New directions in information technology law: learning from human–computer interaction

Lachlan Urquhart and Tom Rodden

Horizon Digital Economy Research Institute, University of Nottingham, Nottingham, UK

ABSTRACT
Effectively regulating the domestic Internet of Things (IoT) requires a turn to technology design. However, the role of designers as regulators still needs to be situated. By drawing on a specific domain of technology design, human–computer interaction (HCI), we unpack what an HCI-led approach can offer IT law. By reframing the three prominent design concepts of provenance, affordances and trajectories, we offer new perspectives on the regulatory challenges of the domestic IoT. Our HCI concepts orientate us towards the social context of technology. We argue that novel regulatory strategies can emerge through a better understanding of the relationships and interactions between designers, end users and technology. Accordingly, closer future alignment of IT law and HCI approaches is necessary for effective regulation of emerging technologies.

ARTICLE HISTORY
Received 6 January 2017
Accepted 19 January 2017

KEYWORDS
Human–computer interaction; technology regulation; Internet of Things

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 information technology (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. We need deeper understanding of their epistemological positions to better situate their role within technology regulation. Accordingly, we turn to a specific domain of design, human–computer interaction (HCI), and three prominent concepts from this community. We present these ideas to reframe regulatory challenges of domestic IoT and to show what HCI designers can offer as regulators. This process highlights 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 frequently questioned in technology regulation, from strategies for ensuring consumer rights to meeting compliance requirements with data protection law. We argue for a deeper understanding of how technologies impact...
rights of users and how designers can respond effectively requires a turn to the context of use. 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. In contrast, the user centric focus of HCI can offer valuable perspectives on designing effective regulatory strategies.

To understand what an HCI-led approach can offer IT law, we reframe three prominent design concepts for a technology regulation context: provenance, affordances (Norman 2013) and trajectories (Benford et al. 2009). Firstly, we look at the growing emphasis in HCI on retaining provenance of domestic IoT objects. This concept provides new perspectives on how to balance the right to be forgotten (RTBF) with other interests. By considering the histories and stories of objects alongside the legal rights of end users in their personal data, more nuanced discussions can emerge. Secondly, we consider the connected concepts of affordances, signifiers and mental models (Norman 2013). These help us structure thinking around how user interactions with technologies are designed, particularly in the way design shapes and mediates user behaviour. Affordances can inform thinking about designing regulatory interventions by highlighting the importance of looking beyond the technological artefact, to the setting, relationships and interactions users have with systems in context. Regulating domestic IoT, for example, requires engaging with the home: a heterogeneous, sensitive, socially contested domain composed of local routines, hierarchies and complex relationships between members. Lastly, we consider the regulatory challenges in obtaining informed user consent with the IoT. We propose new mechanisms to doing this through trajectories (Benford et al. 2009), a framework 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 repurposing them for a technology law and regulation audience. To understand why we are doing this we firstly need to outline the various premises of this paper.

Firstly, we believe effective regulation of and by 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 embed regulatory norms within a technical architecture to shape end-user behaviour (Brownsword 2004). Good examples include privacy by design (Cavoukian 2011; Danezis 2014) situational crime prevention (Von Hirsch, Garland, and Wakefield 2004) or digital rights management (Jondet 2006). 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 is the proximity of HCI designers to users. Their focus on understanding contexts of technology use involve reflecting the interests and environment of end users, with the goal of designing better systems. Designing user interfaces and experiences that meet the expectations and needs of end users is a key part of this (Shneiderman 2000). However, HCI is broader
than usability heuristics and metrics. It has been undergoing a shift from functional concerns like interface efficiency and optimisation towards more cultural, emotional and ethical dimensions of computing Bødker (2006, 1–2, 2016). 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 ethnomet hodology from sociology and anthropology (Garfinkel 1967; Crabtree, Rouncefield, and Tolmie 2012). Greater interaction between the law and HCI communities is necessary and elsewhere we have proposed routes to doing this, particularly the concept of ‘user centric regulation’ (Urquhart 2016; Urquhart and Rodden 2016). In this paper, we focus on unpacking concepts from HCI to reframe legal discussions and situate the role of designers in regulation.

Thirdly, we contend the definition of regulation has sufficiently broadened to accommodate a view of HCI designers as regulators. Selznick’s (1985) more traditional, state centric view of regulation can be contrasted with Black, who foregrounds the role of non-state actors (Black 2002, 26). Further widening regulation, Baldwin and Cave (1999) assert it incorporates different types of control ‘all forms of social control, state and non-state, intended and non-intended’ (91). Similarly, Jaap Koops (2006) frames the purposes widely as ‘controlling human or societal behaviour by rules or restrictions’ (81).

