designers' engagement with data protection law in order to do PbD in practice. We wanted to move privacy by design from theory into practice, and our information privacy by design cards work towards this. By translating the GDPR into a deck of physical playing cards, we communicate legal principles, concepts and values to technology designers in a structured manner. They make legalese more accessible and communicate the relevance of law to designers through workshops using the cards. We tested these in a series of six such workshops with twenty-four technology designers from three settings: large global media firm ("MOZ"); a small technology businesses trade association ("SBA"); and an innovation network centre for SMEs/start-ups ("INC")). The range of participants highlighted the breadth of actors involved in the design process, from those working in business strategy and management to technology design and research.

The workshops showed us how designers negotiate around legal concepts. In particular, we observed their competencies in dealing with law and what support is required to help them understand their role as regulators. We framed our findings within the concept of regulatory literacy, in order to encapsulate the range of skills, knowledge and strategies designers possess. In particular, we look at their interaction with regulation, their sense-making strategies, and how they manage complexity.

Regulatory interaction is driven by necessity and authority of law in SMEs, whereas in larger companies their focus is beyond compliance, instead on upholding professional values like reputation and trust. Negotiating around technical legal terms on the cards, designers bring their own perspectives and experience to bear,

often showing rich understanding of the rationale and implications behind law. Foreseen wider implications of the cards vary, but are often framed as a tool to empower designers. With larger organisations, cards can provide greater awareness of risk, helping designers to reshape relationships with other internal stakeholders eg security department. For SMEs/start-ups, they can provide a more accessible entry point to legal issues, to see if further training is necessary, thus helping management of limited resources.

We observed sense making strategies around law vary depending on the organisation. With SMEs/start-ups, self-help is critical. Face to face contact with other businesses is a preferred mechanism to understand legal issues. Their professional community, trade associations and social networks provide vital peer support. Legal advice can be accessed through a range of sources, from membership of formal organisations (eg Chambers of Commerce), free advice on big law firms, and through service providers (eg accountants or web designers). In large organisations, managerial leadership and internal advice bodies are vital. Furthermore, whilst cards raise awareness in an enjoyable manner, they do not provide a roadmap of what to do next, hence a range of further resources and supporting material are necessary. This is further work, as discussed below.

Lastly, we observed designers manage complexity in a number of ways. Balancing risk and utility whilst handling personal data is a challenge. They need to balance their compliance risks, legitimate need for more detailed information, ensure systems have utility for end users, and avoid negative impact on their rights. Responses often involve managing granularity of flows of data and managing risks stemming from legitimate (third party) or illegitimate (hacker) access to that data. Other approaches involve redesigning systems, for example, faced with rules on third country data transfer, designers often respond by avoiding the cloud, preferring local data storage to avoid associated legal costs to guarantee compliance.

The user is central in formulation of responses to legal issues, often in a very pragmatic manner. Their convenience, comfort, and protection of their data factor highly in the designers' approaches. As we can see, by presenting designers with legal concepts in a more accessible medium, they can reflect on their

responsibilities, with pragmatic and user centric responses manifesting. Accordingly, tools like the cards are invaluable for supporting, situating and structuring the role of designers as regulators doing user centric regulation.

We now present where further work is necessary, before concluding with our contributions, and the implications therein.

Further Work

We recognise there are number of areas of further work stemming from the thesis, and we present these briefly below.

Firstly, we focused our investigation on those who design these technologies, to support their understanding of their role as regulators and to develop their awareness of legal concepts. Accordingly, we primarily looked at design led solutions from the 'human' perspective of designers and users. We did not focus on technical aspects of how to instantiate legal norms in programming languages, in order to embed design responses at that level. Therefore, critical work analysing the legal theory on formulations of rules and legal norms, and examining how these are translated into computational language could complement this research.

Secondly, we primarily focus on data protection law, understanding the concept of user centric regulation through information privacy by design. However, there are other domains of law sitting at the interface with design, and it would be beneficial to extend this concept into areas like accessibility, product safety or environmental protection laws.

Thirdly, our case studies in part II were developed from approaches including extensive documental analysis, international research visits, workshop participation and so forth. This worked well for developing our legal analysis. However, further work conducting design ethnographies (Crabtree et al, 2012) focused explicitly on regulatory dimensions of users' interactions with emerging technologies would be useful. This would provide insight into how the technology challenges user rights

in context, how the technology mediates relationships and behaviours for different rights, and how designers respond.

Fourthly, our interviews were conducted with a broad range of expert actors from technology law and design. Our interest was to explore multiple dimensions of information privacy by design for the internet of things in practice. However, further work, with a focus on different, narrower groups of interviewees, would be valuable. For example, interviewing solely user interface designers or requirements engineers could help establish a tighter understanding of perceptions of UCR within a specific group. This would help inform how different types of designers perceive their role in regulation.

Fifthly, whilst the six cards workshops provided us a wealth of data, we would like to extend our approach to observe either whole or part of the design process around an IoT product or service in an SME/start-up and large organisation. This would provide rich, contextual understanding of how regulatory concerns manifest at different points in the design cycle, how different designers respond, and the approaches taken. This could be conducted in different sectors too, such as health informatics, intelligent mobility, and education analytics. This approach would extend our understanding in a more targeted direction, in contrast to the more exploratory workshops where participants build a hypothetical system.

Sixthly, as the cards are based on new legislation, they do not incorporate interpretative elements like case law (as none exists yet), expert opinion or state regulatory guidance. Keeping the card text reflective of legal changes and up to date is a key issue for this physical tool. This requires developing ways to augment the cards with new information, but also creating an approach for oversight, updating and maintaining the information. Further work is necessary to work out how best to do this, in order to protect the longevity of the cards as a reliable resource for designers.

Lastly, the cards are one approach and medium for communicating legal principles to designers. We have learnt a lot from them, and will continue to develop them as an approach. However, there is further work to be done in developing a range of

tools, looking at other mediums to communicate the law. As starting points, participants raised the desire for other tools to support cards, like training, checklists, websites, decision trees and crowdsourced best practice, to name a few. Investigating which are most apt through prototypes and evaluation with designers would be a useful line of inquiry.

Key Contributions

In terms of contributions, the thesis is neither solely targeted to the IT law or HCI communities, but instead offers a novel, multidisciplinary contribution to both. Practically, the breadth of work here has implications and insights for legal and HCI researchers, practitioners, regulators, and different organisations, from SMEs/start-ups to larger companies. Furthermore, the overall goal of this research is to show how to bring the two broad communities together, to begin the process of building a shared conceptual understanding and offering practical approaches to help both appreciate the role of designers in regulation of emerging technologies. Key contributions can be summarised as:

- **We provide a critical, conceptual investigation of the role of technology designers in regulation.** This consolidates, evaluates, and aligns a range of disparate theories and perspectives. It draws particularly on human computer interaction (HCI) and information technology (IT) law. We draw together our critique of both fields under the **concept of user centric regulation**. This advocates a new, user focused, interaction led approach to understanding the role of designers in regulation. It draws on the turn to human values and societal issues in HCI, and the increasing reliance in IT law on design for regulation of emerging technologies.

- We present two **detailed case studies of emerging technologies** (domestic internet of things and smart metering) mapping the emerging legal landscape and challenges therein. We situate the role of designers, as regulators, within this space, and show how they can respond accordingly through their user centric focus.

- We analyse practical experiences from leading experts in technology design and regulation to understand the challenges of **doing information privacy by design (PbD)** for the IoT. We present our findings within the framing of **technological, business and regulatory** perspectives.

- We present a design tool, information privacy by design cards, to support designers in doing PbD. This tool has been designed, tested and refined, providing us with a practical approach to doing user centric regulation. Based on our findings from using the cards, we provide the concept of **regulatory literacy** to clearly conceptualise the role of designers in regulation.

Bibliography

1. Aarts, E., & Marzano, S. (2003) *The New Everyday: Views on Ambient Intelligence,* 010 Publishers, Rotterdam, Netherlands

2. Abowd, G.D. and Mynatt, E.D. (2000) Charting Past, Present and Future Research in Ubiquitous Computing, *ACM TOCHI,* 7(1), 29-58

3. Acar, G. et al (2014) The Web Never Forgets: Persistent Tracking Mechanisms in the Wild, *Proceedings of CCS 2014,* 674-689

4. ACM Code of Ethics and Professional Conduct (1992) at https://www.acm.org/about-acm/acm-code-of-ethics-and-professional-conduct

5. Adams, A. A. (2015) Possessing Mobile Devices. *IEEE Security and Privacy Magazine,* 13 (6), 89-95

6. Akrich, M. (1992) The de-scription of technological objects, in Bijker, W.E and Law, J. (eds.), *Shaping Technology / Building Society*. Cambridge: MIT Press, pp. 205-224.

7. Alsheikh. T. et al (2011) Whose Value-Sensitive Design: A Study of Long-Distance Relationships in an Arabic Cultural Context, *CSCW '11*, 75-84 http://research.microsoft.com/apps/pubs/default.aspx?id=149025

8. Anderson, R. (1994) Representations and Requirements: The Value of Ethnography in System Design, *Human Computer Interaction* 9, 151-182

9. Arkko, J et al, (2015) *IETF RC 7452: Architectural Considerations in Smart Object Networking,* Internet Engineering Task Force, Fremont, US

10. Article 29 Working Party (2011) Opinion 12/2011 on Smart Metering, *European Commission*, Brussels

11. Article 29 Working Party (2011b) Opinion 15/2011 on Consent, *European Commission*, Brussels

12. Article 29 Working Party (2014) Opinion 8/2014 on the Recent Developments on the Internet of Things WP 23, *European Commission*, Brussels

13. Article 29 Working Party, (2014b) Opinion 9/2014 on the Application of Directive 2002/58/EC to Device Fingerprinting (2002) WP 224, *European Commission*, Brussels

14. Ayres, I., and Braithwaite, J. (1992) *Responsive Regulation: Transcending the Deregulation Debate*, OUP, Oxford

15. Bachour. K., et al (2015), Provenance for the People: A User-Centered Look at the W3C PROV Standard through an Online Game, *ACM SIGCHI '15,* 2437 - 2446

16. Baldwin, R., & Cave, M. (1999) *Understanding Regulation: Theory Strategy and Practice*, OUP, Oxford

17. Baldwin, R. Cave, M and Lodge, M. (2011) *Understanding Regulation: Theory, Strategy and Practice*, OUP, Oxford, 2nd Ed

18. Bansler, J. (1989) Systems Development Research in Scandinavia: Three Theoretical Schools, *SJIS* 1(1) at http://aisel.aisnet.org/sjis/vol1/iss1/1

19. Barnard Wills, D (2012) Privacy Game, *VOME* at http://vome.org.uk/2012/05/03/privacy-game-now-available-to-download-under-a-creative-commons-license/

20. Beard, C (2014), *Smart Metering Implementation Programme (SMIP) for Dummies* CGI Group

21. Beck, E. (2002) P is for Political: Participation is not enough, Scandinavian *Journal of Information Systems* 13, 7-20

22. Bell, G., & Dourish, P. (2006) Yesterday's Tomorrow's: Notes on Ubiquitous Computing's Dominant Vision, *Personal and Ubiquitous Computing* 11(2), 133-143.

23. Belman, J. et al (2011) Grow A Game: A Tool for Values Conscious Design and Analysis of Digital Games, *DIGRA '11: Think Design Play* at http://www.tiltfactor.org/wp-content/uploads2/Digra2011-GrowAGameTool-BelmanNissenbaumFlanaganDiamond.pdf

24. Belotti, V., and Sellen, A. (1993) Design for Privacy in Ubiquitous Computing Environments, *ECSCW '93,* 77-92

25. Benford, S et al (2009) From Interaction to Trajectories: Designing Coherent Journeys Through User Experiences, *ACM CHI '09,* 709 - 718

26. Benford, S. et al (2015) Ethical Implications of HCI's Turn to the Cultural, *TOCHI,* 22(5), 24

27. Bennett, C and Raab, C. (2006) *The Governance of Privacy*, MIT Press, Cambridge, MA

28. Berleur, J. and Brunstein, K. (1997) *Ethics of Computing Codes, Spaces for Discussion and Law*, Kluwer: Dordecht

29. Bernal, P (2014) *Internet Privacy Rights*, Cambridge University Press, Cambridge UK

30. Bjerknes, G. and Bratteteig, T. (1995) User Participation and Democracy: A Discussion of Scandinavian Research on System Development, *Scandinavian Journal of Information Systems,* 7(1) 73-98

31. Black, J. (2001) Decentring Regulation: Understanding the Role of Regulation and Self-regulation in a Post-Regulatory World, *Current Legal Problems* 54(1), 103-146

32. Black, J. (2002) Critical Reflections on Regulation, *Australian Journal of Legal Philosophy* 27, 1-35

33. Black, J. (2007) Tensions in the Regulatory State, *Public Law*, Spring, 58-73

34. Blomberg, J. and Henderson, A. (1990) Reflections on Participatory Design: Lessons from the Trillium Experience, *ACM CHI '90,* 353-360

35. Birnhack, M., Toch, E., & Hadar I. (2014) Privacy Mindset, Technological Mindset, *Jurimetrics* 55, 55-114

36. Bødker, K., Kensing, F., and Simonson, J. (2011) Participatory Design in Information Systems Development, in Isomaki, H., and Pekkola, S. (Eds) (2011) *Reframing Humans in Information Systems Development*, Springer London

37. Bødker, S. (1989) A Human Activity Approach to User Interfaces, *Human Computer Interaction* 4(3) 171-195

38. Bødker, S. (2006) When Second Wave HCI Meets Third Wave Challenges *In Proceedings of the 4th Nordic conference on Human-computer interaction*, (NORDICHI '06)

39. Bødker, S. (2016) Third Wave HCI, 10 years later – Participation and Sharing, *Interactions - September-October.* 24

40. Borning, A. and Muller, M. (2012) Next Steps for Value Sensitive Design, *In Proceedings SIGCHI Conference Human Factors in Computer Systems (CHI'12) ACM Press, New York, NY, USA,* 1125-1134

41. Bourgesius, F. (2013) Behavioural Targeting: A European Legal Perspective, *IEEE Security and Privacy* 82-85

42. Bouverot, A. (2015) *GSMA: The Impact of the internet of Things - The Connected Home,* GSMA at http://www.gsma.com/newsroom/wp-content/uploads/15625-Connected-Living-Report.pdf

43. Bowker, G. and Star, SL (1999) *Sorting Things Out: Classification and Its Consequences* Cambridge MA: MIT Press 1999)

44. Braithwaite, J. (2000) The New Regulatory State and the Transformation of Criminology, *British Journal of Criminology*, 40(2), 222-238

45. Braithwaite, J. (1997) On Speaking Softly and Carrying Big Sticks: Neglected Dimensions of a Republication Separation of Powers *University of Toronto Law Journal.* 47. 305-36

46. Braithwaite, J, Coglianese, C, Levi-Faur, D (2007) Can Regulation and Governance Make a Difference? , *Governance and Compliance,* 1(1), 1-6

47. Braun, V. and Clarke, V. (2006) Using thematic analysis in psychology *Qualitative Research in Psychology*, 3 (2). pp. 77-101.

