Final_Draft_Summer_2016

Working Title:

New Directions in Information Technology Law: Learning from Human Computer Interaction

Authors: Lachlan Urquhart and Tom Rodden

Affiliation: School of Computer Science, University of Nottingham, Nottingham, UK

Email: lachlan.urquhart@nottingham.ac.uk

Address: Mixed Reality Lab and Horizon Digital Economy Research, School of Computer Science, Jubilee Campus, University of Nottingham, NG8 1BB

Biographies:

Lachlan Urquhart is a Research Fellow in Information Technology Law at Horizon Digital Economy Research Institute, School of Computer Science, University of Nottingham.

Tom Rodden is Professor of Computing, Deputy Director of Horizon Digital Economy Research Institute, School of Computer Science, University of Nottingham, and Deputy CEO of the EPSRC.

Introduction

Effective regulation of emerging technologies, like the domestic internet of things (IoT) and the underpinning algorithms, requires a range of approaches. In this paper we focus on the use of technology design as a regulatory tool. Within IT law, there has long been recognition that technology design can be used to shape and regulate individual behaviour (Lessig, 2006; Reidenberg, 1998). In this paper, we assert that regulation, as a concept, has broadened sufficiently that designers are now regulators. Accordingly, we need deeper understanding of their epistemological positions to better situate their role within technology regulation. Accordingly, we look at a specific domain of design, human computer interaction (HCI), and three prominent concepts from this community. We present these concepts to reframe regulatory dimensions of domestic IoT showing what HCI designers can offer as regulators, and more broadly, highlighting channels for conceptual alignment of the HCI and IT law communities.

HCI prioritises understanding the social context of technology, questioning the interactions and relationships between end users and technology. Rights of end users, and responsibilities of designers are often the focus of inquiry in technology regulation, from ensuring consumer rights are protected to compliance with data protection law. However, understanding how technologies impact rights of users, and how designers can respond effectively, requires a turn to the context of use. The user centric focus of HCI can provide valuable perspectives on designing effective regulatory strategies. Furthermore, we argue current models of technology regulation in IT law do not give sufficient weight to the lived, contextual experiences of how users interact with technologies in situ.

To understand what an HCI led approach can offer IT law and technology regulation, we focus on three prominent concepts: trajectories (Benford et al, 2009), affordances (Norman, 2013) and provenance. We reframe these design concepts within the context of regulation. Firstly, we look at the growing emphasis on retaining provenance with domestic IoT objects. We argue this can inform debates around the right to be forgotten by considering the balance maintaining the history and stories of objects with the legal rights of end users over their personal data. Secondly, we consider the connected concepts of affordances, signifiers and mental models (Norman, 2013). These concepts help structure thinking around how interactions are designed with technologies and the importance of shaping and mediating user behaviour through design. This offers insights for thinking about designing regulatory interventions, highlighting the importance of looking beyond the technological artefact, to the setting, relationships and interactions users have with systems in context. Regulating domestic IoT requires engaging with the home: a heterogeneous, sensitive, socially contested domain composed of local routines, hierarchies and complex relationships between members. HCI can offer support on understanding this too. Lastly, we consider the regulatory challenges around consent mechanisms for obtaining informed user consent with the IoT. We do this by repurposing an approach, trajectories (Benford et al, 2009), ordinarily used for designing user experiences with a technology,

Motivation and Context

Our three concepts already have significant traction in the HCI community, but we are reframing these for a technology law and regulation audience. To understand why we are doing this, firstly we need to outline the number of premises which inform the arguments in this paper.

Firstly, we believe effective regulation of and by information technology (IT) requires a greater dialogue between those who build the technologies, and those who seek to regulate them. It has long been recognised that technologies can have politics (Winner, 1980), and that they can be used to instantiate regulatory norms within a technical architecture (Brownsword, 2004). Good examples include privacy by design (Cavoukian, 2011; Danezis,

2014) situational crime prevention (Von Hirsch, A., Garland, D., & Wakefield, A. 2004) or digital rights management (Jondet, 2006). Whether the goal is towards compliance and norm enforcement, nudging towards desirable behaviours (Sunstein and Thaler, 2012) or protecting user rights, the technology has a key regulatory role to play in mediating end user behaviour. In particular, the 'algorithms' underpinning many domestic IoT systems are the instantiations of design decisions that define the processes, permissions and consequences of using a system for end users. Accordingly, we argue there needs to be an increased understanding of the theoretical tools used by those who are designing interactions between users and technologies.

Secondly, we are concentrating our inquiry on the field of human computer interaction, due to its focus on the human element of IT. A significant strength of HCI, as a field of design, is the proximity of such designers to users. HCI designers focus on the contexts of technology use, reflecting the interests and environment of end users in order to design better systems. Designing user interfaces and experiences that meet the expectations and needs of end users is a key part of this (Shneiderman, 2012). However, HCI is broader than just usability heuristics and metrics and has been undergoing a shift from utilitarian concerns like interface efficiency and optimisation towards more cultural and ethical implications 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 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). Furthermore, HCI has long been open to interaction with other disciplines, integrating many perspectives as it has grown (Rogers, 2005) such as cognitive sciences (Gibson 1979; Hutchins, 1995) or ethnomethodology from sociology and anthropology (Garfinkel, 1967; Crabtree, Rouncefield and Tolmie (2012)). We believe there needs to be greater interaction between the Law and HCI communities, and elsewhere we have argued about routes to greater integration, through the concept of 'user centric regulation' (Urquhart, 2016; Urquhart and Rodden, 2016). In this paper, we are trying to understand how concepts from HCI can reframe legal discussions and situate the role of designers in regulation, as we shall discuss below.

Thirdly, we contend the definition of regulation has sufficiently broadened to accommodate a view of HCI designers as regulators in their own right. Selznick's (1985) more traditional, state centric view of regulation as "*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) can be contrasted with Black's emphasis on the role of non-state actors in regulation. Black's wide definition states: "*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). Other authors support a view that regulation has expanded to accommodate different types of control; purposes and actors. With control Baldwin and Cave (1999) assert regulation is "*all forms of social control, state and non-state, intended and non-intended*" (p91); with purposes, Jaap Koops (2006) argues regulation involves "*controlling human or societal behaviour by rules or restrictions*" (p81); and with actors, Leenes (2011) argues "*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).