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. The state retains a key role in regulation due to legitimacy and authority (Leenes 2011; Hood and Margetts 2007). Within the ‘post regulatory state’ where there is a ‘hollowing out of the state’ through the growth of ‘decentred regulation’ (Black 2001, 106–122). In the context of IT 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, 58). Government encourages hybrid regulation between state and non-state actors in both self-regulation and co-regulation (Marsden 2011; Marsden and Brown 2013), and increasingly we see ‘regulation in many rooms’ (Black 2007, 63). 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 here are drawn from our experience and respective understanding of both communities. A common epistemological toolbox between HCI and IT law is necessary to navigate new notions of regulation. This starts by engaging with respective community mind-sets and we briefly sketch a picture here.

HCI is a broad field incorporating quantitative, statistically orientated practices, for example, evaluating usability of interfaces by tracking performance of a user interacting with a novel computer interface, to more qualitative approaches like designing new user experiences for interacting with creative or cultural artefacts. On the more qualitative side, HCI practice prioritises developing situated understandings of how users interact with systems in practice. (Suchman 1987). Participatory methods play a key role here, incorporating user interests and reflecting the social context of the technology (Bjerknes and Bratteteig 1995; Ehn and Kyng 1987; Floyd et al. 1989; Bansler 1989).
We argue that regulation of technology needs to shift towards understanding users’ interactions and experiences with technology. Current models of technology regulation rely on abstracted models of the user, either as ‘pathetic dots’ being acted on by modalities of law, market, norms or code (Lessig 2006) or as ‘nodes’ interacting within a networked community (Murray 2006). These theories have been invaluable in the development of IT law generally, but we argued that closer alignment with HCI requires a turn to practice in IT law (Urquhart 2016; Urquhart and Rodden 2016). Regulatory interventions need to engage with and draw on users lived experiences, interactions and relationships with technologies.

HCI designers are well placed to engage with the needs, values, practices and expectations of users from IT in context. Design ethnographies, for example, are used to investigate the social context of technology design, build a rich, situated picture of actors, their relationships and practices therein (Crabtree, Rouncefield, and Tolmie 2012). These could be repurposed to reflect on regulatory dimensions in design too. Similarly, value sensitive design frameworks that integrate interests and values of users into system design (Friedman, Kahn, and Borning 2008; Nissenbaum 2005) can be extended to legal values (Urquhart and Rodden 2016). Methods for adapting these tools to regulatory ends go beyond the conceptual scope of this paper, although as an example, design tools like privacy idea- tion cards exist to support HCI designers doing privacy by design in practice (Luger et al. 2015).

Situating the conceptual and practical role of designers in regulation needs greater attention. By presenting key concepts with traction within the HCI community here, we offer an entry point to engaging with the epistemological commitments from HCI, to help both communities move forward together.

We now briefly situate our analysis in the context of this special issue on algorithms. The analysis does not focus on algorithms in the abstract, but on socio-technical dimensions of domestic IOT 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 IoT

Algorithms have prompted much discussion 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 (2012) 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’ (1). 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’ (1). Whilst there is concern around the social impacts of algorithms, there is a risk of weaving a deterministic narrative about their role. Barocas, Hood, and Ziewitz (2013) capture this well, stating: ‘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”?’ (3)
Accordingly, we focus on the socio-technical context of the algorithms, namely the home in domestic IoT, following Kitchin’s (2016) assertion that assessing the wider assemblage around a technology is critical, that is, ‘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 … [framed by] forms of knowledge, legalities, governmentalities, institutions, marketplaces, finance … ’ (12)

The focus should be on how algorithms instantiated within IoT technologies mediate the practices and behaviours of users. Emphasis needs to be on how algorithms function 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. IoT devices are socially embedded technical artefacts. They use algorithmic approaches to automate 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; Gartner Hype Cycle for Emerging Technologies 2015). Various technology and consultancy firms predict vast numbers of internet connected devices over the coming years, from Cisco at 24 billion 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 and Marzano 2003); pervasive computing (Satyanarayanan 2001), ubicomp (Caceres and Friday 2012; Weiser 1993), calm computing (Weiser and 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, Eldridge, and Chapin 2015, 8). Unlike ubicomp or ambient intelligence, there is no overarching canonical vision of IoT and defining the parameters of what is or is not IoT may not be necessary (McAuley 2016). Nevertheless, it can be descriptively useful to appreciate what different organisations understand by the term IoT. Following assessment of literature from a range of different stakeholders including UK Government Office for Science (Walport 2014, 13); EU Article 29 Working Party (A29 WP 2014, s1.3); UN International Telecoms Union (2012, 1); Cisco (2013, 1); IETF (Arkko, Thaler, and McPherson 2015, 1) and Cambridge Public Policy (Deakin 2015, 8), 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, for example, 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 too like the smart built environment, healthcare, wearables and intelligent mobility. We focus in this paper on the domestic setting, considering objects in the home and the domestic IOT (e.g. home automation of energy, security or lighting management).