48. Brown, I. (2015) GSR *Discussion Paper: Regulation and the Internet of Things,* International Telecommunications Union, Geneva

49. Brownlee, K (2013), Civil Disobedience, *Stanford Encyclopaedia of Philosophy*

50. Brownsword, R., What the World Needs Now: Techno-Regulation, Human Rights and Human Dignity in Brownsword, R. (ed) (2004) Human Rights: Global Governance and the Quest for Justice, Hart Publishing, Oxford

51. Brownsword, R. (2005) Code, Control and Choice: Why East is East and West is West, *Legal Studies* 25(1) 1-21 hereinafter Brownsword (2005);

52. Brownsword R. (2006) Neither East or West: Is Midwest Best *Script-Ed* 3(1) 15-33 hereinafter Brownsword (2006);

53. Brownsword, R. (2008) *Rights, Regulation and the Technological Revolution*, Oxford University Press, Oxford

54. Brownsword, R. (2008b) So What Does the World Need Now? Reflection on Regulating Technologies, in Brownsword, R., and Yeung, K., (2008) *Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes*, OUP, Oxford

55. Brownsword, R. (2008) *Rights, Regulation and the Technological Revolution* OUP

56. Brush, A. et al (2011) Home Automation in the Wild: Challenges and Opportunities, *CHI 2011* http://research.microsoft.com/apps/pubs/default.aspx?id=145863

57. Busse, DK et al (2013) CHI at the Barricades: An Activist Agenda? *In Proceedings SIGCHI Conference Human Factors in Computer Systems (CHI'13) ACM Press, New York, NY, USA,* 2407-2412

58. Buttarelli, G (2012) *Opinion of the European Data Protection Supervisor on the Preparations for the roll out of Smart Metering Systems*, European Data Protection Supervisor.

59. Bynum, T. (2008) Computer and Information Ethics, *Stanford Encyclopaedia of Philosophy*

60. Caceres R., & Friday, A. (2012) Ubicomp Systems at 20: Progress, Opportunities and Challenges In *IEEE Pervasive Computing* 11(1), 14-21

61. Camp, J., & Osorio, C. (2003). Privacy-Enhancing Technologies for Internet Commerce. In *Trust in the Network Economy*: Springer-Verlag, Berlin

62. Čas, J (2009) Ubiquitous Computing, Privacy and Data Protection in S Gutwirth et al (2009) *Computers, Privacy and Data Protection: An Element of Choice,* Springer

63. Cavoukian, A., (2011) 7 Foundational Principles of Privacy by Design, Information and Privacy Commissioner of Ontario, Ontario

64. Chaudhry, A. et al (2015) Personal Data: Thinking Inside the Box, Proceedings of the *5th Decennial Aarhus Conferences,* Aarhus, accessed at http://aarhus2015.org/accepted-papers-and-demos/

65. Choe, E.K. et al, (2011) Living in a Glass House: A Survey of Private Moments in the Home, *Ubicomp 2011*

66. Cisco (2015) *The Internet of Everything* -at http://www.cisco.com/c/dam/en_us/about/business-insights/docs/ioe-value-at-stake-public-sector-analysis-faq.pdf

67. Cisco Website, (2016) Visual Networking Index, available at http://www.cisco.com/c/en/us/solutions/service-provider/visual-networking-index-vni/index.html

68. Clarke, R (2006) What's Privacy, Available at http://www.rogerclarke.com/DV/Privacy.html

69. Cockton, G. (2004) Value-Centred HCI *In Proceedings of Nordic conference on Human-computer interaction*, *(NORDICHI '04)* 149-160

70. Colesky M., et al (2016) Critical Analysis of Privacy Design Strategies In *2016 International Workshop on Privacy Engineering – IWPE'16*, San Jose, CA, USA, May 26 2016.

71. Constanza, E. et al (2014) Doing Laundry with the Agents: A Field Trial of a Future Smart Energy System in the Home, *ACM SIGCHI '14,* 813-822

72. Cooper, A. et al (2013) Privacy Considerations for Internet Protocols - RFC 6973, *Internet Architecture Board IETF*

73. Crabtree A., Rodden T. (2004) "Domestic Routines and Design for the Home" *Computer Supported Cooperative Work* 13(2), 191-220.

74. Crabtree, A., et al (2012) *Doing Design Ethnography*, Springer Verlag London

75. Crabtree, A and Mortier, R (2015) Human data interaction: historical lessons from social studies and CSCW. *Proceedings of eCSCW*

76. Cranor, LF (2013) A Shortage of Privacy Engineers, *IEEE Security & Privacy* 11(2)

77. Cranor et al (2002) The Platform for Privacy Preferences 1.0 (P3P), *W3C Recommendation*

78. Custers B. (2004) *The Power of Knowledge. Ethical, Legal, and Technological Aspects of Data Mining and Group Profiling in Epidemiology*, Wolf Legal Publishers, Nijmegen

79. Cuijpers, C. and Jaap Koops, B. (2013) Smart Metering and Privacy in Europe: Lessons from the Dutch Case in S. Gutwirth et al. (2013), *European Data Protection: Coming of Age*, Dordrecht: Springer

80. Danezis, G. et al (2014). *Privacy and Data Protection by Design – from policy to engineering* European Network Information Security Agency, Heraklion

81. Data Communications Company/DCC (2015) *Factsheet: Building a smart metering network for Great Britain* DCC

82. Deakin, S. et al, (2015) *The Internet of Things: Shaping Our Future*, Cambridge Public Policy, Cambridge

83. De Hert, P. et al (2009) Legal Safeguards for Privacy and Data Protection in Ambient Intelligence, *Personal and Ubiquitous Computing* 435-444

84. Dennedy, M., Fox, J. and Finneran, T. (2014) *Privacy Engineer's Manifesto*, Apress, New York

85. Denning, T et al. (2013a) Control Alt Hack: The Design and Evaluation of a Card Game for Computer Security Awareness and Education, *CCS '13*, 915-928

86. Denning, T et al (2013b) The Security Cards: A Security Threat Brainstorming Toolkit at http://securitycards.cs.washington.edu/assets/security-cards-information-sheet.pdf

87. Department of Business, Innovation and Skills/BIS (2012) *Better Choices: Better Deals – Report on Progress on the User Empowerment Strategy* at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/39386/12-1324-better-choices-better-deals-report-on-progress-on-the-consumer-empowerment-strategy.pdf

88. Department of Business, Innovation and Skills/BIS (2013) *midata: Privacy Impact Assessment* at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/69924/13-604-midata-privacy-impact-assessment-report.pdf

89. Department of Energy and Climate Change/DECC (2012) *Smart Meter Implementation Program Privacy Impact Assessment* at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/43044/7226-sm-privacy-ia.pdf

90. Department of Energy and Climate Change/DECC (2012b) *Smart Meter Implementation Program: Government Response to Consultation on Information Requirements for Monitoring and Evaluation* at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/43136/7206-gov-resp-cons-sm-monitor-evaluation.pdf

91. Department of Energy and Climate Change cited as DAPF (2012), SMIP *Data Access and Privacy Framework* at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/43046/7225-gov-resp-sm-data-access-privacy.pdf

92. Department of Energy and Climate Change (2014) *Smart Metering Implementation Programme Data access and privacy: Government response to consultation* at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/43046/7225-gov-resp-sm-data-access-privacy.pdf

93. Department of Energy and Climate Change (2015) *Smart Meters: A Detailed Guide* at https://www.gov.uk/guidance/smart-meters-how-they-work

94. Department of Energy and Climate Change, (2015b) *Consultation on the Timing of the Review of the Data Access and Privacy Framework* at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/413712/Consultation_on_review_of_Data_Access_and_Privacy_framework_final.pdf

95. Department of Energy and Climate Change (2016) *Smart Meters, Great Britain: Quarterly Report to End March 2016* at

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/533060/2016_Q1_Smart_Meters_Report.pdf

96. Dillahunt, et al (2009) It's Not All About "Green": Energy Use in Low-Income Communities, *Ubicomp '09* 255-264

97. Dourish, P., & Anderson, K. (2006) Collective Information Practice: Exploring Privacy and Security as Social and Cultural Phenomena, *Human Computer Interaction* 21, 319-342

98. Dourish, P (2004) What We Talk About When We Talk About Context, *Personal and Ubiquitous Computing*, 8(1), 19-30

99. Drahos, P., and J Braithwaite, J. (2000) *Global Business Regulation,* OUP, Oxford

100. Dray, S. (2012) Human Computer Interaction for Development: Changing HCI to Change the World In Jacko, J. *The Human-Computer Interaction Handbook: Fundamentals, Evolving Technologies, and Emerging Applications* Third Edition CRC Press, Boca Raton, p1369 – 1394

101. Ducatel, M. et al, (2001) *ISTAG: Scenarios for Ambient Intelligence in 2010*, JRC: Seville

102. Edwards, K., Grinter R. (2001) At Home with Ubiquitous Computing: Seven Challenges In *Proceedings of the 3rd international conference on Ubiquitous Computing (UbiComp'01) ACM Press, New York, NY, USA* 256-272

103. Edwards, L (2009) Privacy and Data Protection Online: The Laws Don't Work? Edwards and Waelde (2009), *Law and the Internet*, Third Edition, Hart Publishing, Portland

104. Edwards, L (2010) *Role and Responsibility of the Internet Intermediaries in the Field of Copyright and Related Rights,* WIPO

http://www.wipo.int/export/sites/www/copyright/en/doc/role_and_responsibility_of_the_internet_intermediaries_final.pdf

105. Edwards, L and Harbinja, E (2013) What Happens to my Facebook Profile When I Die? Legal Issues Around Transmission of Digital Assets on Death, *CREATe Working Paper* https://zenodo.org/record/8375/files/CREATe-Working-Paper-2013-05.pdf

106. Edwards, L. (2016) Privacy, Security and Data Protection in Smart Cities: A Critical EU Law Perspective, *Working Paper SSRN* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2711290

107. Ehn, P. and Kyng, M. (1987) The Collective Resource Approach to System Design in Bjerknes et al (1987) *Computers and Democracy: A Scandinavian Challenge.* Aldershot, Avebury 17–58

108. Energy UK (2013) *Smart Meter Data, A Guide to Your Rights and Choices* at http://www.energy-uk.org.uk/files/docs/Policies/Smart%20Meter%20policies%20%20consultation%20responses/2013/smart_meter_data_guide_version_1-june-13.pdf

109. Eshelmann, A (2014) 'Moral Responsibility', *Stanford Encyclopedia of Philosophy* at http://plato.stanford.edu/entries/moral-responsibility/

110. European Court of Human Rights (2015) *Internet: Case Law of ECHR* Council of Europe, Strasbourg. http://www.echr.coe.int/Documents/Research_report_internet_ENG.pdf

111. European Commission Justice Website (2016) at http://ec.europa.eu/justice/data-protection/law/index_en.htm

112. European Commission (2011) *Set of Common Functional Requirements of the Smart Meter* at

https://ec.europa.eu/energy/sites/ener/files/documents/2011_10_smart_meter_funtionalities_report.pdf

113. European Commission (2014) *Benchmarking Smart Metering Deployment in the EU 27 with a Focus on Electricity*, COM (2014) 356 Final

114. European Commission (2015) *Delivering a New Deal for Energy Consumers*, COM (2015) 339 Final

115. European Commission (2015b) Special Eurobarometer 431 'Data Protection' http://ec.europa.eu/justice/newsroom/data-protection/news/240615_en.htm

116. European Data Protection Supervisor (2015) Towards a New Digital Ethics Opinion 4/2015, EDPS,

117. European Data Protection Supervisor (2015) mHealth - Opinion of 21 May 2015, EDPS, Brussels

118. European Data Protection Supervisor (2014) Drones - Opinion of 26 November 2014, EDPS, Brussels

119. European Data Protection Supervisor (2013) eCall System - Opinion of 29 October 2013, EDPS, Brussels

120. European Data Protection Supervisor Website, Duties, accessed at https://secure.edps.europa.eu/EDPSWEB/edps/site/mySite/Duties

121. Fischer, J et al (2014) Energy advisors at work: charity work practices to support people in fuel poverty, *UbiComp '14* 447–458 at http://dl.acm.org/citation.cfm?id=2632048.2636081

122. Flanagan, M., Howe, D., and Nissenbaum, H. (2008) Embodying Values in Technology: Theory and Practice in Van Den Hoven, J. and Weckert, J.