As we can see, the practice of regulation is no longer limited to the purview of the state or a legislative mandate, but social control and behaviour shaping by a range of actors. Nevertheless, the state retains a key role in regulation due to legitimacy and authority (Leenes, 2011; Hood and Margetts, 2007). Indeed, as Black's work more generally argues, we have moved to a 'post regulatory state' where there is a *'hollowing out of the state'* through the growth of 'decentred regulation' (Black 2001, p106-122), involving regulatory agencies like "*governments, formal or informal associations, firms…professional advisers, accreditors, auditors, non-governmental organisations, charities, voluntary organisations, and so on*" (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 to improve their powers to steer and control these decentralised institutions (Black, 2007, p58). Government encourages hybrid regulation between state and non-state actors in both self-regulation (Black, 2001) and co-regulation (Marsden, 2011; Marsden and Brown, 2013), and increasingly we see '*regulation in many rooms*' (Black, 2007, p63). A good example is Article 25 of the General Data Protection Regulation 2016 requiring information privacy by design, where there is an explicit legal turn to technology designers in doing data protection compliance. We maintain these shifts in regulation generally are sufficiently broad that designers of technology can be seen as regulators too. However, the nature of their new role within regulation is not settled. As Reidenberg (1998) long ago argued "*the technical community, willingly or not, now has become a policy community, and with policy influence comes public responsibility* (p584)." More critical inquiry is necessary to understand the nature of their responsibility, for example how they can be deemed legitimate regulatory actors (Leenes, 2011) and what this community can bring to regulation. Elsewhere, we argue their user centric focus is key to their legitimacy (Urquhart, 2016), but given the range of sources, activities, aims and methods now involved in regulation, learning what HCI designers have to offer to the traditional regulatory community is key.

Lastly, the HCI concepts presented have been drawn from our experience, and respective understanding of both communities. For both groups to work together as 'regulators' (in the sense noted above), growth of a common epistemological toolbox is necessary. This begins by understanding the mind-set of each community. It is important to observe that the field of HCI is broad, with work from more quantitative, statistically orientated research focused on tracking usability of interfaces (e.g. tracking performance of a user trying a novel computer interface technique) to more qualitative, experiential design (eg thinking about designing user interactions with artistic content on smart displays in a town high street). On the more qualitative side, many mainstream HCI designers have moved past systems theoretical models to understanding how end users interact with systems (Bansler 1989; Ehn and Kyng, 1987; Floyd et al, 1989; Suchman, 1987). Instead, they have developed participatory methods and approaches to understanding the social context of the technology, obtaining users input during the design process to ensure technologies better meet their needs (Bjerknes and Bratteteig, 1995; Ehn and Kyng, 1987; Törpel et al, 2006).

Technology regulation requires a similar focus on users' interactions with technology in context. However, current systems theory based models of understanding technology regulation remain prominent (Lessig, 2006; Murray, 2008; Hood and Margetts, 2007). We cover these themes in much greater depth elsewhere (Urquhart and Rodden, 2016; Urquhart 2016), but to recount briefly, Lessig's (2006) 'code is law' has been canonical in expressing how code can be functionally comparable to law as a regulatory mechanism

(Lessig, 2006, p5). As Lessig puts it "*technology is plastic. It can be remade to do things differently*" (p32-37). His model of regulation involves mixing and interaction of four interdependent modalities (i.e. market forces, social norms, law and architecture) (p72-74) acting on the passive subject of regulation: the individual. His model does not assign agency to the individual, which is a significant shortcoming. Murray addresses this concern in his model of networked communitarianism, where individuals have agency, existing in a networked environment where actions to and by them affect others (Murray, 2008, p301). The individuals form a community, "*which determines whether or not a regulatory intervention is successful or if it fails*" (Murray 2008, p302). Regulation needs to symbiotically respond to the community, adjusting to their needs, learning what is necessary by observing the community, how they communicate both internally and with other subsystems (Murray, 2008, p309-315; Luhmann, 1996; Forrester, 1961). Whilst building on Lessig, by giving users agency, we argue the need to go further than Murray's model where individuals are still abstracted to nodes within a series of interacting social systems.

These theories have been invaluable in the development of IT law. However, the time has come to move past social systems theory led models. For technology design to progress as a regulatory tool, and to closely align the two communities, users lived experiences with technologies need to be foregrounded and integrated into regulatory interventions. Current models, where users are nodes or dots within interacting social sub-systems, do not foreground how the user interacts with a technology in a sufficiently situated way. Accordingly, we argue they cannot design regulatory interventions that address contextual needs of users. Instead, IT law needs to integrate with HCI, to move towards user centric approaches (Urquhart, 2016) to developing ways of providing a richer, situated understanding of end users, their needs, practices, values and expectations. By focusing at this level, the users' perspectives are brought to the fore, where the relationship with technology in context can be understood, enabling regulatory interventions to be designed accordingly.

HCI has the necessary tools, from conducting design ethnographies to investigate the social context of design, actors and practices therein (Crabtree, Tolmie and Rouncefield, 2012) to participatory and value sensitive design methods that foreground the interests and values of users (Friedman, Kahn and Borning, 2008; Törpel et al, 2009). The practicalities of adapting these tools to focus on regulation and legal concerns of users are beyond the scope of this paper. As an aside, we have developed an approach to support designers doing privacy by design in practice by bringing legal principles into the design process (Luger, Urquhart, Rodden and Golembewski, 2015). However, the process of situating the conceptual and practical role of designers in regulation needs greater attention. By presenting key concepts with traction within the HCI community, we offer an accessible entry point to understanding epistemological commitments from HCI, to help both communities to move forward together.

We will now situate our analysis by briefly discussing algorithms and the domestic internet of things. To clarify, in this piece we focus our examples not on abstract algorithms, but on domestic internet of things devices (themselves composed of hardware and firmware based on algorithms). We are interested in understanding the human context of algorithms, as they shape the lives of end users, and feel this approach is more fruitful than isolating just one algorithm or process for critique.

Algorithms and the Internet of Things

Algorithms have prompted much critique as a subject matter (Gillespie and Seaver, 2016) but fundamentally, an algorithm is just a set of instructions, and accordingly can be framed very broadly. They are the building blocks of many technologies and services, instantiating approaches and processes into formal computational languages.