We now briefly set the scene of overarching regulatory dimensions of IoT in the home. This is to better situate the context aligned HCI/IT law user centric regulatory approaches need to address. 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 (25). 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/A29 WP 2014, 6). 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’ (15).

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, 6; Rose, Eldridge, and Chapin 2015, 26–29). Indeed, there is significant user apprehension over control of personal data in Europe. A 2015 survey of 28,000 EU citizens on attitudes to personal data protection shows 66% are ‘concerned about not having complete control over the information they provide online’ (European Commission 2015, 6). 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, 58). New rights in the General Data Protection Regulation (GDPR 2016), like the RTBF or right to data portability, seek to address concerns by increasing user control over their personal data. We now turn to first HCI concept, object provenance, reflecting on how it reframes discussions on balancing the RTBF against other interests.

**Object provenance and the RTBF**

We now outline 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 of balancing between interests, and what the concept of object provenance adds to these discussions.

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, approaches to creating provenance from information management or archiving through creation of cultural objects with digital stories and histories are emerging.
For information management, provenance can be as simple as tracking and recording the changes made to 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 and changes around 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 Ministry of Provenance (MoP) 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, 245)

For object-based archiving, we see emphasis on tracking the provenance of physical objects, often digitally. Giaccardi (2011) highlights new technologies, like IoT, as enabling new forms of remembering and cultural heritage. Digital footprints can be curated across different, non-traditional forums. Similarly, Speed et al. (2013) tackle the idea by creating a social network between objects, namely cars, where photos and stories of travels of occupants are shared with other cars on the motorway. An 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, Li, and Wattenhofer 2013) 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, we have a range of interesting examples. Firstly, playfully, art project ‘Brad the Toaster’ plays with agency of objects where toaster who ‘feels’ neglected (i.e. not being used to make toast regularly enough) can put himself up onto eBay to find a new owner to use them more (Vanhemert 2014). With this object goes the story of negligence at the hands of the previous owners. Secondly, Darzentas et al. (2015) have been looking at Warhammer 40 K, understanding the community of players, the processes of creation, play and curation around war-gaming miniatures. They look at how to digitally augment their footprints whilst not disrupting core practices of the game or the community. Importantly, as IoT progresses Darzentas et al. (2016) argue ‘… 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’ (2).

Lastly, the Carolan Guitar project is a travelling guitar adorned with a range of machine readable codes called Artcodes (Meese et al. 2013). Whilst aesthetically pleasing, the codes
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’, that is, ‘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’ (1168) 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. This work highlights the shift towards objects having their own stories to tell, beyond the interests of individual users. 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.

Record keeping enabled by the digital age is not always viewed favourably. Scholars like Mayer-Schonberger (2009) and Dodge and Kitchin (2007) 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’ (92). 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’ (124).

Similarly, Dodge and Kitchin (2007) argue that forgetting is so important in the digital age that ethically different forms of forgetting should be built into systems where ‘… algorithmic strategies … such as erasing, blurring, aggregating, injecting noise, data perturbing, masking … ’ (442). Mayer-Schonberger (2009) proposes users should set a timeframe for data expiration dates to prompt reflection on the lifespan of their information (173). 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 RTBF might give mandate to such approaches. The RTBF 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, but there has been extensive discussion around both (Ausloos and Kuczerawy 2016; 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 public in freedom of information (Edwards 2016b). In essence the GDPR states that data subjects have a right to personal data deletion without delay given certain conditions (Art 17(1), GDPR). 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. The RTBF is particularly important for adults seeking to remove information about their actions, on social media for example, that were carried when they were children.³ 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 a range of safeguards for individuals’ rights and freedoms are necessary (Article 89(1)).
amounts to putting technical or organisational processes in place to ensure data minimisation, perhaps pseudonymisation too. Interestingly, following a deletion request where data has been made public, controllers, (subject to limits of cost, technology, etc.) still need to take reasonable steps to pass this request on (Article 17(2), GDPR). These rights do not extend to the deceased.

Establishing who is responsible for ensuring protection of these legal rights, that is, 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 object provenance. It is not the polarised extremes of absolute privacy vs absolute censorship, but sits somewhere in the middle. In any case, wherever the balance is pitched, the two communities, HCI and law, need to come together and think about practicalities of how to implement it.

On that point, privacy by design has much to offer here, but binaries of delete/not delete may be too blunt in the future. The absolute of complete deletion on a RTBF request may be prudent in some cases, but not in others. 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. Lawyers may help navigate if 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 occurs with social media profiles? What are reasonable steps are necessary to manage public vs private information in objects and how can designers and lawyers come together to create technically feasible solutions? Input from the users and communities around digital memories of objects is important. HCI approaches can provide insight into the practices and relationships with objects, and in turn this can better inform the balancing exercise necessary for the RTBF. We now turn to the second concept, affordances, and their role in designing interactions with technologies.