(2008) *Information Technology and Moral Philosophy* Cambridge University Press, Cambridge

123. Flores, F., Graves, M., Hartfield, B., Winograd, T. (1988) Computer Systems and the Design of Organisational Interaction *ACM Transactions on Office Information Systems* 6(2) 153-172

124. Floyd et al, C. (1989) Out of Scandinavia: Alternative Approaches to Software Design and System Development, *Human Computer Interaction* 4, 253-350

125. Forrester, J. (1961) *Industrial Dynamics*, Pegasus Communications, Waltham

126. Friedman, B., Kahn, P., and Borning, A. (2008) Value Sensitive Design and Information Systems in Himma, K., and Tavani. H. (2008) *The Handbook of Information and Computer Ethics,* Wiley and Sons, New York

127. Friedman, B. (1999) Value Sensitive Design: A Research Agenda for Information Technology: A Report on the May 20-21 1999 Value Sensitive Design Workshop, available at http://vsdesign.org/publications/pdf/friedman99VSD_Research_Agenda.pdf

128. Friedman, B. and P Kahn, P. (2006) Human Values, Ethics and Design in Sears, A., and Jacko, J. (2006) *The Human Computer Interaction Handbook* 2nd Ed, CRC Press, Boca Raton

129. Friedman, B and Hendry, D (2012) The Envisioning Cards: A Toolkit for Catalyzing Humanistic and Technical Imaginations, *ACM CHI '12*, 1145-1149

130. Garfinkel, H. (1967) *Studies in Ethnomethodology* Prentice Hall, New Jersey

131. Gartner Hype Cycle for Emerging Technologies (2015) https://www.gartner.com/newsroom/id/3114217

132. Gavison, R (1980) Privacy and the Limits of Law, 8 *Yale Law Journal* 421

133. GDPR, (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), *Official Journal of European Union*, L119/1

134. Gibson, J.J. (1979) *The Ecological Approach to Visual Perception*, Houghton Mifflin, Boston

135. Goater, A (2014) POSTNote 471: Smart Metering of Energy and Water, *Parliamentary Office of Science and Technology*

136. Goater, A. and Casey, A. (2015) POSTNote 503: Trends in Energy, *Parliamentary Office of Science and Technology* *http://researchbriefings.parliament.uk/ResearchBriefing/Summary/POST-PN-0503*

137. Goguen, J. (1994) Requirements Engineering as the Reconciliation of Social and Technical Issues in J Goguen and M Jirotka (1994) *Requirements Engineering: Social and Technical Issues* Academic Press

138. Goldsmith, J. and Wu, T. (2008) *Who Controls the Internet? Illusions of a Borderless World,* OUP, New York

139. Golembewski, M. and Selby, M. (2010) Ideation Decks: A Card Based Design Ideation Tool, *ACM DIS '10,* 89-92

140. Gomer, R. et al (2014) Consenting Agents: Semi Autonomous Interactions for Ubiquitous Consent *Ubicomp 2014*

141. Gomer, R, et al (2013) Network Analysis of Third Party Tracking: User Exposure to Tracking Cookies Through Search, *International Conference on Web Intelligence and Intelligent Agent Technology*

142. Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González. (2014), European Court of Justice, Case C-131/12.

143. Gotterbarn, D. (1991) "Computer Ethics: Responsibility Regained" *National Forum: The Phi Beta Kappa Journal* 71, 26-31

144. Gotterbarn, D. (1999) "How the New Software Code of Ethics Affects You" *IEEE Software* 16(6) 58-64

145. Goulden, M et al (2014) Smart Grids, Smart Users? The Role of the User in Demand Side Management, *Energy Research and Social Science* 2. 21-29

146. Greenfield, A. (2006) *Everyware: The Dawning Age of Ubiquitous Computing,* Preachpit Press: New York

147. Grimpe, B., Hartswood, M., Jirotka, M (2014) Towards a Closer Dialogue Between Policy and Practice: Responsible Design in HCI *In Proceedings of CHI Conference on Human Factors in Computer Systems, (CHI '14.) ACM Press, New York, NY*

148. Grudin, J. (1990) The Computer Reaches out: The Historical Continuity of Interface Design, *In Proceedings SIGCHI Conference Human Factors in Computer Systems (CHI'90) ACM Press, New York, NY, USA,* 261-268.

149. Gürses, S (2014) Can you Engineer Privacy, *Communications of the ACM*, 57(8), 20-23

150. Halloran, J. et al (2009) The Value of Values: Resourcing Co-Design of Ubiquitous Computing, *CoDesign* 1-29

151. Halskov, K. and Hansen, N.B. (2015) The Diversity of Participatory Design Research practice at PDC 2002-2012, *International Journal of Human Computer Studies*, 74

152. Harbinja, E. (2013) Does the EU Data Protection Regime Protect Post-Mortem Privacy and What Could Be the Potential Alternatives? *SCRIPTed* 10(1) 19

153. Harper R. (Ed) (2003) *Inside the Smart Home* Springer, Verlag, London

154. Harper, R., Rodden, T., Rogers, Y., and Sellen, A. (2008) *Being Human: Human Computer Interaction in the Year 2020*, Microsoft Research: Cambridge

155. Harrison. S, P Sengers, P., Tatar, D. (2011) Making Epistemological Trouble: Third Paradigm HCI as Successor Science" *Interacting with Computers* 385-392

156. Hern, A (2014) Sir Tim Berners Lee Speaks out on Data Ownership, *The Guardian 8 October*

157. Hildebrandt, M. (2011) Legal protection by design: objections and refutations, *Legisprudence*, 2(5). 223- 248

158. Hildebrandt, M, and Jaap Koops, B (2010) The Challenges of Ambient Law and Legal Protection in the Profiling Era, *Modern Law Review*, 73(3), 428

159. Hildebrandt, M. (2013) Chapter 0: Prefatory Remarks on Human Law and Computer Law in Hildebrandt, M., Gaakeer, J. (2013) *Human Law and Computer Law: Comparative Perspectives* Springer Netherlands

160. Hildebrandt, M., & Backhouse J. (2005) *D7.2: Descriptive analysis and inventory of profiling practices,* Future of Identity in the Information Society

161. Hochheiser, H. & Lazar, J. (2010) HCI and Societal Issues: A Framework for Engagement, *International Journal of Human Computer Interaction* 23(3), 339-374

162. Hong, J (2009) Usable Privacy and Security: A Grand Challenge for HCI, *Human Computer Interaction Institute*

163. Hood, C. & Margetts, H.Z. (2007) *The Tools of Government in the Digital Age* Palgrave MacMillan, New York

164. Hood, C. (1996) Control over Bureaucracy: Cultural Theory and Institutional Variety, *Journal of Public Policy*, 15, 207

165. Hourcade, JP et al (2012) HCI For Peace, *Interactions, September/October*. 40

166. House of Commons Energy and Climate Change Select Committee (2015) *Smart Meters: Progress or Delay*, Report HC 665

167. Horn, M. et al (2015) Kids and thermostats: Understanding children's involvement with
Household energy systems, *International Journal of Child-Computer Interaction*, 3-4, 14-22

168. Huawei Website, (2016) Global Connectivity Index 2016

169. Hutchins, E. (1995) *Cognition in the Wild*, MIT Press, Cambridge

170. Iachello, G., and Hong, J. (2007) End User Privacy in Human Computer Interaction, *Foundations and Trends in Human Computer Interaction* 1(1), 1-137

171. IEEE (1963) *Code of Ethics*

172. Information Commissioner Website, (2016) Privacy By Design, accessed at https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-by-design/

173. ICO Website, 2016b, accessed at https://ico.org.uk/action-weve-taken/enforcement/

174. ICO Guidance for Organisations, 2016c, accessed at https://ico.org.uk/for-organisations/

175. Ihde, D. (1990), *Technology and the Lifeworld*, Bloomington / Minneapolis: Indiana University Press.

176. Ihde, D. (2011) Smart? Amsterdam Urinals and Autonomic Computing in Hildebrandt, M. and Rouvroy, A. (2011) *Law Human Agency and Autonomic Computing: Philosophy of Law Meets the Philosophy of Computing* Routledge: New York

177. Information Commissioner Website, (2016) Privacy By Design, accessed at https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-by-design/

178. International Telecommunications Union (2012) *Overview of the Internet of Things, Rec* ITU Y.2060 (06/2012)

179. Jaap Koops B., & Leenes, R. (2014) Privacy Regulation Cannot Be Hardcoded. A Critical Comment on the Privacy by Design provision in Data-Protection Law *International Review of Computers, Technology and Law*. 28(2) 159-171

180. Jaap Koops, B. (2006) *Starting Points for IT Regulation: Vol 9 – Deconstructing Prevalent Policy One Liners*, Asser Press, The Hague

181. Jaap Koops, B. (2010) Ten Dimensions of Technology Regulation. Finding Your Bearings in the Research Space of an Emerging Discipline in M Goodwin, B J Koops and R Leenes (2010) *Dimensions of Technology Regulation* Wolf Legal Publishing, Nijmegen

182. Jaap Koops B et al (2016) A Typology of Privacy, *University of Pennsylvania Journal of International Law*, 38

183. Jaap Koops, B (2013) A Taxonomy for Descriptive Research in Law and Technology in E Palmerini and E Stradella (2013) *Law and Technology: The Challenge of Regulating Technological* Pisa University Press, Pisa

184. Jirotka, M et al (2005) Collaboration and Trust in Healthcare Innovation: The eDiaMoND Case Study, *CSCW* 14(4), 369-398

185. Johnson, D., and Post, D. (1995-96) The Rise of Law in Cyberspace, *Stanford Law Review,* 48, 1367-1402.

186. Jondet, N. (2006) La France v Apple: Who's the Dadvsi in DRMs, *SCRIPTed* 3(4), 473

187. Johnson, J. et al (1999) SIGCHI's Role in Influencing Technology Policy, *In Proceedings SIGCHI Conference Human Factors in Computer Systems (CHI'99) ACM Press, New York, NY, USA,* 349

188. Johnson, D (1985) *Computer Ethics*, Englewood Cliffs NJ

189. Kelley, P.G et al (2009) A Nutrition Label for Privacy, *Symposium on Usable Privacy and Security (SOUPS) Conference*

190. Kosta, E (2013) Peeking into the Cookie Jar: The European Approach Towards the Regulation of Cookies, *International Journal of Law and Information Technology* Vol 21(4) 380-406

191. King, N and Jessen, P. (2014) Smart Metering Systems and Data Sharing: Why Getting a Smart Meter Should also mean Getting Strong Information Privacy Controls to Manage Data Sharing, *International Journal of Law and Information Technology* 22. 215-253

192. Kleiminger, W. Beckel, C. and Santini, S. (2015) Household Occupancy Monitoring Using Electricity Meters, *Ubicomp '15* 975-986

193. Knobel, C. and Bowker, G. (2011) Computing Ethics: Values in Design *Communications of the ACM* 54(7) 26-28

194. Kraft, P., and Bansler, J. (1992) The Collective Resource Approach: The Scandinavian Experience, In *Proceedings of the Participatory Design Conference, MA, US*

195. Kranzberg, M. (1986) Technology and History: Kranzberg's Laws, *Technology and Culture* 27, 544-56

196. Kuneva, M (2009) Roundtable on Online Data Collection, Targeting and Profiling, *Press Release* at http://europa.eu/rapid/press-release_SPEECH-09-156_en.htm

197. Kvale, S. and Brinkmann, S. (2004) *InterViews: Learning the Craft of Qualitative Research Interviewing: An Introduction to Qualitative Research Interviewing*, 2nd Ed, SAGE

198. Kyng, M. (2010) Bridging the Gap Between Politics and Techniques, *Scandinavian Journal of Information Systems,* 22(1) 49-68

199. Laidlaw, E (2015) *Regulating Speech in Cyberspace Gatekeepers, Human Rights and Corporate Responsibility*, CUP, Cambridge

200. Langefors B. (1966) *Theoretical Analysis of Information Systems* Imprint Unknown

201. Latour, B. (1992), Where are the Missing Masses? – The Sociology of a Few Mundane Artifacts, In: W.E. Bijker and J. Law (eds.), *Shaping Technology / Building Society*. Cambridge: MIT Press, pp. 205-224.