As Gillespie (2014) has argued, computers are 'algorithm machines' as they are "*designed to store and read data, apply mathematical procedures to it in a controlled fashion, and offer new information as the output*" (p1). Similarly, they have a key role in software, as Kitchin (2016) puts it "*software is fundamentally composed of algorithms: sets of defined steps structured to process instructions/data to produce an output*" (p1). Whilst there is concern around the social impacts of algorithms, there is a risk of weaving a deterministic narrative about their impact, as Barocas et al (2013) capture when they argue: "*A simple test would go like this: would the meaning of the text change if one substituted the word "algorithm" with "computer", "software", "machine", or even "god"? What specifically about algorithms causes people to attribute all kinds of effects to them?*" (p3)

Accordingly, we focus on the socio-technical context of the algorithms, in our examples, the home, following Kitchin's (2016) position where he states:

"… *algorithms are not formulated or do not work in isolation, but form part of a technological stack that includes infrastructure/hardware, code platforms, data and interfaces, and are framed and conditions by forms of knowledge, legalities, governmentalities, institutions, marketplaces, finance and so on. A wider understanding of algorithms then requires their full socio-technical assemblage to be examined, including an analysis of the reasons for subjecting the system to the logic of computation in the first place*." (p12)

The focus should be on how algorithms instantiated within IoT technologies mediate the practices and behaviours of users. However, emphasis needs to shift to how they operate within their context of use, and to reflect on how they shape the lived experiences of users. Such analysis cannot stem from algorithms seen purely in their abstract form. Internet of Things devices are socially embedded technical artefacts. They use algorithmic approaches to mediate many mundane and routine aspects of a user's daily lives. The ambient nature of the technologies can pose challenges for regulating data driven interactions. Effective regulation through design needs knowledge of how end users use, negotiate and manage these technologies in situ. Therefore, our inquiry focuses at the human level, as opposed to looking at the technicalities of the algorithms which underpin these systems, in their different syntactical instantiations.

We now turn briefly to the nature of the IoT (Ashton, 2009). Various technology and consultancy firms predict vast 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). IoT builds on a long lineage of foregoing technological visions, including ambient intelligence (Aarts & Marzano, 2003); pervasive computing (Satyanarayanan, 2001), ubicomp (Weiser, 1993; Caceres & Friday, 2012;), calm computing (Weiser & Brown, 1997), and home automation (Crabtree and Rodden, 2004; Harper, 2003). In terms of drivers, 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). We do not offer a canonical technical definition of IoT, and indeed as McAuley (2016) as argued, this may not be necessary as "*<u>IoT is not about technical capabilities or novelty</u>, rather it is a social phenomenon that reflects a significant proportion of society, and importantly businesses, who have started to recognise that there is <u>value in building a virtual presence for many of our everyday physical things</u>*" (p1). Nevertheless, to appreciate what different organisations practically mean by IoT we look at a spread of definitions from across different stakeholders including: UK Government Office for Science (Walport, 2014, p13); EU Article 29 Working Party (A29 WP 2014, s1.3); UN International Telecoms Union (2012, p1); Cisco (2013, p1); Internet Engineering Task Force (Arkko et al, 2015, p1) and Cambridge Public Policy (Deakin et al, 2015, p8). Accordingly, we find IoT is largely seen as:

- 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

Many IoT application areas exist, like the smart built environment, healthcare, wearables and intelligent mobility, but we focus here on the domestic setting, with objects in the home and the domestic internet of things (eg home automation of energy, security or lighting management).

In terms of regulatory dimensions of IoT, privacy is a prominent concern. Brown (2015) argues IoT is challenging for privacy precisely because it operates in private settings, like homes, and presents an attack target that is harder to secure (p25). Profiling is also a concern, with detailed inferences being drawn about daily life 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). Further to this point, Deakin et al (2015) note combinations of non-personal data may create sensitive personal data (which consequently need explicit user consent) such as 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).

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 are other privacy concerns (A29 WP, 2014 p6; Rose et al, 2014, p26-29). Indeed, there is significant user apprehension over 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). Later we consider examples of how users engage with IoT type technologies in context, but for now we note the need for control. New rights in the GDPR (2016), like the right to be forgotten or right to data portability, seek to increase user control over their personal data. As we discuss below, perspectives on provenance with IoT objects provides another layer to how to balance valuable rights that increase control against other interests.

Object Provenance and The Right to Be Forgotten

We begin by outlining the concept of provenance, and work within HCI in this domain on IoT and digitally augmented objects. We then look at discussions around the RTBF, focusing on the process balancing against other interests, and what the concept of object provenance adds to these discussions.

Our first concept is the notion of *provenance*. Provenance as a term has differing connotations for different communities. For antiques enthusiasts, it may mean knowing the historical ownership, financial records, and social or cultural knowledge surrounding a sculpture, musical instrument or painting. For the sustainability minded individual, it may mean knowing more about the food supply chain, for example with tinned sardines in the cupboard, who caught them, where, the method used and the sustainability of that breed. Broadly, provenance is concerned with understanding the history of an object.

Within HCI, we see a range of approaches to creating provenance from information management or archival orientations to creation of cultural objects with digital stories and histories. For the former, provenance can be as simple as tracking and recording the changes made to pieces of information, for example in a digital document. The W3C Data PROV model works in this vein, defining provenance as "*a record that describes the people, institutions, entities, and activities involved in producing, influencing, or delivering a piece of data or a thing*" (Moreau and Missier, 2012). It 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 varies from worries about linking otherwise distinct information to privacy concerns about the permanency of information they may want removed. (Bachour et al, 2015, p245)

For the former we see emphasis on the provenance of physical objects, and, particularly for the IoT, their accompanying digital footprint. Giaccardi (2011) highlights, new technologies, like IoT, enable new forms of remembering and cultural heritage is now being curated across different, non-traditional forums. Speed et al (2013), for example, considers the idea of creating a social network between objects, namely cars, where photos and stories of travels of occupants are shared with other cars on the motorway. Earlier project, Tale of Things and Electronic Memory (TOTem), looks at creating an 'internet of old things', where people attach their memories, stories and meaning to analogue objects like cups and spoons using QR codes or RFID tags (Barthel et al, 2011). Both projects reflect on the implications of personal narratives and memories travelling with physical objects, not just users. Significant Objects is another take on the theme, where random objects were sold on eBay attached with fictitious narratives of their history written by professional writers like William Gibson and Bruce Sterling (Glenn and Walker, 2012). They sold for increasingly more with these stories attached, highlighting the value of provenance. As an aside, Sterling coined the term 'Spimes' to describe objects that exist across space and time, with a physical instantiation and digital story (Sterling, 2005; Urquhart, 2013). Other projects like Where's George (Brockmann and Theis, 2008) and Book Crossing (Eidenbenz et al, 2012) track the provenance of money and books respectively, through global following of notes or novels in a community led online database. In the IoT space, art projects like Brad the Toaster, have added an element of object agency to the mix, where an object who 'feels' neglected (i.e. not being used to make toast regularly enough) can opt to put themselves up onto eBay and find a new owner who to use them more (Vanhemert, 2014). With this object goes the story of negligence at the hands of his previous owners.