**Affordances, signifiers and mental models**

With affordances, designers are creating a device or object offering possibilities for action by the user but 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. We argue that within the setting of the home a greater awareness of the social context of users can help formation of more effective regulation through design.

Norman’s *The Design of Everyday Things* (Norman 2013) helps us think about how user interactions with technologies are designed. We briefly reflect on three of his core ideas: *affordances, signifiers and mental models*. His overall focus is on how to achieve ‘good design’ by putting end users at the ‘centre’ of interest, and actively involving them in the iterative development of a product or system (Norman 2013, 9–10). For Norman, if a user cannot use a product, that is the fault of the designer for ineffectively communicating with them or not understanding their needs (Norman 2013, 8).

One of the key concepts for understanding the relationship between user and technology is the notion of *affordances*. 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 …’ (Norman 2013, 11). Affordances are very much an interactive relationship (Gaver 1991) and require us to look beyond just the technology or user towards the *interactions* between the two.

In shaping this relationship, *signifiers* are key to ensuring effective communication between designers and users. They indicate that a technology can be used in a particular manner, for example, a handle on a cup enabling it to be picked up. Signifiers can vary greatly depending on the technology, but broadly they are any mechanism that communicates the nature of the affordance from the designer to the end user (Norman 2013, 14). Another element to consider is how users interpret the signifier will depend upon their own circumstances and understanding of the technology. Accordingly, *mental models*, that is, ‘the conceptual models in people’s minds that represent their understanding of how things work’ (Norman 2013, 26) are key. As different users may possess different models of what a technology does and designers cannot speak directly to them, 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, 26). Whilst designers have some control over how these models are formed, often the user obtains their understanding from a range of different sources from discussions with peers to manuals or experience (Norman 2013, 26).

Bringing these design elements together, we have a richer understanding of how relationships between designer and user are constructed. Furthermore, it helps us to understand how designers can provide or prevent end users exercising control, for example with IoT. These same concepts could help think about how end-user rights are factored into their interactions with technologies. How might we design affordances and signifiers to provide increased control over personal data and enable a positive relationship between users, technology and their information.

Alongside these elements, the setting is a key consideration in building relationships between users and technology. For regulating domestic IoT, HCI has long considered design challenges of the home. The home will not become ‘smart’ overnight (Edwards and Grinter 2001, 257) and how technologies are embedded into the home will vary because ‘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’ (Rodden and Benford 2003, 11). For designers, homes are complex social spaces where different practices and routines persist (Crabtree and Rodden 2004). As Tolmie et al. (2002) has said ‘routines are the very glue of everyday life … Routines help provide grounds whereby the business of home life gets done.’ (185) and technology needs to engage with domestic routines, as underlying practices of the setting, whilst not disrupting them (Tolmie et al. 2003).

When considering how to regulate IoT effectively, considering how users interact with these systems in context is important. A range of studies from HCI and beyond have looked at this. Mäkinen (2016) studies home surveillance systems7 in Finland finding internal tensions for 13 residents around trade-offs, like benefits of safety and home protection against fear of unpermitted watching or perceived spying on others (75). Similarly, Ur, Jung, and Schechter (2014) US study of 13 teens and 11 parents showed broad support for smart home security like connected locks due to remote control, improved safety and convenience (129). However, erosion of trust between teens and parents also resulted due to increased monitoring, with teens forming resistance strategies in response (135). Choe et al.’s (2011) US smart home study8 of 22 participants cited benefits like health and safety (e.g. keeping an eye on elderly relatives) or saving money (e.g. watching which appliances use too much electricity (65). Concerns about sensitive, private activities of the home being captured (being used against them by other members of the home, e.g. in a divorce) and being hacked/leaked externally (Choe et al.2011, 66). 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 and changed behaviour to ‘regulate what the surveillers perceived’. Interestingly, over the six months they ‘showed no negative effects on stress and mental health attributable to surveillance’ (49).

Accordingly, domestic IoT technologies impact different users in different ways and regulatory strategies need to engage nuances of these perspectives. We need to look beyond the artefacts and intended uses to the different relationships they create in practice. With home security systems, for example, benefits like safety and protection need to be balanced against adverse impacts on family dynamics or risks of unauthorised access to data. User accounts help unpack the situated social dynamics of technology, informing the landscape regulatory strategies need to function within. Heterogeneous devices with different affordances, signifiers used by users with varying mental models complicate the landscape for managing legal rights in the home. Ensuring adequate control over personal data is difficult if users do not understand how a system collects information. Nevertheless, considering the relationships between technologies and users, and accounting for the settings and interactions between them gives us a richer picture of the landscape for designing effective regulatory approaches in context. We now turn to our final section.