202. Laudon, KC (1996) Markets and Privacy, *Communications of the ACM* 39(9)

203. Lazar, J., et al (2012). Investigating the Accessibility and Usability of Job Application Web Sites for Blind Users. *Journal of Usability Studies* 7(2), 68-87

204. Lazar, J. et al (2012) HCI Public Policy Activities in 2012: A 10 Country Discussio*n Interactions* May/June, 78-81

205. Le Dantec, C., Poole, E., and Wyche, S. (2009) Values as Lived Experience: Evolving Value Sensitive Design in Support of Value Discovery *In Proceedings SIGCHI Conference Human Factors in Computer Systems (CHI'09) ACM Press, New York, NY, USA,* 1141-1150

206. Leenes, R. (2011) Framing Techno-Regulation: An Exploration of State and Non-State Regulation by Technology, *Legisprudence* 5(2) 143-169

207. Leontiev, A.N. (1978) *Activity, Consciousness and Personality*, Prentice Hall, Upper Saddle River

208. Leppänen, S and Jokinen, M. (2003) Daily Routines and Means of Communication in a Smart Home, in R Harper (2003) *Inside the Smart Home*, Springer Verlag: London

209. Lessig, L. (1999) *Code and Other Laws of Cyberspace*, Basic Books, New York

210. Lessig, L. (2006) *Code Version 2.0* Basic Books, New York

211. Lessig, L. (1998) The New Chicago School *The Journal of Legal Studies*. 27 (3)

212. Lessig, L, (1996) The Zones of Cyberspace, *Stanford Law Review,* 48, 1403

213. Leygue et al (2014) Energy Sharing and Energy Feedback: affective and behavioural reactions to communal energy displays, *Frontiers in Energy Research* 29(2)

214. Lindwer, M, et al (2003) Ambient Intelligence visions and achievements: Linking abstract ideas to real-world concepts, *Design, Automation and Test* in Europe Conference 2003

215. Liu, Y. et al (2014) Identity Crisis of Ubicomp? Mapping 15 years of the Field's Development and Paradigmatic Change, *Ubicomp 2014*

216. Luger, E., Urquhart, L., Rodden, T., and Golembewski, M. (2015) Playing the Legal Card: Using Ideation Cards to Raise Data Protection Issues within the Design Process, *In Proceedings SIGCHI Conference Human Factors in Computer Systems (CHI'15) ACM Press, New York, NY, USA* 457-466

217. Luger, E., and Rodden, T. (2013) An Informed View on Consent, *Proceedings of the international conference on Ubiquitous Computing (UbiComp'13) ACM Press, New York, NY, USA*, 529-538

218. Luhmann, N (1996) *Social Systems*, (Translated by Bednarz, J and Baecker, D) Stanford University Press, Stanford

219. Luhmann, N (1992) The Coding of the Legal System. *European Yearbook in the Sociology of Law* 145-185.

220. Mackay, M. (2002) Interactive Thread: A participatory design toolkit *interLiving, KTH,* at interliving.kth.se/publications/thread/index.html

221. Mäkinen, L (2016) Surveillance On/Off: Examining Home Surveillance Systems From The User's Perspective, *Surveillance & Society* 14(1): 59-77.

222. Maner, W. (1980) *Starter Kit in Computer Ethics*, Helvetia Press, NY

223. Manson, N. and O'Neill, (2007) O. *Rethinking Informed Consent in Bioethics*, CUP: Cambridge

224. Marsden, C. (2011) *Internet Co-Regulation: European Law, Regulatory Governance and Legitimacy in Cyberspace*, Cambridge University Press, Cambridge, UK.

225. Marsden, C. (2012) Internet co-regulation and constitutionalism: Towards European judicial review, *International Review of Law, Computers & Technology*, 26:2-3, 211-228

226. Marsden, C. and Brown, I. (2013) *Regulating Code* MIT Press, Cambridge MA

227. McAuley, D. (2016) What is IoT? That is not the Question, *IoT UK*, Accessed at http://iotuk.org.uk/what-is-iot-that-is-not-the-question/

228. McDonald, A and Cranor, L.F. The Cost of Reading Privacy Policies, *I/S - A Journal of Law and Policy for the Information Society*, 540-565

229. McStay, A. (2015) Now advertising billboards can read your emotions … and that's just the start *The Conversation* at https://theconversation.com/now-advertising-billboards-can-read-your-emotions-and-thats-just-the-start-45519

230. Millar, J (2014) Technology as Moral Proxy: Autonomy and Paternalism by Design, *IEEE International Symposium on Ethics in Science, Technology and Engineering*. 1-7

231. Millar, J (2008) Blind Visionaries: A Case for Broadening Engineers' Ethical Duties, *IEEE International Symposium on Technology and Society*, ISTAS 2008.

232. Mingers (1995) *Self Producing Systems: Implications and Applications of Autopoeisis*, *Contemporary Systems Thinking*, Plenum, New York

233. Mitchell W.J. (1995) *City of Bits: Space, Place, and the Infobahn*, The MIT Press, Cambridge

234. Moor, J. (1985) What is Computer Ethics: A Proposed Definition, *Metaphilosophy* 16(4), 266-275

235. Moreau, L. and Missier, P. *PROV-DM: The PROV Data Model.* 2012

236. Mortier, R. et al, (2014) Human-Data Interaction: The Human Face of the Data Driven Society, *SSRN*, accessed at http://www.eecs.qmul.ac.uk/~hamed/papers/HDIssrn.pdf

237. Muller, M., Wharton, C., McIver, W, and Laux, L. (1997) Toward an HCI Research and Practice Agenda Based on Human Needs and Social Responsibility *In Proceedings SIGCHI Conference Human Factors in Computer Systems (CHI'97) ACM Press, New York, NY, USA,* 155-160

238. Muller, M., Blomberg, J., Carter, K., Dykstra, E., Halskov, K., Greenbaum, J. (1991) Participatory Design in Britain and North America: Responses to the Scandinavian Challenge, *In Proceedings SIGCHI Conference Human Factors in Computer Systems (CHI, 91) ACM Press, New York, NY, USA* 389-392

239. Muller, M., Wildman, D., White, E. (1993) Taxonomy of PD Practices: A Brief Practitioners Guide *Communications of the ACM* 36(4). 26-28

240. Mumford, E. (2006) The story of socio-technical design: reflections on its successes, failures and potential, *Information Systems* 16(4) 317-342

241. Murray, A., and Scott, C (2002) Controlling the New Media: Hybrid Responses to New Forms of Power, *Modern Law Review* 65(4), 491-516

242. Murray, A. Conceptualising the Post-Regulatory (Cyber) State in Brownsword, R and Yeung, K (Eds) (2008b) *Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes*, Hart Publishing, Oxford

243. Murray, A. (2006) *The Regulation of Cyberspace: Control in the Online Environment*, (Routledge Cavendish, Abingdon

244. Neyland, D. (2015) Bearing account-able witness to the ethical algorithmic system. Science, Technology and Human Value. 35(1): 55 –80.

245. Nissenbaum, H. (2009) *Privacy In Context: Technology, Policy and the Integrity of Social Life,* Stanford University Press, Stanford

246. Nissenbaum, H. (2001) How Computer Systems Embody Values*, Computer,* March. 118-120

247. Nissenbaum, H. (2005) Values in Technical Design in Mitcham, C (2005) *Encyclopaedia of Science, Technology and Ethics*, MacMillan, New York

248. Nissenbaum, H. (2001) How Computer Systems Embody Values, *Computer* March, 118-120

249. Ofgem, (2014) *The Enforcement Guidelines* at https://www.ofgem.gov.uk/publications-and-updates/enforcement-guidelines

250. Ofgem (2015) *Decision on extending the smart meter Framework for data access and privacy to Remote Access Meters*, Ofgem available at https://www.ofgem.gov.uk/sites/default/files/docs/2015/02/data_privacy_extension_-_decision_1.pdf

251. Oliver, I. (2014) *Privacy Engineering*, Independently Published

252. Oulasvirta, A. et al (2012) Long-term Effects of Ubiquitous Surveillance in the Home, *Ubicomp 2012*

253. Out-Law, (2014) Personal data lockers can protect privacy and help businesses, says consultant, *Out-Law.com*, 12 Jun 2014

254. Parkhill, K et al (2013) Transforming the UK Energy System: Public Values, Attitudes, and Acceptability*, Energy Research Centre*

255. Perry Barlow, J (1996) A Declaration of Independence for Cyberspace

256. Pierce, J. et al (2015) Expanding and Refining Design and Criticality in HCI *In Proceedings of CHI Conference on Human Factors in Computer Systems, (CHI '15). ACM Press, New York, NY.* 2083-2092

257. Post, D (2002) Against 'Against Cyber-anarchy, *Berkeley Technology Law Journal* 17, 1365 -1387

258. Pounder, C (2014) Roll out the Bunting: Durant Judgment as Good as Dead and Buried, *Amberhawk Blog* 19 Feb 2014 http://amberhawk.typepad.com/amberhawk/2014/02/roll-out-the-bunting-durant-judgment-is-good-as-dead-and-buried.html

259. Pressman, R. (2009) *Software Engineering: A Practitioners Approach* 7th Ed, McGraw Hill, New York

260. Prins, C. (2006) Property and Privacy: European Perspectives and the Commodification of our Identity in L. Guibault and P.B. Hugenholtz (2006), *The Future of the Public Domain*, 223–257

261. Public Accounts Committee (2014) *Twelfth Report: Update on Preparations for Smart Metering,* PAC

262. Rauhofer, J. (2011) Privacy is Dead, Get Over It! Information Privacy and the Dream of a Risk Free Society, *ICTL* 185-197

263. Raw, G and Ross, D. (2011) *Energy Demand Research Project: Final Analysis*, Ofgem https://www.ofgem.gov.uk/ofgem-publications/59105/energy-demand-research-project-final-analysis.pdf

264. Reed, C (2010) How to Make Bad Law: Lessons from the Computing and Communications Sector, *Queen Mary School of Law Legal Studies Research Paper No. 40/2010*

265. Reeves, S. (2012) Envisioning Ubiquitous Computing, *CHI 2012*, 1573-1582

266. Reidenberg, J. (1998) Lex Informatica: The Formulation of Policy Rules through Technology, *Texas Law Review*, 76, 553

267. Reeves, S. (2012) Envisioning Ubiquitous Computing *In Proceedings SIGCHI Conference Human Factors in Computer Systems (CHI'12) ACM Press, New York, NY, USA*. 1573 -1582

268. Rendle, A. (2014) Who Owns the Data in the Internet of Things, *Taylor Wessing Feb 2014* at http://united-kingdom.taylorwessing.com/download/article_data_lot.html

269. Rodden, T., and Benford, S. (2003) The Evolution of Buildings and Implications for the Design of Ubiquitous Domestic Environments, *In Proceedings SIGCHI Conference Human Factors in Computer Systems (CHI'03) ACM Press, New York, NY, USA*

270. Rodden et al (2013) At Home With the Agents: Exploring Attitudes towards Future Smart Energy Infrastructures, *ACM SIGCHI '13*. 1173-1182

271. Rogers, A et al (2012) Delivering the Smart Grid: Challenges for Autonomous Agents and Multi-Agent Systems, *AAAI '12* http://www.orchid.ac.uk/eprints/56/1/smart_grid.pdf

272. Rogers Y. (2006) Moving on from Weiser's Vision of Calm Computing: Engaging Ubicomp Experiences in *Proceedings of the 8th International Conference on Ubiquitous Computing (UbiComp'06) ACM Press, New York, NY, USA* 404-421

273. Rogers, Y. (2005) New Theoretical Approaches for Human Computer Interaction, *Annual Review of Information Science and Technology* 38(1), 87-143

274. Rose et al (2015) *Internet of Things: An Overview*, Internet Society

275. František Ryneš v Úřad pro ochranu osobních údajů (2014) European Court of Justice, Case C-212/13

276. Satyanarayanan, M (2001) Pervasive Computing: Visions and Challenges, *IEEE Personal Communications*

277. Savirimuthu, J. (2013) Smart Meters and the Information Panopticon: Beyond the Rhetoric of Compliance, *International Review of Law, Technology and Society*, 27(1-2), 161–186

278. Scott, C. (2004) Regulation in the Age of Governance: The Rise of the Post Regulatory State in Jordana J and Levi-Faur D (eds) (2004) *The Politics of Regulation*, Edward Elgar, Cheltenham

279. Scaife, M. and Rogers. Y. (1996) External Cognition: how do graphical representations work? *International Journal of Human Computer Studies*, 45(2), 185-213

280. Schwartz, P.M (2003) Property, privacy, and personal data, 117 *Harvard Law Review* 2056-2128.

281. Sellen, A., Rogers, Y., Harper, R., and Rodden, T. (2009) Reflecting Human Values in the Digital Age *Communications of the ACM* 52(3). 58-66

282. Shneiderman, B. (1990) Human Values and the Future of Technology: A Declaration of Empowerment, *CQL '90 Proceedings of the conference on Computers and the quality of life,* 1-6

283. Shneiderman, B. (2012) Universal usability, *Communications of the ACM* 43(5), 84-91.

284. Selznick, P. (1985) Focusing Organizational Research on Regulation In Noll, R.G. (1985) *Regulatory Policy and the Social Science,* University of California, Berkeley

285. Sengers, P., Boehner, D. and Kaye, J. (2005) Reflective design, *In Proceedings of 4th Decennial Conference on Critical Computing*, 49–58

286. Sloan, M (2014) Government Publishes It's Review into the MiData Scheme, *Brodies* at http://www.brodies.com/blog/government-published-review-midata-scheme/

287. Smart Energy Code (2015) version 4.4 available at https://www.smartenergycodecompany.co.uk/

288. Solove, D.J (2008) *Understanding Privacy*, Cambridge: Harvard University Press

289. Spence, A. et al (2015) Public Perceptions of Demand-Side Management and a Smarter Energy Future, *Nature Climate Change* 5. 550-554

290. Spiekermann, S (2011) The RFID PIA – developed by industry agreed by regulators in Wright, D. and de Hert, P. *Privacy Impact Assessment: Engaging Stakeholders in Protecting Privacy* (Springer)

291. Spiekermann, S. (2012) The Challenges of Privacy by Design. *Communications of the ACM (CACM)* 55 (7), 34-37.

292. Spiekermann, S., & Cranor, L.F. (2009) Engineering Privacy *IEEE Transactions on Software Engineering* 35 (1), 67-82

293. Spiekermann, S. and Pallas, F. (2005) Wider Implications of Ubiquitous Computing, *Poiesis & Praxis: International Journal of Ethics of Science and Technology Assessment* 4(1), 6-18

294. Stahl, B. C. (2013). Responsible research and innovation: The role of privacy in an emerging framework. *Science and Public Policy*, 40(6), 708–716

295. Stahl, B.C, Eden, G., Jirotka M. (2013) Responsible research and innovation in information and communication technology—identifying and engaging with the ethical implications of ICTs, *Responsible Innovation,* 199-218