Two particularly interesting examples have emerged recently. Darzentas et al (2015) have been looking at Warhammer 40K, understanding the community of players, the processes of creation, play and curation around war-gaming miniatures, and importantly, how to digitally augment their footprints whilst not disrupting core practices of the game or the community. The provenance around objects could grow as the shift to IoT progresses, as Darzentas et al (2016) have argued "*The digital footprints of things in the future IoT may be far richer, pervasive and persistent than traditional forms of documentation. Indeed, it could well be that the entire existence of future things, from their manufacture through to everyday use by various owners, to ultimate obsolescence, might be charted and examined, or even re-experienced*" (p2).

Secondly, the Carolan Guitar project is a travelling guitar adorned with a range of machine readable codes called Artcodes (Meese et al, 2013). The codes are both aesthetically pleasing and link to a wealth of content about the guitar, its travels, videos of who has played it, and photos from recent gigs. Benford et al (2016) term this an 'accountable artefact' i.e. "*a 'thing' that becomes connected to an evolving digital record over its lifetime and that can be interrogated to reveal diverse accounts of its history and use*" (p1168) and such artefacts can help us unpack the relationship between the physical objects, digital records and how the two interact. These devices may have multiple owners over their lifetime, and this project seeks to understand how the relationships between object, user(s) and record (s) are managed. For now, we merely flag this work to highlight the extent to which we are seeing a shift towards objects having their own stories to tell, beyond the interests of individual users, and by looking at IoT objects in this way, it gives us a richer understanding of what is at stake when pitching the balance between object memories and legal rights.

Scholars like Mayer Schonberger (2009) and Kitchin & Dodge (2007) have been critical of record keeping enabled by the digital age, and see forgetting as an important phenomenon in the digital age. For Mayer-Schonberger (2009) analogue forgetting is a virtue because it lets bad memories fade, fragment and decay. Yet, digital storage, lossless file formats and global accessibility of indexed, searchable and retrievable information means "*today, forgetting has become costly and difficult, while remembering is inexpensive and easy*". (p92) With temporality diminished, he argues information from different life points is held and judged entirely in present day, without context or coherent chronological narrative leading to a "*timeless collage*" (p124).

Similarly, Dodge and Kitchin (2007) argue within the context of life-logging and pervasive computing, that forgetting is so important in the digital age that ethically different forms of forgetting should be built into systems where "*a range of algorithmic strategies could be envisioned, such as erasing, blurring, aggregating, injecting noise, data perturbing, masking, and so on, that would be used to `upset' the life-log records*." (p442) Mayer Schonberger (2009) proposes users should set a timeframe for data expiration dates in order to prompt reflection on the lifespan of their information (p173). He also advocates mimicking human forgetting patterns, allowing gradual decay of memories, partial obfuscation or "rusting" where retrieval requires trigger events or takes longer.

Legally speaking, the strong legal footing for the right to be forgotten (RTBF) is interesting to consider. It has two flavours, with search engine delisting of content, due to the *Google Spain* case (2014), and the broader right to erasure, as found in the Article 17 General Data Protection Regulation (GDPR, 2016). We focus on the latter, briefly, but there has been extensive discussion around both (Ausloos and Kuczerawy, 2015; Bernal, 2011). Legally, much of the tension around the right has focused on where the balance should be pitched between the rights of individuals to control what is done with their personal data, and rights of the collective in freedom of information (Edwards, 2016). In essence the final GDPR text states that data subjects have a right to personal data deletion without delay given certain conditions. Most relevant are if the user withdraws consent and there are no other grounds for processing, or data are no longer necessary for the original purposes of collection. As the recitals stress, this right is particularly important for adults seeking to remove information about their actions, on social media for example, that were carried when they were children. [1] This right must be balanced with other rights such as when processing is necessary for "*exercising the right of freedom of expression and information*" or "*for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes*" (Article 17(3), GDPR). With archiving in particular, a range of safeguards for individuals' rights and freedoms are necessary (Article 89(1)). This amounts to putting technical or organisational processes in place to ensure data minimisation, possibly even using pseudonymisation too. [2] These rights do not extend to the deceased.[3]

---

[1] Recital 65

[2] Recital 156

[3] Recital 158

Interestingly, where there has been a deletion request, but the data has been made public, Article 17(2) states "*the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data. (emphasis added)*" (GDPR, 2016)

Establishing who is responsible for ensuring protection of these legal rights, i.e. the controller, can be more complex in practice, when dealing with physical objects that have passed to multiple owners over their life time. What are the limits of the household processing exemption to the GDPR, when much of the curation may be done by hobbyists or in the context of the home? What is the nature of the responsibilities? Even if a responsible party can be established, thinking about the *balancing process*, not just from the perspective of the user, but from the object provides a different angle. How will we balance individual interests against interests of the object as a cultural or social artefact? If objects are moving towards carrying digital stories and memories as they move through the physical world, this creates richer provenance about their existence. This enables preservation, curation and creation of archives, beyond formal institutions of galleries or museums, and instead at the level of individual objects and communities. As the projects show above, these practices can deliver value and foster creation of new cultural heritage. However, user control over their data, stories and memories, and a right to be removed from these archives is an equally important right. Hence, thinking about what is at stake in balancing becomes more nuanced when considered from the perspective of the object provenance. It is not the polarised extremes of absolute privacy vs absolute censorship, but sits somewhere in the middle. In any case, wherever balances are pitched, the two communities, HCI and law, need to come together and think about practicalities of how to implement their balance.

On that point, privacy by design has much to offer here, but binary absolutes of delete/not delete may come to be too blunt in the future. The binary instrument of complete deletion on a RTBF request may be prudent, but in others it may not. Will we see emergence of more ephemeral interactions with objects? Expiry dates? mimicking of human memory? In any case, there will need to be technical implementation, requiring dialogue between these two communities. For example, lawyers helping to navigate if this kind of curation of stories and memories through a range of objects can be deemed 'archiving'? And thus a balance between the public interest in archiving against RTBF can be made? What about memorialisation of objects, as we see with social media profiles, will there need to be legal guidance of any transition? What are reasonable steps that need to be taken to deal with public information, and most importantly, how can designers implement these, and inform the legal community of what is possible technically. Importantly, there needs to be input from the users and communities around these objects, accordingly, HCI has much to offer in learning about what the right to be forgotten may mean in practice in a future of physical objects with digital memories. We now turn to the second notion, designing interactions with technologies.