**Trajectories and designing for consent**

In this final section, we turn to the concept of trajectories, mapping how they consent can be designed into domestic IoT devices. Benford et al.’s (2009) trajectories framework is a process for designing interactive user experiences, particularly in performative and cultural
settings, for example, theatrical performances, art installations or mixed reality games. Importantly, experiences go 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, 709).

The process of designing the trajectory of an experience involves considering 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. Tension can arise in differences 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 both these divergences and multiple trajectories, where many users are involved in the experience (Benford et al. 2009).

We believe trajectories can be reframed to incorporate regulatory and legal dimensions of the user experience. To unpack this further, we analyse challenges around obtaining end-user consent to data processing with IoT.

The dominant approach to obtaining user consent for data processing is form contracts. The contracts create a model of notice and choice, where the notice is the details of processing provided in the contract (e.g. 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 and conditions (T&C) often include clauses that are not favourable to end users, from arbitration clauses to handing over your firstborn or your soul to the service provider (Fox-Brewster 2014; Caddy 2013). Consumers are unlikely to read these T&C in any case hence they do not know what they are signing up to when using a service (Smithers 2011; Bakos, Marotta-Wurgler, and Trossen 2014). The recent example of Facebook manipulating users’ news feeds to provoke happy or sad emotions, whilst unethical, was arguably not illegal as Facebook’s T&C permitted such a practice for research purposes. 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, Moran, and Rodden (2013) browser plug in Literatin showed that to understand many of the most popular T&C 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 and 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 standard 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 ground 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),9 and when consent is the grounds for legal processing, it must be
explicit, although what that means in practice is not defined. For general consent (Article 4(11), GDPR 2016) the requirements are that:

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.

Accordingly, many aspire to creating alternative legal mechanisms to consent as regulatory challenges posed by technologies like 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’ (32) whereas Edwards (2016a) 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’ (34).

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 RTBF.

(1) Time – As it is embedded in the home, the relationship between the user and the IoT device is not transient. Accordingly, designers and lawyers can think longitudinally about how information is presented. As opposed to providing all information upfront and taking consent when hardware is unboxed (e.g. through shrink-wrap contracts) information can be spread over the lifetime of the user–device relationship. Requesting renewed consent, at appropriate time intervals, would also be pertinent. Reflecting on important milestones in the user–device relationship could guide this (e.g. when quarterly or even monthly bills are issued by an energy supplier).
(2) Actors – The goal of domestic IoT is not for all devices to sit in isolation, but to communicate and work together to provide value added services. Manufacturer platforms like Works with Nest link together multiple stakeholders via products and services from different manufacturers. Interests in the personal data will vary for actors across domestic IoT ecosystems. Accordingly, reflecting on third party data flows and highlighting these in the design of end-user experiences could foster increased transparency. Furthermore, the home may have visitors like distant family members, friends, plumbers and joiners. Considering their more transitory experiences with the system is important, as their legal rights are equally important. Designing mechanisms to inform, obtain and enable withdrawal of consent will require creative thinking from both lawyers and designers.

(3) Space – Homes involve complexities of social life, with associated domestic politics and tensions, for example, authority of different occupants to manage heating (Horn et al. 2015). How legal interests, like control of personal data, manifest within such spaces may be shaped by domestic hierarchies, for example, between teenagers and parents, older relatives, student flatmates (Yang and Newman 2013). Many IoT technologies seek to understand their context and environment to tailor their service. The Nest Thermostat builds a profile of room occupancy based on motion detection to create a tailored heating schedule that meets needs of the occupants. Some may want extra control over their footprint in the Nest schedule, hence how consent mechanisms are designed to enable their withdrawal is key. As the home will not become smart overnight, designers and lawyers will need to address how interactions and consent mechanisms may differ across heterogeneous devices that are replaced at different paces (e.g. old devices interacting with new).

(4) Interface – Computer interfaces can both limit and enable how information is communicated to end users. Different signifiers could be used to interact with users. Beeping noises could flag possible data sharing with third parties, flashing lights for collecting new types of data and even speech to advise of new information when reobtaining consent. Text-based approaches may be frustrated by screen size and device computational limitations. Function, aesthetics and costs will all need to be balanced. The interface may also afford different means of signifying consent from gestures like waving and pointing to provide consent, and beeps to notify users of logged consent. Different levels of user literacy (digital and traditional) may shape how (and what) information is presented. Collaboration between designers and lawyers could lead to more innovative and rewarding uses of IoT interfaces for obtaining consent.

As we see, by viewing user experiences with technologies in terms of trajectories, we can start to unpack how experiences intersect with legal considerations. We can create novel means of tackling regulatory challenges, such as addressing the legal fiction of informed consent from form contracts. We now offer some brief conclusions.