296. Stahl, B. C., Eden, G., Jirotka, M., & Coeckelbergh, M. (2014). From Computer Ethics to Responsible Research and Innovation in ICT: The transition of reference discourses informing ethics-related research in information systems. *Information & Management* 51(6), 810-818

297. Stilgoe, J. et al (2013) Developing a Framework for Responsible Innovation *Research Policy* 42(9), 1568-1580

298. Suchman, L. (1987) *Plans and Situated Actions: The Problem of Human-Machine Communication,* Cambridge University Press, New York

299. Suchman, L. (1994) Do Categories Have Politics? The Language/Action Perspective Reconsidered, CSCW 2. 177-190

300. Suchman, L. (1995) Speech Acts and Voices: Response to Winograd et al, *CSCW*, 3 85-95

301. Suchman. L. (2007) *Human Machine Reconfigurations*, Cambridge University Press, Cambridge

302. Taylor, F. W. (1911) *Principles of Scientific Management*, Harper and Brothers

303. Tolmie, P. et al (2002) Unremarkable Computing *In Proceedings SIGCHI Conference Human Factors in Computer Systems (CHI'12) ACM Press, New York, NY, USA*

304. Tolmie, P. et al (2003) "Towards the Unremarkable Computer: Making Technology at Home in Domestic Routine" in Harper, R. (Ed) (2003) *Inside the Smart Home* Springer Verlag, London

305. Törpel, B., Voss, A., Hartswood, M., and Procter, R. (2009) Participatory design: issues and Approaches in Dynamic Constellations of Use, Design and Research, in Voss, A. et al (2009) *Configuring User-Designer Relations: Interdisciplinary Perspectives*, Springer: London

306. Tuebner, G (1998) After Privatization: The Many Autonomies of Private Law. *Current Legal Problems* 51, 393-424.

307. Ur, B, Jung, J and Schechter, S (2014) Intruders Versus Intrusiveness: Teens' and Parents' Perspectives on Home- Entryway Surveillance *Proceedings of the international conference on Ubiquitous Computing (UbiComp'14) ACM Press, New York, NY, USA*

308. Urquhart, L., Luger, E. (2015) Smart Cities: Creative Compliance and the Rise of 'System designers as Regulators' *Computers and Law* 26(2) http://www.scl.org/site.aspx?i=ed42790

309. Urquhart, L. (2016) Privacy and Freedom of the Press from 2004-2015: From Campbell to Leveson" In Edwards, L. (2016) *Law, Policy and the Internet*, Hart Publishing, Oxford

310. Van Den Berg, B (2011) "Robots as Tools for Techno-Regulation" *Law, Innovation and Technology* 3(2) 317-332

311. Van Den Hoven, J. (2006) ICT and Value Sensitive Design in Goujon, P. et al (2006) *The Information Society: Innovations, Legitimacy, Ethics and Democracy, IFIP International Federation for Information Processing, Volume 233.* Springer, Netherlands

312. Van Den Hoven, J. et al, (2011) Engineering and the Problem of Moral Overload *Science and Engineering Ethics* 18(1). 143-155

313. Van de Poel, I and Van Gorp, A (2006) The Need for Ethical Reflection in Engineering Design: The Relevance of Type of Design and Design Hierarchy, *Science, Technology and Human Values* 31(3) 333-360

314. Van Gorp, A and Van de Poel, I (2001) Ethical Considerations in Engineering Design Processes *IEEE Technology and Society Magazine*, Fall 15-22

315. Verbeek, P. (2006) Materialising Morality: Designing Ethics and Technological Mediation, *Science, Technology and Human Values* 31(3)

316. Vermaas, P. et al (2010) Designing for Trust: A Case of Value Sensitive Design, *Knowledge, Technology & Policy*, 23(3), p491–505

317. Von Hirsch, A., Garland, D., & Wakefield, A. (2004) *Ethical and Social perspectives on Situational Crime Prevention* Hart Publishing, Oxford. http://www.hartpub.co.uk/BookDetails.aspx?ISBN=9781841135533

318. Von Schomberg, R (2011) Prospects for Technology Assessment in a Framework of Responsible Research and Innovation In M Dusseldorp, R Beecroft (Eds) *Technikfolgen Abchätzen Lehren: Bildungspotenziale Transdisziplanärer*. Vs Verlag Methoden, Wiesbaden

319. Walport M (2014) Internet of things: making the most of the second digital revolution, UK Government Office of Science

320. Wang, Y. et al (2014) A Field Trial of Privacy Nudges for Facebook, *Proceedings of CHI 2014*

321. Warren, S. & Brandeis, L (1890) The Right to Privacy, 4 *Harvard Law Review* 193

322. Weiser, M (1991) The Computer for the 21st Century, *Scientific American*, 94-104

323. Weiser, M. (1993) Some Computer Science Issues in Ubiquitous Computing In *Communications of the ACM* 36(7), 75-84.

324. Weiser, M., & Brown, J.S. (1997) The Coming Age of Calm Technology In Denning, PJ and Metcalfe, R.M (1997) *Beyond Calculation,* Copernicus, New York

325. Westin, A F (1967) *Privacy and Freedom*, New York: Athenaeum

326. Wetzel, R (2014) Introducing Pattern Cards for Mixed Reality Game Design, *Third Workshop on Design Patterns in Games. Foundations in Digital Games Conference 2014*.

327. Wilson, C. et al (2015) Smart Homes and Their Users: A Systematic Analysis and Key Challenges, *Personal and Ubiquitous Computing* 19. 463-476

328. Winner, L. (1980) Do Artifacts Have Politics? *Daedalus* 109(1), 121

329. Winner, L. (1978) *Autonomous Technologies,* MIT Press, MA

330. Winograd, T. and Flores, F. (1986) *Understanding Computers and Cognition: A New Foundation for Design*, Norwood, NJ

331. Winograd, T. (1994) Categories, Discipline, and Social Coordination, *CSCW* 2, 191-197

332. Wittgenstein, L. (1953) *Philosophical Investigations*, Blackwell Publishing

333. World Economic Forum (2011) *Personal Data: The Emergence of A New Asset Class?* At http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf

334. Wright, D. et al (2008) *Safeguards in a World of Ambient Intelligence*, Springer, Netherlands

335. Wright, D., & De Hert P. (2012) *Privacy Impact Assessment* Springer, Netherlands

336. Yang, R. and Newman, M (2013) Learning from a Learning Thermostat: Lessons for Intelligent Systems for the Home, *Ubicomp '13,* 93-102

337. Yang et al (2014) Making Sustainability Sustainable: Challenges in the Design of Eco-Interaction Technologies, *ACM SIGCHI '14*

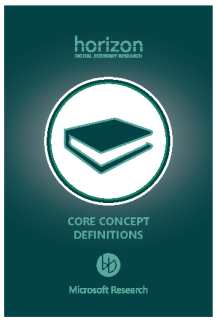
338. Yeung, K (2014) Design for Regulation, In Van Den Hoven, J, Van De Poel, I. and Vermaas, P. (eds) (2014) *Handbook of Ethics, Values and Technological Design*, Springer, Netherlands

339. Yeung, K (2011) Can We Employ Design-based regulation while avoiding Brave New World? *Journal of Law, Innovation and Technology* 3, 1-30

340. Zittrain, J. (2009) *Future of the Internet and How to Stop It,* Penguin Books, London

Appendices

Appendix 1: PDF of Privacy by Design Cards




CORE CONCEPT DEFINITIONS
KEY IDEAS AND TERMS

Data Controllers and System Designers.

Those who determine the purposes of collection, and the means by which personal data is processed.


CORE CONCEPT DEFINITIONS
KEY IDEAS AND TERMS

Personal Data.

Information that directly or indirectly relates to the end user.


CORE CONCEPT DEFINITIONS
KEY IDEAS AND TERMS

Data Processors.

Those who process personal data on behalf of others.


CORE CONCEPT DEFINITIONS
KEY IDEAS AND TERMS

Data Processing.

Processing is broadly defined, and includes any use of, or operation performed on, personal data. Common examples are collection, recording, structuring, alteration and storage of data.


CORE CONCEPT DEFINITIONS
KEY IDEAS AND TERMS

Territory.

EU data protection law also applies to those offering goods or services, and monitoring behaviour of EU citizens, even if they are outside Europe (i.e. US companies).


CORE CONCEPT DEFINITIONS
KEY IDEAS AND TERMS

Personal Data Breach.

A security breach where data is accidentally or illegally destroyed, lost, altered, or shared.


CORE CONCEPT DEFINITIONS
KEY IDEAS AND TERMS

Proportionality & Necessity.

Many user rights in data protection law need to be balanced against other societal rights, such as national security and freedom of the press. Any balancing of rights should not be unnecessary, or disproportionately impact the end user.


DATA PROTECTION & CONSENT
PRINCIPLES OF DATA PROTECTION

Lawfulness, Fairness, and Transparency.

Data must be processed lawfully, fairly, and transparently.


DATA PROTECTION & CONSENT
PRINCIPLES OF DATA PROTECTION

Purpose Limitation.

Data can only be processed for defined purposes and cannot be used in ways inconsistent with these.


DATA PROTECTION & CONSENT
PRINCIPLES OF DATA PROTECTION

Data Minimisation.

Data processing must be kept to the minimum amount necessary for the specific purposes of the system or service.


DATA PROTECTION & CONSENT
PRINCIPLES OF DATA PROTECTION

Accuracy.

Data must be kept up to date, and inaccuracies should be corrected or deleted quickly.


DATA PROTECTION & CONSENT
PRINCIPLES OF DATA PROTECTION

Storage Limitation.

Data must only be stored as long as is necessary for the purposes of processing.


DATA PROTECTION & CONSENT
PRINCIPLES OF DATA PROTECTION

Integrity and Confidentiality.

Data must be secure and protected from loss, destruction, or damage.


DATA PROTECTION & CONSENT
LAWFULNESS

Lawfulness.

Lawful data processing requires user consent. Data processing can also be based on other legal grounds when it is necessary, like protecting the public interest.

DATA PROTECTION & CONSENT

CONSENT

Giving User Consent.

Consent must be freely given. The user must make a specific, informed and unambiguous agreement to data processing.

DATA PROTECTION & CONSENT

CONSENT

Proving User Consent.

Consent must be provable. It can be withdrawn by the user at any time, and when it is given as part of a written contract it must be flagged up in clear and plain language.

DATA PROTECTION & CONSENT

CONSENT

Children and Consent.

Consent must be given or authorised by parents when children under 16 are using online shopping, social media and similar types of services and systems.

DATA PROTECTION & CONSENT

CONSENT

Special Categories of Data.

Political opinions, ethnic origin, biometric and health information, religious/philosophical beliefs and similar forms of data cannot be processed unless explicit consent is obtained or processing is necessary.

END USER RIGHTS

TRANSPARENCY

Transparency.

Information provided to end users must be concise, transparent, easy to understand and written in simple language.

END USER RIGHTS

TRANSPARENCY

Information Provision.

When end users make information requests, responses must be provided within one month, or exceptionally two. The responses should be given electronically and free of charge.

END USER RIGHTS

INFORMATION AND ACCESS TO DATA

Rights to Information.

Data controllers should provide users with information on their identity, contact details, purposes and legal grounds of the data collection.

END USER RIGHTS

INFORMATION AND ACCESS TO DATA

Right of Access.

End users have a right to know who processes their data, and to request a copy for a fee. They must be able to find out why the data is collected, what data is stored and where, and how that data is used or shared.

END USER RIGHTS

RECTIFICATION, ERASURE, RESTRICTION, PORTABILITY

Right to Rectification.

Sometimes, data stored or collected by a system that relates to a user might not be correct. All users have a right to get inaccurate information corrected.

END USER RIGHTS

RECTIFICATION, ERASURE, RESTRICTION, PORTABILITY

Right to Erasure, Right to Be Forgotten.

Users have a right to data deletion without delay. If user consent is withdrawn or data is no longer necessary, controllers must delete that data. This right must be balanced with other rights, like freedom of expression.

END USER RIGHTS

RECTIFICATION, ERASURE, RESTRICTION, PORTABILITY

Right to Restriction.

Users have a right to restrict data processing. Instead of full deletion, they may choose to restrict the use of their data. Restricted data can only be processed in limited circumstances.

END USER RIGHTS

RECTIFICATION, ERASURE, RESTRICTION, PORTABILITY

Information Recipients.

Controllers should let all subsequent data recipients know about rectification, restriction or erasure requests, unless this is too difficult or impossible.

END USER RIGHTS

RECTIFICATION, ERASURE, RESTRICTION, PORTABILITY

Right to Data Portability.

Users have the right to get their data in a structured, commonly used, machine readable format, such as XML or JSON. This allows them to easily move it to another controller.

END USER RIGHTS

RIGHTS TO OBJECT / AUTOMATED DATA PROFILING

Right to Object.

Users can object to their data being processed, particularly for direct marketing. After they do so, the direct marketer must stop using their data.

END USER RIGHTS

RIGHTS TO OBJECT / AUTOMATED DATA PROFILING

Right against Profiling.

Users have the right not to be profiled or subject to algorithmic decisions with legal effects. They have a right to request such decisions get human oversight and review.

END USER RIGHTS

RIGHTS TO OBJECT / AUTOMATED DATA PROFILING

Restrictions.

Rights to erasure, restriction and data portability can be restricted when necessary for national security or prevention and detection of crime.

INTERNATIONAL CONSIDERATIONS

THIRD COUNTRIES

Data Sent Outside Europe.

Ordinarily, data should not be transferred out of the European Economic Area. Sometimes, it can be sent to specific countries that guarantee data protection like Canada or New Zealand.

INTERNATIONAL CONSIDERATIONS

THIRD COUNTRIES

The USA.