Affordances, Signifiers and Mental Models

In this section we look at affordances. Designers are creating a device or object offering possibilities for action by the user. The interaction has to be accomplished by the user. Viewing technology as being designed for possibilities of use moves us past just the artefact to incorporating the role of users. This notion is useful for regulation as attempts to control behaviour can benefit from realising technology design actively factors in the user and their actions into the design. We argue that within the setting of the home, awareness of the social complexities, and responding to these in design can help formation of more effective regulation.

We now turn to Norman's *The Design of Everyday Things* (Norman, 2013) [4] which helps us think about how user interactions with technologies are designed. Accordingly, we briefly reflect on three of his core ideas: *affordances, signifiers and mental models*. His overall focus is on how to achieve 'good design', putting end users at the 'centre' of interest, and actively involving them in the iterative development of a product or system (Norman, 2013, p9-10). For Norman, if a user cannot use a product, that is the fault of the designer for not communicating effectively with them or understanding their needs. (Norman, 2013, p8). The relationship between designer and end user needs to accommodate human frailties, to make mistakes, as Norman puts it, "*design is concerned with how things work, how they are controlled and the nature of the interaction between people and technology… it is the duty of machines and those who*

[4] Updated version of Norman, D. (1988) *The Psychology of Everyday Things*

design them to understand people. It is not our duty to understand the arbitrary, meaningless dictates of machines" (Norman, 2013, p5-6).

One of the key concepts for understanding the relationship between user and technology is the notion of *affordance*s. Building on Gibson's work (Gibson 1979), Norman states an affordance "*is a relationship between the properties of an object and the capabilities of the agent that determine just how the object could possibly be used…the presence of an affordance is jointly determined by the qualities of the object and the abilities of the agent that is interacting*". (Norman, 2013, p11) Affordances are very much an interactive relationship, as Gaver (1991) also stresses, a key strength is they look beyond just the technology *or* user and towards the *interactions* between the two.

In shaping the relationship, effective communication between designers and users is necessary. This comes in the form of *signifiers,* mechanisms designers use to indicate that a technology can be used in a particular manner, for example, a handle on a cup enabling it to be picked up. The *nature* of signifiers is a matter of design in themselves, as they can vary greatly depending on the technology, any tool that communicates to the end user. (Norman, 2013, p14).

The signifier needs to communicate the nature of the affordance from the designer to the user, yet how users interpret the signifier will depend upon their own circumstances and understanding of the technology. Accordingly, *mental models* are key i.e. "*the conceptual models in people's minds that represent their understanding of how things work*" (Norman, 2013, p26), As different users may possess different models of what a technology does and designers cannot speak directly to users, the models users hold are particularly important, as he states "*in providing understanding, in predicting how things will behave and in figuring out what to do when things do not go as planned. A good conceptual model allows us to predict the effects of our actions*" (Norman, 2013, p26). Whilst designers have some control over how these models are formed, often the user obtains their understanding from a range of different sources. As he puts it "*conceptual models are often inferred from the device itself. Some models are passed on from person to person. Some come from manuals. Usually the device itself offers very little assistance, so the model is constructed from experience. Quite often these models are erroneous, and therefore lead to difficulties in using the device. The major clues to how things work come from the perceived structure – in particular from signifiers, affordances…"* (Norman, 2013, p26)

Bringing these elements together can give us a richer understanding of how relationships between designer and user are constructed. Furthermore, it helps us to understand how designers provide or prevent end users exercising control, especially when we consider personal data driven physical technologies, like the IoT. These same concepts could help think about how end user rights are factored into their interactions with technologies. Design for affordances that provide increased control over personal data, with designers thinking about what signifiers can help shape a positive relationship between users, technology and their information.

Within the context of domestic IoT, the setting of the home is a key consideration. The house will not become 'smart' overnight. As Edwards and Grinter (2001) have long recognised, "*new technologies will be brought piecemeal into the home; unlike the 'lab houses' that serve as experiments in domestic technology today these homes will not be custom designed from the start*" (p257). Similarly, how technologies are embedded into the home will vary, as Rodden and Benford (2011) 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). Homes are complex social spaces where different practices and routines persist (Crabtree and Rodden, 2004). As Tolmie (2002) has said "*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 of the setting (Tolmie, 2003).

To further understand how IoT type technologies integrate with the complex social setting of the home, we briefly consider a number of studies on domestic IoT and users interactions. Mäkinen (2016) study of home surveillance systems [5] 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) US study of 13 teens and 11 parents on attitudes to use of home

---

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

security cameras and smart locks to audit home entry/exit showed broad support for connected locks due to remote control, improved safety and convenience (p129). However, trust between teens and parents could be damaged by increased monitoring, and that teens would find ways to resist the monitoring (p135).[6] Choe et al (2011) similar US study[7] 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).

Domestic IoT technologies can have a range of impacts on users, and we can look beyond the artefacts and intended uses to reflect on the different interactions they create in practice. As we see, 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. These kinds of user accounts are invaluable for unpacking the kinds of social dynamics and reactions to technology that users face in context. Heterogeneous devices, interactions and user mental models of how these systems work complicate the landscape for managing legal rights in the home, like adequate control over personal data. Nevertheless, thinking about technologies and users in terms of relationships and interactions between them gives us a richer setting to reflect on how regulatory strategies can manifest in context. We now turn to the final section.

---

[6] 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.

[7] 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.

Trajectories and Designing for Consent

In this final section, we turn to the concept of trajectories and the example of how they can help structure thinking about designing for consent.

Benford et al's (2009) *trajectories* framework describes the process for designing interactive user experiences, often in performative and cultural settings e.g. theatrical performances, art installations or mixed reality games. Importantly, *experiences* involve 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 an 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 tension 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 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.*" (Benford et al, 2009).

Again, this framework was developed in the context of designing cultural experiences, for example an interactive installation in a theatre or a mixed reality game taking place across an entire city involving remote and physical players. Nevertheless, we think it has significant value for thinking about how we experience IoT technologies in the home, especially, how the intersection with regulation and legal aspects, particularly consent. To unpack this further, we now discuss the challenges with obtaining end user consent to data processing around technologies.

The normal approach to obtaining user consent is *form contracts*. The 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 where the user accepts or declines these terms by ticking a box. These are problematic for a number of reasons.