**Conclusions**

Regulation as a concept has broadened, both in motivation 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 IoT, 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 RTBF can be enriched by considering the concept of provenance. 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 RTBF.

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 contractual T&C. Our contribution proposes a route forward for changing how consent is obtained for the domestic IoT. 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 IT law. Importantly, we offer three overarching concepts and actively frame how they can be used to reconsider regulatory challenges, particularly referring to the domestic IoT. In the 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 towards how to build stronger links with HCI.

Notes

1. Regulation is ‘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’ (Selznick 1985, 363).

2. ‘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, 26).
3. Recital-65.
4. Recital-156.
5. Recital-158.
6. Update of Norman (1988).
7. Access control systems, for example, intruder sensors, cameras.
8. p62; Attitudes for in-home systems sensing and inferring through video, audio, electricity use.
9. Article 9(1) GDPR.

Funding
EPSRC Ubiquitous Computing for a Digital Economy EP/G037574/1 and EPSRC From Human Data to Personal Experience EP/M02315X/1.

Disclosure statement
No potential conflict of interest was reported by the authors.

References
Aarts, E., and S. Marzano. 2003. The New Everyday: Views on Ambient Intelligence. Rotterdam: 010 Publishers.
Arko, J., D. Thaler, and D. McPherson. 2015. IETF RC 7452: Architectural Considerations in Smart Object Networking. Fremont, CA: IETF.
Article 29 Working Party. 2014. Opinion 8/2014 on the Recent Developments on the Internet of Things WP 23. Brussels: European Commission.
Ashton, K. 2009. “That Internet of Things Thing.” RFID Journal 22: 97–114.
Ausloos, J., and A. Kuczerawy. 2016. “From Notice-and-Takedown to Notice-and-Delist: Implementing the Google Spain Ruling.” CTLJ 14: 219–258.
Bachour, K., R. Wetze, M. Flintham, T. D. Huynh, T. Rodden, and L. Moreau. 2015. “Provenance for the People: A User-Centered Look at the W3C PROV Standard through an Online Game.” Proceedings CHI ’15, 2437–2446.
Bakos, Y., F. Marotta-Wurgler, and D. Trossen. 2014. “Does Anyone Read the Fine Print? Consumer Attention to Standard Form Contracts.” JLS 43 (1): 1–35.
Baldwin, R., and M. Cave. 1999. Understanding Regulation: Theory Strategy and Practice. Oxford: OUP.
Bansler, J. 1989. “Systems Development Research in Scandinavia: Three Theoretical Schools.” SJIS 7 (1): 73–98.
Barocas, S., S. Hood, and M. Ziewitz. 2013. “Governing Algorithms: A Provocation Piece.” Governing Algorithms, NY, USA.
Barthel, R., K. Leder Mackley, A. Hudson-Smith, A. Karpovich, M. de Jode, and C. Speed. 2011. “An Internet of Old Things as an Augmented Memory System.” PUC 17 (2): 321–333.
Benford, S., G. Giannachi, B. Koleva, T. Rodden. 2009. “From Interaction to Trajectories, Designing Coherent Journeys through User Experiences.” Proceedings of CHI ’09, 709–718.
Benford, S., A. Hazzard, A. Chamberlain, K. Glover, C. Greenhalgh, L. Xu, M. Hoare, and D. Darzentas. 2016. “Accountable Artefacts: The Case of the Carolan Guitar.” Proceedings CHI ’16, 1163–1175.
Bernal, P.A. 2011. “A Right to Delete?” EJLT 2 (2). http://ejlt.org/issue/view/6.
Bjerknes, G., and T. Bratteteig. 1995. “User Participation and Democracy: A Discussion of Scandinavian Research on System Development.” SJIS 7 (1): 73–98.
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.
Black, J. 2002. “Critical Reflections on Regulation.” AJLP 27: 1–35.
Black, J. 2007. “Tensions in the Regulatory State.” Public Law (Spring): 58–73.

Bødker, S. 2006. “When Second Wave HCI Meets Third Wave Challenges.” Proceedings of NORDICHI ’06, 1–8.

Bødker, S. 2016. “Third Wave HCI, 10 Years Later – Participation and Sharing.” Interactions – September-October.

Brockmann, D., and F. Theis. 2008. “Money Circulation, Trackable Items, and the Emergence of Universal Human Mobility Patterns.” IEEE Pervasive Computing 7 (4): 28–35.

Brown, I. 2015. “GSR Discussion Paper: Regulation and the Internet of Things.” ITU, Geneva.