The EU-US Safe Harbor Agreement is now invalid. A new framework is emerging, but currently legal transfer of data requires extra safeguards like special contract clauses.

SYSTEM DESIGNER RESPONSIBILITIES

GENERAL OBLIGATIONS

Data Protection by Design and Default.

Technical methods and organisational approaches (like pseudonymisation) should be used to safeguard rights of users and comply with appropriate regulations.

SYSTEM DESIGNER RESPONSIBILITIES

GENERAL OBLIGATIONS

Joint Controllers.

There may be two or more data controllers jointly deciding purposes and means of processing. All of the controllers need to agree upon respective responsibilities and duties to users, and make these available to the user.

SYSTEM DESIGNER RESPONSIBILITIES

GENERAL OBLIGATIONS

European Representative.

Controllers outside the EU who target goods and services to EU citizens on a large scale (such as social media services), should have an EU representative to oversee compliance.

SYSTEM DESIGNER RESPONSIBILITIES

GENERAL OBLIGATIONS

Processors & Controllers.

A controller may define the means and purposes of processing, and a separate processor may carry this out. Controllers need to strictly and contractually define their relationship with processors.

SYSTEM DESIGNER RESPONSIBILITIES

GENERAL OBLIGATIONS

Record Keeping.

Comprehensive records of processing need to be maintained by controllers and processors. These include logs of data, recipients, transfers abroad, and any security measures put in place.

SYSTEM DESIGNER RESPONSIBILITIES

DATA SECURITY

Security of Processing.

Safeguards to address data security risks should be used. These would include data encryption and pseudonymisation, and should ensure confidentiality, integrity, or resilience of systems.

SYSTEM DESIGNER RESPONSIBILITIES

DATA SECURITY

Data Breach Notification. (Authorities)

When a data breach may impact an end user's fundamental rights and freedoms, controllers should inform the authorities, ordinarily within 72 hours.

SYSTEM DESIGNER RESPONSIBILITIES

DATA SECURITY

Data Breach Notification. (Data Subject)

Controllers need to inform end users without undue delay if a breach risks their fundamental rights and freedoms unless: a) data is encrypted; b) mitigating measures are already taken or; c) contacting all end users is too difficult.

SYSTEM DESIGNER RESPONSIBILITIES

IMPACT ASSESSMENTS AND PRIOR CONSULTATION

Data Protection Impact Assessments.

New technologies that are risky for fundamental rights and freedoms needs a data protection impact assessment. This assessment must contain a systematic analysis of privacy risks and safeguards.

SYSTEM DESIGNER RESPONSIBILITIES

IMPACT ASSESSMENTS AND PRIOR CONSULTATION

Data Protection Officer.

New internal Data Protection Officers will work with organisations on all aspects of data protection such as advice and informing or monitoring compliance.

SYSTEM DESIGNER RESPONSIBILITIES

NEW CODES OF CONDUCT, SEALS, MARKS, AND CERTIFICATION

New Codes of Conduct.

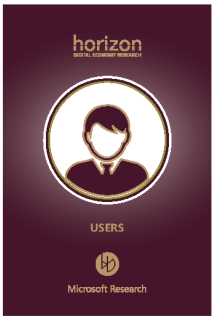
New industry codes on issues like pseudonymisation, third country transfer and child rights are being developed and monitored by competent, expert, independent bodies.

SYSTEM DESIGNER RESPONSIBILITIES

NEW CODES OF CONDUCT, SEALS, MARKS, AND CERTIFICATION

New Seals, Marks and Certifications.

New data protection certifications, seals and marks showing compliance with regulations are being developed and will be granted for maximum of three years.



USERS

THE PEOPLE WHO USE YOUR SYSTEM

Older People.

Your users might be age 65 or older.

USERS

THE PEOPLE WHO USE YOUR SYSTEM

Mental Health.

Your users might suffer from poor mental health.

USERS

THE PEOPLE WHO USE YOUR SYSTEM

Children.

Your users might be children or adolescents.

USERS

THE PEOPLE WHO USE YOUR SYSTEM

Visual Impairment.

Your users might be blind, or have other visual impairments that could impact their use of the system.

USERS

THE PEOPLE WHO USE YOUR SYSTEM

Poor Literacy.

Your users might be adults with low levels of literacy.

USERS

THE PEOPLE WHO USE YOUR SYSTEM

Gender Spectrum.

Your users might identify with any of a range of different genders.

USERS

THE PEOPLE WHO USE YOUR SYSTEM

Ex-Offenders.

Your users might be ex-offenders, and might include people on probation.

USERS

THE PEOPLE WHO USE YOUR SYSTEM

Second Language.

Your users might understand English as a second or third language, at varying levels of fluency.

USERS

THE PEOPLE WHO USE YOUR SYSTEM

Country of Residence.

Your users might reside in a country other than your own.

CONSTRAINTS

LIMITATIONS APPLIED TO YOUR SYSTEM

Default Sharing.

The system should allow for default sharing with third parties.

CONSTRAINTS

LIMITATIONS APPLIED TO YOUR SYSTEM

User Control.

The system should allow the user a high level of control.

CONSTRAINTS

LIMITATIONS APPLIED TO YOUR SYSTEM

Limited Connection.

The system should be able to operate with limited or sporadic network connectivity.

CONSTRAINTS

LIMITATIONS APPLIED TO YOUR SYSTEM

Social Sharing.

The system should engage with third party social media services.

CONSTRAINTS

LIMITATIONS APPLIED TO YOUR SYSTEM

Low Cost.

The system should be designed as inexpensively as possible.

CONSTRAINTS

LIMITATIONS APPLIED TO YOUR SYSTEM

Data Maximisation.

The system should collect as much data as possible about the user.

CONSTRAINTS

LIMITATIONS APPLIED TO YOUR SYSTEM

Privacy.

The system should enhance a users' perception of privacy.

CONSTRAINTS

LIMITATIONS APPLIED TO YOUR SYSTEM

Minimal Distraction.

The system should not distract the user from primary goals or day-to-day activities.

CONSTRAINTS

LIMITATIONS APPLIED TO YOUR SYSTEM

Data Minimalisation.

The system should collect as little data as possible.

CONSTRAINTS

LIMITATIONS APPLIED TO YOUR SYSTEM

Careful Collection.

The system should not collect (by accident or intention) any third party data.

CONSTRAINTS

LIMITATIONS APPLIED TO YOUR SYSTEM

Low Energy.

The system should rely on low levels of power or energy to operate.

SYSTEMS

SYSTEM YOU ARE BUILDING

Autonomous Vehicle.

The smart vehicle can transport passengers without the driver needing to be in control. They can be used in inner cities, but need to navigate safely for both passengers and pedestrians.

SYSTEMS

SYSTEM YOU ARE BUILDING

Intelligent Public Display.

The public display can be positioned in shops or on the high street to detect when someone walks by and offer them tailored content like adverts.

SYSTEMS

SYSTEM YOU ARE BUILDING

Connected Home.

Intelligent devices can manage energy, lighting, security & comfort in the home. Routine tasks like scheduling laundry, can be automated & remotely controlled at a distance via mobile apps.

SYSTEMS

SYSTEM YOU ARE BUILDING

Big Social Media Analytics.

Analytics services can let companies monitor discussion around their products or services on social networks. They analyse the content to understand consumer trends, needs & attitudes.

SYSTEMS

SYSTEM YOU ARE BUILDING

Smart Energy Management

Smart meters can use energy consumption data to help customers manage their energy usage & costs. Smart grids use the data to manage energy generation and supply more sustainably.

SYSTEMS

SYSTEM YOU ARE BUILDING

Social Sharing Plug In.

Plug ins can link a website to a third party social media service like Facebook or Twitter. It can share some meta-data with the service.

SYSTEMS

SYSTEM YOU ARE BUILDING

Quantified Self.

Wearable body sensors can help users monitor daily activity, sleep patterns or biometrics like heart rate. This information can be used to inform life choices around health, wellbeing & exercise levels.

SYSTEMS

SYSTEM YOU ARE BUILDING

Personal Cloud

Users can sync data from all their different devices to one personal cloud that they control. They can then trade their data with third parties, like marketing companies, for a fee.

SYSTEMS

SYSTEM YOU ARE BUILDING

Care Robot.

With the robot, elderly users can live independently without need to move into care. The robot needs to monitor & assist with their health, safety & wellbeing. Accordingly, it needs to be trustworthy.

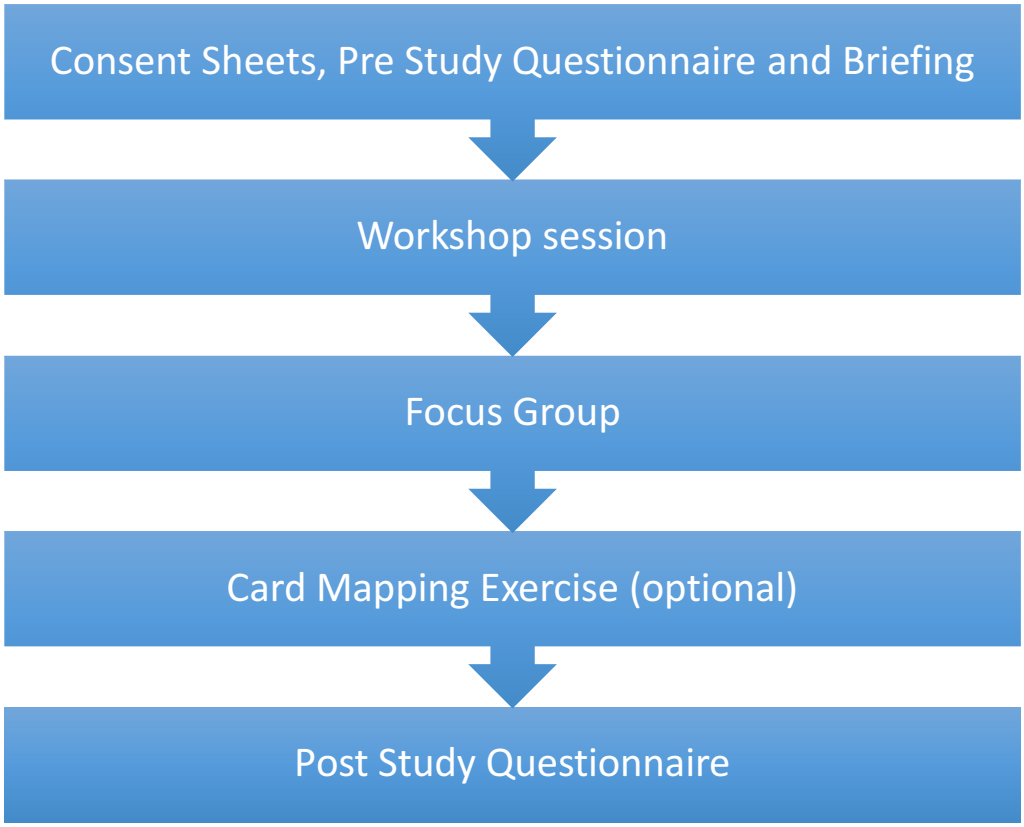
SYSTEMS

SYSTEM YOU ARE BUILDING

Augmented Reality Glasses.

The glasses can layer digital content over the real world. They can help users navigate around a new city or serve them dynamic, tailored adverts. They can be used in both private & public spaces.

Appendix 2: Workshop Structure Guide



1) **Pre Card workshop – pre questionnaire and briefing**

- Participants fill in pre-study questionnaire and consent/info sheets already on desks

- *Briefing* as to what the session involves

  - Split people into groups of 4 or 5

  - Deck already on each table split into suits: participants pick 1 system card; 1 user card; 2 constraints cards; 2 Regulation cards / 1 sub cluster –

  - Explain turning of cards – can turn when ready (max time on each); can change cards but keep discarded one; ask them to make notes as they see fit, we observe discussions and be there to help.

2) Workshop

We will record each group, time and observe the sessions; take notes, help with any queries etc – sit with 1 specific group (to see whole decision making process – rationale, reasoning, confusions)

Card	Time
turn 1 System card	Max 5 mins discussion
turn 1 User card	Max 5 mins discussion
turn 2 Constraints cards	Max 10 min discussion
turn 2 Regulation cards/1 sub cluster	Max 10-15 min discussion

Completed (40 mins)

We let them turn over when they are ready, hence intervals depend on discussion and dynamics of the group

3) Post Cards workshop:

- focus group with whole group
- card mapping exercise (optional ask them to map most and least important cards)
- post questionnaire

Focus Group Questions

Themes we want to explore in this study

1) Did they **like it**?

    a. Is it *useful?*
        i. Can they see a role for it in their work?
    b. Challenges in use?
        i. Changes they would suggest?
        ii. If more info? What type? How?

2) Do you think the concepts discussed here are **relevant** to you?

    a. Why/why not?
    b. When is best to consider them in design?

3) Comfortable dealing with *DP issues*?

4) Do you see any **barriers** to engaging with privacy/DP law?
   Like? e.g. knowledge gaps?

5) What impact, if any, on your **creativity** now having to about law during design?

6) What are your **motivations,** if any, for thinking about privacy/data protection?

    - Responsibility?
    - Why? Ethical, Legal?

7) What **current strategies** do you have for dealing with privacy in your work (if at all)

Workshop Equipment Required:

- Digital video cameras with memory; tripods setup at each table; digital dictaphones with memory;
- print off consent/information sheets for each table;
- A0; notepads; pens, post-its for each table;
- enough decks of cards (5-10?);
- Tables setup with chairs; timer?