The terms of these contracts often provide terms that are not favourable to end users, from arbitration clauses to handing over your first born or your soul to the service provider (Fox-Brewster, 2014; Caddy, 2013). Consumers are unlikely to read these terms and conditions (Ts&Cs) in any case hence they do not know what they are signing up to when using a service (Smithers, 2011; Bakos et al, 2014). The recent example of Facebook manipulating users' news feeds to provoke happy or sad emotions, whilst unethical, was arguably not illegal as Facebook include a clause around research in their terms of use (). Broadly, individuals are not informed about the nature of processing, and thus the idea that they have provided informed consent becomes a legal fiction.

However, the nature of these contracts is dense, illegible, lengthy legalese hence even if they did read them, chances are they would be incomprehensible. 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.

Nevertheless, consent remains a key legal tenet in the new GDPR, although it is not the only legal grounds for data processing. 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),[8] and when consent is the grounds for legal processing,[9] it has to be *explicit*, although what that means in practice is not defined. For general consent (Article 4(11), GDPR, 2016) the requirements are that:

---

[8] Article 9(1) GDPR

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

> "*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)

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). Despite relative clarity in the law, the challenges of obtaining consent remain for the IoT where interactions may be ambient, pervasive and longitudinal. As Edwards (2016) has argued due "…*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)

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; with greater communication and a stronger relationship between different parties, 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) for example 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 feel 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. in the IoT era of embedded physical devices, intimately mediating our everyday lives, we will need consent more than ever. However, the default model cannot continue to be form contracts, consent needs to become more relevant and purposeful. We think Benford et al's (2009) trajectories framework is a useful tool for thinking about consent mechanisms within the design of user experiences with technologies, especially IoT.

Trajectories are a useful mechanism for both conceptualising, and indeed, designing, the end user experience. From our perspective, this is valuable from two perspectives. On the one hand, sensitising designers to legal concerns, such as obtaining proper consent to data processing, means they can integrate responses and approaches into the end user experience. On the other, a greater understanding of how users are meant to use technologies can help us begin to create more effective regulatory tools.

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.

1. 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.

2. 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. They 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.

3. 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.

4. 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 advice of new information around the nature of consent. 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. We now turn to brief conclusions.

Conclusions

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 means a turn to the design community, and in this paper we focus on HCI design. The user centric perspective is important to bring into technology law scholarship, as we often rely on more abstracted views of technology, regulation, and the end user. If we wish to regulate technologies effectively, then we need to engage with their context of use to understand the impacts on real users, and that means a turn to HCI. Importantly, HCI teaches us to look at the practices, routines, and social context of a technology. The regulatory challenges posed by technologies like the domestic Internet of Things, and the underlying algorithms, need to be understood in their context of interactions with end users and the environment of use. We argue, this involves an explicit turn to those who create the technologies, specifically the HCI designers who are most proximate to users. As they are not conventionally involved in regulation, the nature of their role is not well defined, and in this paper we have proposed three approaches that move towards understanding what HCI can offer IT law.

Firstly, we consider how debates around the right to be forgotten can be enriched by considering the concept of provenance. In particular, we reflect on how valuable cultural and social value preserved in the rich archive of the life of an object, which has clear interactions with users and their personal data. Accordingly, regulation needs to engage with notions of provenance, how stories are retold, and how the memories of objects are balanced against other interests, like the right to be forgotten.

Secondly, we look at the concept of affordances, and the associated ideas of signifiers and mental models. We use these to help us think about how user interactions with technologies are designed, and consequently, what scope there is for reflection on regulatory considerations during this process. Recognising the richness of the home as a setting for technology, and the nature of the relationship between designer and user, how they communicate can help structure thinking around the site of regulatory interventions.

Lastly, we provide new perspectives on overcoming the legal fiction of informed user consent through form contracts. Consent mechanisms for the IoT age need to move past reliance on Ts and Cs. Our contribution is proposing a route forward for actually changing how consent is obtained for domestic internet of things. We use the concept of trajectories, mapping different elements of the framework to the consent process: time, actors, space, interface.

Despite the range of ideas in this article, the overall goals remain modest. We are trying to prompt provocation and reflection on possible intersections between HCI and information technology law. Importantly, we offer three overarching concepts and actively frame how they can be used to reconsider regulatory challenges, particularly referring to the domestic internet of things. Long term, we hope this paper starts a process of bringing together two distinct communities, as there is significant mutual benefit from doing so. By presenting new concepts to the legal community in this way, we have started the process of exploration and a move towards building stronger links between these two fields.

References

1. Aarts, E., & Marzano, S. (2003) *The New Everyday: Views on Ambient Intelligence,* 010 Publishers, Rotterdam, Netherlands

2. Arkko, J. et al, (2015) IETF RC 7452: Architectural Considerations in Smart Object Networking, IETF, Fremont, US

3. Article 29 Working Party (2014) *Opinion 8/2014 on the Recent Developments on the Internet of Things WP 23*, European Commission, Brussels

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

5. Ausloos, J and Kuczerawy, A. (2016) From Notice-and-Takedown to Notice-and-Delist: Implementing the Google Spain Ruling, *Colorado Technology Law Journal* 14

6. Bachour. K., et al (2015), Provenance for the People: A User-Centered Look at the W3C PROV Standard through an Online Game, *In Proceedings SIGCHI Conference Human Factors in Computer Systems (CHI, '15) ACM Press, New York, NY, USA*

7. Baldwin, R., & Cave, M. (1999) *Understanding Regulation: Theory Strategy and Practice*, OUP, Oxford

8. Bakos, Y., Marotta-Wurgler, F, Trossen, D. (2014) Does Anyone Read the Fine Print? Consumer Attention to Standard Form Contracts, *Journal of Legal Studies*, 43(1)

9. Bansler, J. (1989) Systems Development Research in Scandinavia: Three Theoretical Schools, *SJIS* 1(1) at http://aisel.aisnet.org/sjis/vol1/iss1/1

10. Barocas, S., Hood, S., and Ziewitz, M. (2013) Governing Algorithms: A Provocation Piece, In *Governing Algorithms*, May 2013, New York, USA.

11. Barthel, R, et al (2011) An Internet of Old Things as an Augmented Memory System, *Personal and Ubiquitous Computing,* 17 (2) pp. 321-333.