Brownsword, R. 2004. “What the World Needs Now: Techno-Regulation, Human Rights and Human Dignity.” In Human Rights: Global Governance and the Quest for Justice, edited by R. Brownsword, 203. Oxford: Hart. https://kclpure.kcl.ac.uk/portal/en/publications/what-the-world-needs-now-technoregulation-human-rights-and-human-dignity(3cc2cf53-bf1f-4a53-b6e9-ec7d72bb3a2c).html.

Caceres, R., and A. Friday. 2012. “ubicomp Systems at 20: Progress, Opportunities and Challenges.” IEEE Pervasive Computing 11 (1): 14–21.

Caddy, P. 2013. “Surrendering Your Immortal Soul: Does Anybody Ever Read Terms and Conditions?” LexisNexis Comet, September 19.

Cavoukian, A. 2011. 7 Foundational Principles of Privacy by Design. Ontario: Information and Privacy Commissioner of Ontario.

Choe, E.K., S. Consolvo, J. Jung, B. Harrison, and J. Kientz. 2011. “Living in a Glass House: A Survey of Private Moments in the Home.” Proceedings Ubicomp ’11.

Cisco. 2013. “The Internet of Everything.” http://www.cisco.com/c/dam/en_us/about/business-insights/docs/iee-value-at-stake-public-sector-analysis-faq.pdf.

Cisco Website. 2016. “Visual Networking Index.” http://www.cisco.com/c/en/us/solutions/service-provider/visual-networking-index-vni/index.html.

Crabtree, A., and T. Rodden. 2004. “Domestic Routines and Design for the Home.” CSCW 13 (2): 191–220.

Crabtree, A., M. Rouncefield, and P. Tolmie. 2012. Doing Design Ethnography. London: Springer Verlag.

Danezis, G., J. Domingo-Ferrer, M. Hansen, J.-H. Hoepman, D. Le Métayer, R. Tirtea, and S. Schifffner. 2014. Privacy and Data Protection by Design – From Policy to Engineering. Heraklion: ENISA.

Darzentas, D., M. Brown, M. Flintham, and S. Benford. 2015. “The Data Driven Lives of Wargaming Miniatures.” Proceedings CHI ’15, 2427–2436.

Darzentas, D., A. Hazzard, M. Brown, M. Flintham, and S. Benford. 2016. “Harnessing the Digital Records of Everyday Things.” Proceedings of DRS ’16.

Deakin, S., C. Sausman, B. Sones, and C. Twigg. 2015. The Internet of Things: Shaping Our Future. Cambridge: Cambridge Public Policy.

Dodge, M., and R. Kitchin. 2007. “Outlines of a World Coming into Existence: Pervasive Computing and the Ethics of Forgetting.” Environment and Planning B: Planning and Design 34 (3): 431–445.

Edwards, L. 2016a. “Privacy, Security and Data Protection in Smart Cities: A Critical EU Perspective.” EDPL 2 (1): 28–58.

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

Edwards, K., and B. Grinter. 2001. “At Home with Ubiquitous Computing: Seven Challenges.” Proceedings Ubicomp ’01, 256–272.

Ehn, P., and M. Kyng. 1987. “The Collective Resource Approach to System Design.” Computers and Democracy: A Scandinavian Challenge, edited by G. Bjerknes, P. Ehn, and M. Kyng, 17–58. Aldershot: Avebury.

Eidenbenz, R., Y. Li, and R. Wattenhofer. 2013. “Reading Up on Bookcrossing.” International Journal of the Book 10 (2): 11–26.

European Commission. 2015. “Special Eurobarometer 431 ‘Data Protection’.” http://ec.europa.eu/justice/newsroom/data-protection/news/240615_en.htm.

Floyd, C., W.-M. Mehl, F.-M. Resin, G. Schmidt, and G. Wolf. 1989. “Out of Scandinavia: Alternative Approaches to Software Design and System Development.” Human–Computer Interaction 4: 253–350.
Fox-Brewster, T. 2014. “Londoners Give Up Eldest Children in Public WiFi Security Horror Show.” The Guardian, September 29.

Friedman, B., P. Kahn, and A. Borning. 2008. “Value Sensitive Design and Information Systems.” In The Handbook of Information and Computer Ethics, edited by K. Himma and H. Tavani, 69–101. New York: Wiley.

Garfinkel, H. 1967. Studies in Ethnomethodology. Englewood Cliffs, NJ: Prentice Hall.

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

Gaver, B. 1991. “Technology Affordances.” Proceedings SIGCHI Conference Human Factors in Computer Systems (CHI, 91). New York, NY: ACM Press.

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. http://eur-lex.europa.eu/eli/reg/2016/679/oj.

Giaccardi, E. 2011. “Things We Value.” Interactions 18 (1): 17–21.

Gibson, J. J. 1979. The Ecological Approach to Visual Perception. Boston: Houghton Mifflin.