Appendix 3: Legal Text from GDPR Cards

- **Cluster 1: Principles of DP and Consent**

- **Sub Cluster: Principles of DP**

    - Card 1 **'Lawfulness, fairness and transparency'** - Data must be processed lawfully, fairly and transparently.
    - Card 2 **'Purpose Limitation'**: Data can only be processed for defined *purposes* and cannot be used in ways inconsistent with these.
    - Card 3 **'Data Minimisation'**: Data processing must be kept to the minimum amount necessary for the specific purposes of the system or service.
    - Card 4 '**Accuracy**': Data must be kept up to date, and inaccuracies should be corrected or deleted quickly.
    - Card 5 **'Storage Limitation'**: Data must only be stored as long as is necessary for the purposes of processing.
    - Card 6 **'Integrity and Confidentiality'**: Data must be secure and protected from loss, destruction, or damage

- **Sub Cluster: Lawfulness**

- Card 7 **Lawfulness:** Lawful data processing requires user *consent*. Data processing can also be based on other legal grounds when it is necessary, like protecting the public interest.

- **Sub Cluster: Consent cards**

  - Card 8 **User Consent 1:** Consent must be freely given. The user must make a specific, informed and unambiguous agreement to data processing.

  - Card 9 **User Consent 2:** Consent must be provable. It can be withdrawn by the user at any time, and when it is given as part of a written contract it must be flagged up in clear and plain language.

  - Card 10 **Children and Consent:** Consent must be given or authorised by parents when children under 16 are using online shopping, social media and similar types of services and systems.

  - Card 11 **Special categories of data**: Political opinions, ethnic origin, biometric and health information, religious/philosophical beliefs and similar forms of data cannot be processed unless *explicit consent* is obtained or processing is *necessary***.**

- **Cluster 2: End User Rights**

  - **4 sub clusters**

    - **Sub Cluster: Transparency**

  - Card 12 **Transparency:** Information provided to end users must be concise, transparent, easy to understand and written in simple language.

  - Card 13 **Information Provision:** When end users make information requests, responses must be provided within one month, or exceptionally two. The responses should be given electronically and free of charge.

    - **Sub Cluster: Information and Access to Data**

  - Card 14 **Rights to Information:** Data controllers should provide users with information on their identity, contact details, purposes and legal grounds of the data collection.

  - Card 15 **Right of Access:** End users have a right to know who processes their data, and to request a copy for a fee. They must be

able to find out why the data is collected, what data is stored and where, and how that data is used or shared.

- **Sub Cluster: Rectification, Erasure, Restriction and Portability**

- Card 16 **Right to Rectification**: Sometimes, data stored or collected by a system that relates to a user might not be correct. All users have a right to get inaccurate information corrected.

- Card 17 **Right to Erasure/Right to Be Forgotten:** Users have a right to data deletion without delay. If user consent is withdrawn or data is no longer necessary, controllers must delete that data. This right must be balanced with other rights, like freedom of expression.

- Card 18 **Right to Restriction:** Users have a right to restrict data processing. Instead of full deletion, they may choose to restrict the use of their data. Restricted data can only be processed in limited circumstances.

- Card 19 **Information Recipients**: Controllers should let all subsequent data recipients know about rectification, restriction or erasure requests, unless this is too difficult or impossible.

- Card 20 **Right to Data Portability:** Users have the right to get their data in a structured, commonly used, machine readable format, such as XML or JSON. This allows them to easily move it to another controller.

- **Sub Cluster: Rights to Object and Automated Data Profiling**

- Card 21 **Right to Object:** Users can object to their data being processed, particularly for direct marketing. After they do so, the direct marketer must stop using their data.

- Card 22 **Right against Profiling:** Users have the right not to be profiled or subject to algorithmic decisions with legal effects. They have a right to request such decisions get human oversight and review.

- Card 23 **Restrictions:** Rights to erasure, restriction and data portability can be restricted when necessary for national security or prevention and detection of crime.

- **Cluster 3: System Designer Responsibilities**
    - **3 Sub Clusters**
        - **Sub Cluster: General Obligations**

    - Card 24 **Data Protection by Design and Default:** Technical methods and organisational approaches (like pseudonymisation) should be used to safeguard rights of users and comply with appropriate regulations

    - Card 25 **Joint Controllers:** There may be two or more data controllers jointly deciding purposes and means of processing. All of the controllers need to agree upon respective responsibilities and duties to users, and make these available to the user.

    - Card 26 **European Representative:** Controllers outside the EU who target goods and services to EU citizens on a large scale (such as social media services), should have an EU representative to oversee compliance.

    - Card 27 **Processor v Controller:** A controller may define the means and purposes of processing, and a separate processor may carry this out. Controllers need to strictly and contractually define their relationship with processors.

    - Card 28 **Record Keeping:** Comprehensive records of processing need to be maintained by controllers and processors. These include logs of data, recipients, transfers abroad, and any security measures put in place.

        - **Sub Cluster: Data Security**

    - Card 29 **Security of Processing:** Safeguards to address data security risks should be used. These would include data encryption, pseudonymisation, ensuring confidentiality, integrity, or resilience of systems.

    - Card 30 **Data Breach Notification (Authorities)**: When a data breach may impact an end user's fundamental rights and freedoms, controllers should inform the *authorities*, ordinarily within *72 hours*.

- Card 31 **Data Breach Notification (Data Subject):** Controllers need to inform end users without *undue delay* if a breach risks their fundamental rights and freedoms unless: **a)** data is encrypted; b) mitigating measures are already taken or; c) contacting all end users is too difficult.

    - **Sub Cluster: DP Impact Assessments and Prior Consultation:**

- Card 32 **Data Protection Impact Assessments:** New technologies that are risky for fundamental rights and freedoms needs a data protection impact assessment. This assessment must contain a systematic analysis of privacy risks and safeguards.

- Card 34 **Data Protection Officer:** New internal Data Protection Officers will work with organisations on all aspects of data protection such as advice and informing or monitoring compliance.

    - **Sub Cluster: New Codes of Conduct, Seals, Marks and Certification**

- Card 35 **New Codes of Conduct**: New industry codes on issues like pseudonymisation, third country transfer and child rights are being developed and monitored by competent, expert, independent bodies.

- Card 36 **New Seals, Marks and Certification:** New data protection certifications, seals and marks showing compliance with regulations are being developed and will be granted for maximum of three years.

Cluster 4: International Considerations

- **Sub Cluster: Third Countries**

- Card 37 **Data Sent Outside Europe:** Ordinarily, data should not be transferred out of the European Economic Area. Sometimes, it can be sent to specific countries that guarantee data protection like Canada or New Zealand.

- Card 48 **USA:** The EU-US Safe Harbor Agreement is now invalid. A new framework is emerging, but currently legal transfer of data requires extra safeguards like special contract clauses.

Background Cards Ch1: Definitions

- Card 42 **The Data Controller / System Designer:** Those who determine the purposes of collection and means by personal data is processed.

- Card 43 **Personal Data:** The information that directly or indirectly relates to the end user.

- Card 44 **Data processor:** those who process personal data on behalf of others

- Card 45 **Data Processing:** Processing is very broad and includes any use or operation performed on personal data. Common examples are collection, recording, structuring, alteration and storage of data.

- Card 46 **Territory:** EU data protection law also applies to those offering goods or services, and monitoring behaviour of EU citizens, even if they are outside Europe (i.e. US companies).

- Card 47 **Personal Data Breach:** this is a security breach where data is accidentally or illegally destroyed, lost, altered, or shared.

- Card 48 **Proportionality and Necessity:** Many user rights in data protection law need to be balanced against other societal rights eg national security, freedom of the press. Any balancing of rights should not be unnecessary or disproportionately impact the end user.

Appendix 4: Consent and Information Sheets

1. Privacy by Design Cards Workshops

Consent Sheet for Privacy Ideation Cards Workshops

By agreeing to be a participant you recognise the following:

All data collected during these workshops will be held in a secure and safe manner in accordance with the Data Protection Act 1998.

The data will be stored in secure digital environment at the University of Nottingham and on a password secured computer. Anonymised data that has informed publications may be placed on University data storage to comply with EPSRC (the funding body) policy.

We have a shared access folder setup by University of Nottingham Information Services (IS), and access to this server will be through IS associate accounts.

This research has passed through the University of Nottingham's ethics procedure. We are offering students Amazon vouchers for participation in the education workshops. We are not offering reimbursement for participation in industry workshops.

The workshops will be digitally recorded with video and audio to enable transcription and analysis, but where possible, data will be anonymised.

There will be no explicit recording of identifying data such as names, addresses and any references to the participants will be anonymised e.g. Participant A; Female; age 20-30; Job: programmer etc.

The data may be shared in confidence with a reputable transcription company.

Direct access to the data is limited to researchers affiliated with the project. Copies of it will not be passed onto others. Anonymised data that has informed publications may be released on request according to EPSRC (the funding body) policy.

Excerpts from the anonymised transcript data and our analysis will also be discussed with collaborating researchers at a partner project being run in the USA. No raw data (eg audio or video files) will be shared with them.

The partner project is based at New York University, with partners at Intel, Microsoft and University of California Irvine. The primary contact for this is Lesley Fosh whose email is below.

Participation is voluntary and participants are free to withdraw from the study at any time and their personal data will be erased from our records.

Email lachlan.urquhart@nottingham.ac.uk or neha.gupta@nottingham.ac.uk if this is necessary.

Data will be used in academic research and outputs publications where it will become publicly available with any quotes anonymous form.

Deciding to withdraw from the study after we've published the data will have limited effect because your data will already be publicly available.

The workshops will primarily be run by Lachlan Urquhart and Neha Gupta, at University of Nottingham.

Prof Tom Rodden, Dr Ewa Luger and Dr Mike Golembewski of Microsoft Research Cambridge and Lesley Fosh of New York University (latter three all formerly of University of Nottingham) will be in attendance at some of the workshops.

Email addresses of all researchers are provided below, so please get in touch at any time with queries.

Mixed Reality Lab and Horizon Digital Economy Research, University of Nottingham:

- Lachlan Urquhart – Lachlan.urquhart@nottingham.ac.uk
- Neha Gupta – psxng1@nottingham.ac.uk
- Professor Tom Rodden (PI) – Tom.Rodden@nottingham.ac.uk

Human Experience and Design, Microsoft Research:

- Dr Ewa Luger – ewluge@microsoft.com
- Dr Mike Golembewski - t-michgo@microsoft.com

US Project:- Lesley Fosh (NYU) - lesley.fosh@nyu.edu
We request your signature below as agreement to the terms of this study:
Signature: Date:
Print Name:

Information Sheet for Information Privacy Ideation Cards Workshops

Industry: We are running the workshops with research and development/system design teams to observe and test use of privacy ideation cards, understand their potential role in system design and get feedback on the implementation for improvement. We are not offering reimbursement for participation.

University: We are interested in running workshops with students for the same reasons, in addition to seeing if the cards are a useful educational tool for engaging with legal and ethical implications of their work (now and in the future). This reflects changes in the Computer Science Curriculum towards raising awareness of students about ethics, as required by ACM. We are offering students Amazon Vouchers for their participation.

These workshops last for approximately 1-2 hours and we would come and run them in person at your offices or at University of Nottingham (whichever is most convenient).

The workshop itself will involve 4 parts:

1: Before the workshop we will ask participants about existing attitudes to privacy, using a short questionnaire sent in advance. We will collect gender, age range and job role eg e.g. Participant A; Female; age 20-30; Job: programmer etc.

2: A high level explanation of how the cards and the ideation session will work before it starts

3: A practical ideation session using the cards in multiple groups of 4-5 people. We will record audio and video from each group using a video camera and Dictaphone. We will physically observe the sessions too, taking notes but not using any identifiable information.

4: Once the ideation session is finished we will conduct a focus group with all participants to ask for feedback, particularly on the concept, implementation, and information privacy. This will be recorded with video and audio too.

Accordingly, we will have questionnaire data, our anonymised notes, video and audio data.

Background

As regulation increasingly emphasises privacy by design, how to embed privacy concerns into the design process needs to be addressed.

We are running a project at the Mixed Reality Lab, University of Nottingham and Human Experience and Design Lab, Microsoft Research Cambridge exploring how to best help technology designers think about European data protection law and privacy.

We have developed a set of ideation cards as a response to the changing European legal landscape, where privacy by design is likely to be legally mandated by the end of 2018. We are focused on how legal requirements from privacy and data protection raise design challenges in new technologies and how designers respond. (e.g. designing for consent in the internet of things).

Our project recognises the importance of raising privacy concerns from the start of the technology design process in order to address both legal requirements and protecting user rights. Our team is made up of experts from computer science, design, HCI, ethnography, political science, ethics and law.

We have a partner project funded by the National Science Foundation running in the US at Tandon School of Engineering at New York University with partners from Intel, Microsoft and University of California, Irvine. We have a website where the cards are publicly available: www.designingforprivacy.co.uk

Contact Information

Mixed Reality Lab and Horizon Digital Economy Research, University of Nottingham:

- Lachlan Urquhart – Lachlan.urquhart@nottingham.ac.uk
- Neha Gupta – psxng1@nottingham.ac.uk
- Professor Tom Rodden (PI) – Tom.Rodden@nottingham.ac.uk

Human Experience and Design, Microsoft Research:

- Dr Ewa Luger – ewluge@microsoft.com
- Dr Mike Golembewski - t-michgo@microsoft.com

US Project:

- Lesley Fosh (NYU) - lesley.fosh@nyu.edu

2. Expert Interviews

Information Sheet for Expert Interviews Study - January 2016

Title: Regulation By Design for Smart Ambient Technologies (Internet of Things?)

This research will explore perspectives from leading experts in technology law, regulation, human computer interaction and technology design.

It builds on the concept of regulation by design as a solution to regulatory challenges posed by emerging information technologies.