12. Benford, S., et al (2016). Accountable Artefacts: The Case of the Carolan Guitar. *In Proceedings SIGCHI Conference Human Factors in Computer Systems (CHI,16) ACM Press, New York, NY, USA*

13. Bernal, P.A., (2011) 'A Right to Delete?', *European Journal of Law and Technology*, 2(2)

14. 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

15. 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

16. Black, J. (2002) Critical Reflections on Regulation, *Australian Journal of Legal Philosophy* 27, 1-35

17. Black, J. (2007) Tensions in the Regulatory State, *Public Law*, Spring, 58-73

18. Bødker, S. (2006) When Second Wave HCI Meets Third Wave Challenges *In Proceedings of the 4th Nordic conference on Human-computer interaction*, (NORDICHI '06)

19. Bødker, S. (2016) Third Wave HCI, 10 years later – Participation and Sharing, *Interactions - September-October*. 24

20. Brockmann, D., and Theis, F. (2008) Money Circulation, Trackable Items, and the Emergence of Universal Human Mobility Patterns. *IEEE Pervasive Computing*, *7*(4), p28–35

21. Brown, I. (2015) GSR *Discussion Paper: Regulation and the Internet of Things,* International Telecommunications Union, Geneva

22. 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

23. Caceres R., & Friday, A. (2012) Ubicomp Systems at 20: Progress, Opportunities and Challenges In *IEEE Pervasive Computing* 11(1), 14-21

24. Caddy, P. (2013) 'Surrendering your Immortal Soul': Does Anybody Ever Read Terms and Conditions?, *LexisNexis Comet*, Sept 19, 2013

25. Cavoukian, A., (2011) *7 Foundational Principles of Privacy by Design,* Information and Privacy Commissioner of Ontario, Ontario

26. Choe, E.K. et al, (2011) Living in a Glass House: A Survey of Private Moments in the Home, *Ubicomp 2011*

27. Cisco (2013) *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

28. Cisco Website, (2016) Visual Networking Index, available at http://www.cisco.com/c/en/us/solutions/service-provider/visual-networking-index-vni/index.html

29. Crabtree, A., Rouncefield, M., and Tolmie, P. (2012) *Doing Design Ethnography*, Springer Verlag London

30. Crabtree A., Rodden T. (2004) "Domestic Routines and Design for the Home" *Computer Supported Cooperative Work* 13(2), 191-220.

31. McDonald, A and Cranor, LF 0 (2008) The Cost of Reading Privacy Policies, *I/S A Journal of Law and Policy for the Information Society*

32. Danezis, G. et al (2014). *Privacy and Data Protection by Design – from policy to engineering* European Network Information Security Agency, Heraklion

33. Darzentas et al (2015) The Data Driven Lives of Wargaming Miniatures. *In Proceedings SIGCHI Conference Human Factors in Computer Systems (CHI,15) ACM Press, New York, NY, USA*

34. Darzentas et al (2016) Harnessing the Digital Records of Everyday Things, *In Proceedings of Design, Research and Society* (DRS '16) at http://www.drs2016.org/400/

35. Deakin, S. et al, (2015) *The Internet of Things: Shaping Our Future*, Cambridge Public Policy, Cambridge

36. Dodge, M. and Kitchin, R.(2007) 'Outlines of a World Coming into Existence': Pervasive Computing and the Ethics of Forgetting, *Environment and Planning* 34(3), 431-445

37. Edwards, L. (2016) Sunny Spells? Non Foggy Thinking About the Right to Be Forgotten, *BILETA 2016* available at SlideShare http://www.slideshare.net/lilianed/sunny-spells-non-foggy-thinking-about-the-right-to-be-forgotten

38. Edwards, L. (2016) Privacy, Security and Data Protection in Smart Cities: A Critical EU Perspective, *EDPL* 2(1) 28-58 at http://ssrn.com/abstract=2711290

39. Edwards, K and Grinter B (2001) At Home with Ubiquitous Computing: Seven Challenges, *Ubicomp '01* 256-272,

40. 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

41. Eidenbenz, R., Yu, L., & Wattenhofer, R. (2013) Reading Up on Bookcrossing. *The International Journal of the Book*, *10* (2) p11–26.

42. European Commission (2015) Special Eurobarometer 431 'Data Protection' http://ec.europa.eu/justice/newsroom/data-protection/news/240615_en.htm

43. Floyd et al, C. (1989) Out of Scandinavia: Alternative Approaches to Software Design and System Development, *Human Computer Interaction* 4, 253-350

44. Forrester, J. (1961) *Industrial Dynamics*, Pegasus Communications, Waltham

45. Fox-Brewster, T, (2014) Londoners Give Up Eldest Children in Public WiFi Security Horror Show, *The Guardian,* 29 September 2014

46. 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

47. Garfinkel, H. (1967) *Studies in Ethnomethodology* Prentice Hall, New Jersey

48. Gartner Hype Cycle for Emerging Technologies (2015) https://www.gartner.com/newsroom/id/3114217

49. 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), OJ, L119/1

50. Gaver, B (1991) Technology Affordances, I*n Proceedings SIGCHI Conference Human Factors in Computer Systems (CHI, 91) ACM Press, New York, NY, USA*

51. Giaccardi, E (2011) Things We Value, Interactions 18(1), p17-21

52. Gibson, J.J. (1979) *The Ecological Approach to Visual Perception*, Houghton Mifflin, Boston

53. Gillespie, T (2012) The Relevance of Algorithms. In Gillespie, T. et al. *Media Technologies*, MIT Press, Cambridge, MA at http://culturedigitally.org/2012/11/the-relevance-of-algorithms/

54. Gillespie, T and Seaver, N. (2016) Critical Algorithm Studies: A Reading List at https://socialmediacollective.org/reading-lists/critical-algorithm-studies/#0.5

55. Glenn, J. and Walker, R. (2012) *Significant Objects: 100 Extraordinary Stories About Ordinary Things*. Fantagraphics: Seattle, USA

56. 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.