Our focus is on smart ambient technologies, and the need to address challenges to protecting user rights and their agency (eg ensuring control and choice over how personal data is shared, used, accessed etc)

We want to explore the current relationship between technology designers and regulators/lawyers, and how they may come together to work in the future.

In particular, we want to consider barriers and commonalities between these communities. We are looking to find best ways to help them work together, and mapping the conceptual and practical challenges and opportunities expressed by experts is a key part of this.

Participants have been asked to participate due to extensive experience and expertise in technology law/regulation practice; technology law/regulation research; technology design/HCI practice; technology design/HCI research. Some may have experience in both practice and research; and even crossover experience in law/regulation and design/HCI.

We are using semi structured interviews with leading experts from academic and/or practicing backgrounds, drawn from universities, industry, government, and NGOs.

We would like to speak to participants in a way that is convenient to them, either in person, phone, via Skype or otherwise for around 1 to 2 hours on a range of questions. These interviews will focus on the professional experience of the experts. We are not offering reimbursement for participation in this study. The study period is from December 2015 until Summer 2016.

The primary researcher who will conduct the interviews is **Lachlan Urquhart**, a final year PhD student at the Horizon Centre for Doctoral Training and Mixed Reality Lab at the University of Nottingham, UK.

This study is part his PhD research with Professor Tom Rodden and Professor Lillian Edwards, and funded by the Research Councils UK Digital Economy Programme and the Engineering and Physical Science Research Council.

Contact details are:
Email: Lachlan.urquhart@nottingham.ac.uk
Website: https://lachlansresearch.wordpress.com/
Address: Mixed Reality Lab, School of Computer Science, Jubilee Campus, University of Nottingham

Consent Sheet for Expert Interviews Study - January 2016

Title: Regulation By Design for Smart Ambient Technologies

By agreeing to be interviewed the interviewees recognise the following:

The interviews will be conducted by Lachlan Urquhart, a PhD researcher at the University of Nottingham. His full details are in the information sheet, please contact him at any time with queries. This research has passed through the University of Nottingham's ethics procedure. We are not offering reimbursement for participation in this study.

Data collected will be held in a secure and safe manner in accordance with the Data Protection Act 1998. We will store the data on servers at the University of Nottingham and on a password protected encrypted hard drive.

The interviews will be digitally audio recorded to enable transcription and analysis.
These audio files may be shared in confidence with a reputable transcription company. The transcripts, in pseudonymous form, may also be shared and discussed with collaborating researchers (in particular PhD supervisors).

Participants are free to withdraw from the study at any time and their personal data will be erased from our records. Email Lachlan.urquhart@nottingham.ac.uk if this is necessary. Data will be used in publications where it will become publicly available in pseudonymous form. Deciding to withdraw from the study after we've published the data will have limited effect because your data will already be publicly available.

The data will be your opinions and perspectives. We will analyse this data looking for themes, relevant quotes etc. The data will be used in subsequent academic research and outputs like publications, conferences etc. We will not publicly attribute the quotes to you, but instead will use pseudonymous details to highlight your expertise. It is important for us to reflect your experience and knowledge hence we will use four metrics:

1) Years of experience (e.g. 25 years as a consultant and 5 years as a university professor);

2) Position eg Professor; Director; Senior Manager; Partner

3) Specialisms (eg networking, privacy law)

4) Group – eg law/research; design/practice

These metrics will be obtained from you at the start of the interview and you can specify your preferences around these.

We request your signature below as agreement to the terms of this study:

Signature: Date:

Print Name:

Appendix 5: Sample of Semi Structured Interview Questions

- Questions for Legal Experts

- What is your working *definition* of Internet of Things (eg key underpinning principles)?

- What do you see as the *primary regulatory challenges* posed by IoT? I'm particularly interested in your thoughts on *end user rights*.

- What *role* (if any) do you see for technology designers being involved in DP 'regulation'?

- With privacy by design/IPbD: What *challenges* do you think IPbD will bring? Do you think it can work in practice? How is it being received in your line of work?

- What *practical* challenges, if any, do you find exist for *technology designers* engaging with legal issues?

- What do you think are the best *solutions* to addressing regulatory challenges of IoT?

- What role, if any, do you see for technology designers in this?

- Questions for Technology Experts

- What is your working ***definition*** of Internet of Things (eg key underpinning principles)?

- What do you see as the ***primary regulatory challenges*** posed by IoT?

- What role design has in addressing issues of ***law*** and ***end user rights***.

- What interactions do you see ***between law*** and technology design in your work?

- What practical challenges, if any, do you find ***engaging with legal issues*** in your work?

- Explain concept of **privacy by design**?

- What ***challenges*** do you think **IPbD** may face?

- What ***role do you think designers*** should have in DP compliance

- What do you think are the best ***solutions*** to addressing regulatory challenges of IoT?

- What role, if any, do you see for technology designers in this?

Appendix 6: Pre and Post Workshop Questionnaires

1. Pre Workshop Questionnaire

Privacy Ideation Cards pre-workshop Short Survey

Gender:

Age:

Job/Specialism:

Years in the current role:

Years in the profession / industry:

- **Have you had any contact with data protection/information privacy in the past for professional purposes?**

If so, in what capacity?

_____

- **Have you ever used the concept of data protection / information privacy in personal life?**

If so, please explain?

_____

- **What are your motivations for thinking about data privacy/data protection?**

Please explain?

_____

- **What level of knowledge do you feel you have about data protection/information privacy?**

1	2	3	4	5
Limited		Some		Expert

- **What sources do you use for finding out about data privacy/data protection ?**

_____

- **Do you feel comfortable engaging with challenges around users' information privacy in your work?**

1	2	3	4	5
Not comfortable		Somewhat		Very Comfortable

Why?

_____

- **Do you consider the informational privacy of your users to be an important consideration in your work?**

1	2	3	4	5
Not at all		Somewhat		Completely

Why?

_____

- **To what extent you think system designers have a responsibility to think about information privacy?**

1	2	3	4	5
Not at all		Somewhat		Completely

Why?

Would you be interested in attending a follow on interview or focus group? Yes/ No

If so, please contact us.

2. Post Workshop Questionnaire

Privacy Ideation Cards post-workshop Short Survey

Gender:

Age:

Job/Specialism:

Years in the current role:

Years in the profession / industry:

- **Do you consider the informational privacy of your users to be an important consideration in your work?**

1 2 3 4 5

Not at all Somewhat Completely

Why?

_____

- **Did you find the cards practical to use?**

1 2 3 4 5

Not at all Somewhat Completely

Please explain ?

_____

- **Did you like the design of the cards?**

1 2 3 4 5

Not at all Somewhat Completely

If so, in what capacity?

_____

- **Were the cards easy to use?**

1 2 3 4 5

Not at all Somewhat Completely

If so, please explain?

_____

- **Have you ever heard of the concepts that were on the cards ever before - at work or outside?**

Please explain?

_____

- **Was the language on the cards easy to understand?**

1 2 3 4 5

Not at all Somewhat Completely

Please explain?

_____

- **Would you want to know more about the concepts that were on the cards?**

Yes / No / Maybe

Please explain why?

_____

- **What are the current methods used by you for engaging with privacy requirements at work?**

Please explain?

_____

- **Are these methods effective in serving your requirements about information privacy?**

Please explain?

_____

- **In what other form would you like to see or use the information that was given on the cards (e.g. a website or a book), and why?**

Please explain?

_____

- **Were the symbols on the cards easy to understand?**

1 2 3 4 5

Not comfortable Somewhat Very Comfortable

Please explain why?

_____

- **Would you recommend these cards to anyone you know?**

Please explain who, why ?

_____

- **Do you think these cards will be useful to you at any point in your work / personal life?**

Please explain?

_____

- **What would you like to change about the cards?**

Please explain?

_____

- **Have the cards made you think differently about the way you see user information privacy ?**

1	2	3	4	5
Not at all		Somewhat		Completely

Why?

Would you be interested in attending a follow on focus group or interview? Yes/ No

If so, please contact us.

Appendix 7: Legal Expert Questionnaire

I Consent

1) To what extent do you agree or disagree we should investigate how designers would ensure they obtain explicit informed consent?

1 2 3. 4 5 6 7 8 9 10
[Strongly Disagree] [Neither Agree nor Disagree] [Strongly Agree]

Please Explain Your Answer:

2) How important or unimportant do you think consent is as a legal mechanism for protecting human autonomy in ubicomp systems?

1 2 3. 4 5 6 7 8 9 10

[Very Unimportant] [Neither Important or Unimportant] [Very Important]

Please Explain Your Answer:

II Right to Be Forgotten

3) To what extent do you agree or disagree we should investigate how designers would implement the right to be forgotten?

1 2 3. 4 5 6 7 8 9 10
[Strongly Disagree] [Neither Agree nor Disagree] [Strongly Agree]

Please Explain Your Answer:

4) How important or unimportant do you think the right to be forgotten is as a legal mechanism for protecting human autonomy in ubicomp systems?

1 2 3. 4 5 6 7 8 9 10

[Very Unimportant] [Neither Important or Unimportant] [Very Important]

Please Explain Your Answer:

III Data Breach Notification

5) To what extent do you agree or disagree we should investigate how designers would implement 24 hour data breach notification requirements?

1 2 3. 4 5 6 7 8 9 10
[Strongly Disagree] [Neither Agree nor Disagree] [Strongly Agree]

Please Explain Your Answer:

6) How important or unimportant do you think breach notifications are as a legal mechanism for protecting human autonomy in ubicomp systems?

1 2 3. 4 5 6 7 8 9 10

[Very Unimportant] [Neither Important or Unimportant] [Very Important]

Please Explain Your Answer:

IV Privacy by Design

7) To what extent do you agree or disagree we should investigate how designers would implement privacy by design?

1 2 3. 4 5 6 7 8 9 10
[Strongly Disagree] [Neither Agree nor Disagree] [Strongly Agree]

Please Explain Your Answer:

8) How important or unimportant do you think privacy by design is as a legal mechanism for protecting human autonomy in ubicomp systems?

1 2 3. 4 5 6 7 8 9 10

[Very Unimportant] [Neither Important or Unimportant] [Very Important]

Please Explain Your Answer:

Thank you for your time and answers. The main part of the questionnaire is now complete (although there is an optional section below which we would be very keen for you to complete).

Please use this final space for any further comments or recommendations on areas we should consider (especially noting if these areas should be in addition to or instead of the four we have suggested.)

Below is an optional part of the survey asking you to please reflect on which data protection principles you think are the most or least relevant to consider as parameters of privacy by design in ambient interactive systems. There is a scale of 1- 10 for rating of importance, and a text box for qualitative feedback.

- How important or unimportant do you think it is to investigate how designers ensure personal data shall:

1) Be processed fairly and lawfully?

2) Only be collected for specific purpose/s and not used for any further purpose/s incompatible with those?

3) Be adequate, relevant and not excessive for the reason of collection (proportionate)?

4) Accurate and up to date(quality of data)?

5) Not be kept for longer than is necessary for the purpose/s of collection?

6) Processed in accordance with the rights of data subjects e.g. subject access rights, control of data integrity, right to object to data processing etc?

7) Be protected against unauthorised or unlawful processing, damage, accidental loss or destruction via appropriate technical and organisational measures?

8) Not be transferred outside the European Economic Area unless adequate protection for the rights and freedoms of data subjects exists in the destination country/territory?

- For your 3 most important principles please explain why you chose these?

- For your 3 most unimportant principles please explain you chose these?

Appendix 8: Legal Areas for Smart Metering

Area of Law	Relevance
International Law	Understanding how internationally agreed environmental regulations that states need to comply with manifest locally eg how do Carbon Dioxide reduction obligations under the Kyoto Protocol filter down to citizens
Tort Law/Delict	Analyse how duties of care and liabilities are managed in the smart grid, eg with fault of smart metering causing issues for vulnerable tenants in rented property.
Intellectual Property Law	Examining protection for smart meter design, manufacture and use through trademarks, patents, registered and unregistered designs, copyright and database rights.
Consumer Protection Law	Understanding protection for consumers on sale of goods and provision of services around smart meter rollout programme eg how Smart Meter Installation Code of Practice engineers do not breach these.
Product Safety Law	Ensures products meet standardised thresholds of safety, do not harm public health, addresses issues of liability when harm occurs eg with faulty smart meters
Administrative Law	Allow citizens to have decisions of public bodies reviewed by judges in court eg questioning actions of a council or the Department of Energy and Climate Change for delays in the programme
Environmental Law	Allow users more insight into how the energy generators produce energy eg at nuclear, fossil fuel power plants; also analyse controls over plastics and materials that can be used in manufacture of smart meters
European Law	A significant source of law with Directives and Regulations and policy agendas that shape everyday life eg Smart Metering is an EU Policy
Data Protection Law	Controls how consumption data can be shared or accessed, by whom, for how long, for what purposes, how it is stored…
Public Procurement Law	Oversight of how contracts were awarded by the government to companies for the national smart meter rollout
Housing Law	With council housing what rights do tenants have around installation of smart meters in homes eg can they object? In communal housing how are costs distributed for problematic installations eg in listed properties?
Criminal Law especially Evidence	Access to consumption data from smart meters, financial records, bill payments from energy firms or insurance companies for evidence in criminal investigations e.g. RIPA 2000 was formerly used by councils for obtaining covert information to assist investigations and enforcement of civil or criminal actions. [245]
Disability Law	Protecting vulnerable people from fuel poverty and ensuring their rights are not adversely affected by smart meters? Ensuring *reasonable adjustments* in smart meter interfaces for blind, deaf etc.

[245] http://www.telegraph.co.uk/news/uknews/crime/8868757/Councils-have-mounted-millions-of-snooping-operations-in-past-decade-finds-report.html