57. Harper R. (Ed) (2003) *Inside the Smart Home* Springer, Verlag,

58. Hood, C. & Margetts, H.Z. (2007) *The Tools of Government in the Digital Age* Palgrave MacMillan, New York

59. Horn, M. et al "Kids and Thermostats: Understanding Children's Involvement with Household Energy Systems" (2015) *Int Journal of Child-Computer Interaction* In Press

60. Huawei Website, (2016) Global Connectivity Index 2016

61. Hutchins, E. (1995) *Cognition in the Wild*, MIT Press, Cambridge

62. International Telecommunications Union (2012) Overview of the Internet of Things, Rec ITU Y.2060 (06/2012)

63. Jaap Koops, B. (2006) *Starting Points for IT Regulation: Vol 9 – Deconstructing Prevalent Policy One Liners*, Asser Press, The Hague

64. Jondet, N. (2006) La France v Apple: Who's the Dadvsi in DRMs, *SCRIPTed* 3(4), 473

65. Kitchin, R (2016) Thinking about and Critically Researching Algorithms, *Information, Communications and Society* 1-16, at http://dx.doi.org/10.1080/1369118X.2016.1154087

66. Leenes, R. (2011) Framing Techno-Regulation: An Exploration of State and Non-State Regulation by Technology, *Legisprudence* 5(2) 143-169

67. Lessig, L. (2006) *Code Version 2.0* Basic Books, New York

68. Luhmann, N (1996) *Social Systems*, (Translated by Bednarz, J and Baecker, D) Stanford University Press, Stanford

69. Luger, E., Urquhart, L., Rodden. T., Golembewski, M. (2015) Playing the Legal Card: Using Ideation Cards to Raise Data Protection Issues within the Design Process, *Proceedings of ACM SIGCHI 2015*, p457-466.

70. Luger E., Moran, S and Rodden, T. (2013) Consent for All: Revealing the Hidden Complexity of Terms and Conditions, *CHI '13*

71. Luger, E. and Rodden, T, (2013) An Informed View on Consent for Ubicomp, *Ubicomp '13*

72. Mäkinen, L (2016) Surveillance On/Off: Examining Home Surveillance Systems From The User's Perspective, *Surveillance & Society* 14(1): 59-77

73. Marsden, C. (2011) *Internet Co-Regulation: European Law, Regulatory Governance and Legitimacy in Cyberspace*, Cambridge University Press, Cambridge, UK.

74. Marsden, C. and Brown, I. (2013) *Regulating Code* MIT Press, Cambridge MA

75. Mingers (1995) Self Producing Systems: Implications and Applications of Autopoeisis, Contemporary Systems Thinking, Plenum, New York

76. Mayer-Schonberger, V. (2009) *Delete: The Virtue of Forgetting in the Digital Age*, Princeton University Press: New Jersey, US

77. 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/

78. Meese, R. et al (2013) From codes to patterns: designing interactive decoration for tableware. *In Proceedings SIGCHI Conference Human Factors in Computer Systems (CHI,13) ACM Press, New York, NY, USA*

79. Moreau, L. and Missier, P. *PROV-DM: The PROV Data Model.* 2012

80. Murray, A. (2006) The Regulation of Cyberspace: Control in the Online Environment, (Routledge Cavendish, Abingdon

81. Nissenbaum, H. (2005) Values in Technical Design in Mitcham, C *Encyclopaedia of Science, Technology and Ethics*, MacMillan, New York

82. Norman, D. (1988) *The Psychology of Everyday Things, Basic Books, New York, USA*

83. Norman, D. (2013) The Design of Everyday Things: Revised and Expanded Edition, MIT Press, Cambridge, MA, USA

84. Oulasvirta, A. et al (2012) Long-term Effects of Ubiquitous Surveillance in the Home, *Ubicomp 2012*

85. Parris, R (2012) Online Ts&Cs Longer Than Shakespeare Plays – Who Reads Them? *Which?* 23 March 2012

86. Reidenberg, J. (1998) Lex Informatica: The Formulation of Policy Rules through Technology, *Texas Law Review*, 76, 553

87. 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*

88. Rose et al (2015) *Internet of Things: An Overview*, Internet Society

89. Rosner, G (2016) In the age of connected devices, will our privacy regulations be good enough? *O'Reilly* 1 Feb 2016

90. Satyanarayanan, M (2001) Pervasive Computing: Visions and Challenges, *IEEE Personal Communications*

91. Selznick, P. (1985) Focusing Organizational Research on Regulation In Noll, R.G. (1985) *Regulatory Policy and the Social Science,* University of California, Berkeley,

92. Shneiderman, B. (2012) Universal usability, *Communications of the ACM* 43(5), 84-91.

93. Smithers, R. (2011) Terms and Conditions: Not Reading Small Print Can Mean Big Problems, *The Guardian*, 11 May 2011

94. Speed, C. et al (2013) An Internet of Cars, *45th Annual UTSG Conference*, Oxford, UK

95. Sterling, B. (2005) *Shaping Things*, MIT Press: Cambridge, MA

96. Suchman, L. (1987) *Plans and Situated Actions: The Problem of Human-Machine Communication,* Cambridge University Press, New York

97. Sunstein, C. and Thaler, R. (2012) *Nudge: Improving Decisions About Health, Wealth and Happiness*, Penguin

98. Tene, O and Polonetsky, (2013) Big Data for All: Privacy and User Control in the Age of Analytics, *Northwestern Journal of Technology and Intellectual Property* 11. 239

99. Tolmie, P. et al (2002) Unremarkable Computing, *CHI '02*

100. Tolmie, P. et al (2003) Towards the Unremarkable Computer: Making Technology at Home in Domestic Routine in R. Harper (2003) *Inside the Smart Home,* Springer, Verlag,

101. 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

102. Urquhart L (2013) The Persistence of Memory Towards the Synchronic Society, *Gikii '13*

103. Urquhart, L. and Rodden, T. (2016) "A Legal Turn in Human Computer Interaction? Towards 'Regulation by Design' for the Internet of Things" Forthcoming, *SSRN Working Paper* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2746467

104. Urquhart, L (2016) *Towards User Centric Regulation: Exploring the Interface Between IT Law and HCI*, PhD Thesis, University of Nottingham

105. Vanhemert, (2014) Needy robotic toaster sells itself if neglected*, Wired.com*, 18 March 2014. at http://www.wired.co.uk/article/addicted-toaster

106. 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

107. Yang, R. et al (2014) Making Sustainability Sustainable: Challenges in the Design of Eco-Interaction Technologies *CHI '14* 823-832

108. Yang, R. and Newman, M. (2013) Learning from a Learning Thermostat: Lessons for Intelligent Systems for the Home, *Ubicomp '13*

109. Walport M (2014) *Internet of Things: Making the Most of the Second Digital Revolution,* UK Government Office of Science

110. Weiser, M. (1993) Some Computer Science Issues in Ubiquitous Computing in *Communications of the ACM* 36(7), 75-84.

111. Weiser, M., & Brown, J.S. (1997) The Coming Age of Calm Technology In Denning, PJ and Metcalfe, R.M (1997) *Beyond Calculation,* Copernicus