Gillespie, T., 2012. “The Relevance of Algorithms.” In Media Technologies, edited by Tarleton Gillespie, Pablo Boczkowski, and Kirsten Foot, 167–195. Cambridge, MA: MIT Press. https://www.scribd.com/document/292547806/The-Relevance-of-Algorithms-Tarleton-Gillespie.

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

Glenn, J., and R. Walker. 2012. Significant Objects: 100 Extraordinary Stories About Ordinary Things. Seattle, WA: Fantagraphics.

Google Spain. 2014. C-131/12.

Harper, R., ed. 2003. Inside the Smart Home. London: Springer-Verlag.

Hood, C., and H. Z. Margetts. 2007. The Tools of Government in the Digital Age. New York: Palgrave MacMillan.

Horn, M. S., Z. S. Leong, M. Greenberg, and R. Stevens. 2015. “Kids and Thermostats: Understanding Children’s Involvement with Household Energy Systems.” International Journal of Child-Computer Interaction 3–4: 14–22.

Huawei Website. 2016. Global Connectivity Index 2016.

Hutchins, E. 1995. Cognition in the Wild. Cambridge: MIT Press.

International Telecommunications Union. 2012. “Overview of the Internet of Things.” Rec ITU Y.2060.

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

Jondet, N. 2006. “La France v Apple: Who’s the Dadvis in DRMs.” SCRIPTed 3 (4): 473–484.

Kitchin, R. 2016. “Thinking About and Critically Researching Algorithms.” Information, Communications and Society 20: 1–16.

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

Lessig, L. 2006. Code Version 2.0. New York: Basic Books.

Luger, E., S. Moran, and T. Rodden. 2013. “Consent for All: Revealing the Hidden Complexity of Terms and Conditions.” Proceedings CHI ’13, 2687–2696.

Luger, E., and T. Rodden. 2013. “An Informed View on Consent for Ubicomp.” Proceedings Ubicomp ’13.

Luger, E., L. Urquhart, T. Rodden, and M. Golembewski. 2015. “Playing the Legal Card.” Proceedings CHI ’15, 457–466.

Mäkinen, L. 2016. “Surveillance On/Off: Examining Home Surveillance Systems from the User’s Perspective.” Surveillance & Society 14 (1): 59–77.

Marsden, C. 2011. Internet Co-Regulation: European Law, Regulatory Governance and Legitimacy in Cyberspace. Cambridge: CUP.

Marsden, C., and I. Brown. 2013. Regulating Code. Cambridge, MAMIT Press.
Mayer-Schonberger, V. 2009. *Delete: The Virtue of Forgetting in the Digital Age*. Princeton, NJ: Princeton University Press.

McAuley, D. 2016. *What is IoT? That is Not the Question*. IoT UK.

McDonald, A., and L. F. Cranor. 2008. “The Cost of Reading Privacy Policies.” *I/S A Journal of Law and Policy for the Information Society*.

Meese, R., S. Ali, E. Thorne, S. Benford, A. Quinn, R. Mortier, B. Koleva, T. Pridmore, and S. Baurley. 2013. “From Codes to Patterns: Designing interactive Decoration for Tableware.” *Proceedings CHI ’13*, 931–940.

Moreau, L., and P. Missier. 2012. *PROV-DM: The PROV Data Model*. W3C.

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

Nissenbaum, H. 2005. “Values in Technical Design.” In *Encyclopaedia of Science, Technology and Ethics*, edited by C. Mitcham, 66–70. New York: MacMillan.

Norman, D. 1988. *The Psychology of Everyday Things*. New York: Basic Books.

Norman, D. 2013. *The Design of Everyday Things: Revised and Expanded Edition*. Cambridge, MA: MIT Press.

Oulasvirta, A., et al. 2012. “Long-term Effects of Ubiquitous Surveillance in the Home.” *Proceedings Ubicomp ’12*.

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

Reidenberg, J. 1998. “Lex Informatica: The Formulation of Policy Rules through Technology.” *Texas Law Review* 76: 553–594.

Rodden, T., and S. Benford. 2003. “The Evolution of Buildings and Implications for the Design of Ubiquitous Domestic Environments.” *Proceedings CHI ’03*, 9–16.

Rogers, Y. 2005. “New Theoretical Approaches for Human Computer Interaction.” *Annual Review of Information Science and Technology* 38 (1): 87–143.

Rose, K., S. Eldridge, and L. Chapin. 2015. *Internet of Things: An Overview*. Internet Society.

Rosner, G. 2016. “In the Age of Connected Devices, Will Our Privacy Regulations Be Good Enough?” *O’Reilly*, February 1.

Selznick, P. 1985. “Focusing Organizational Research on Regulation.” In *Regulatory Policy and the Social Science*, edited by R. G. Noll, 363–364. Berkeley: University of California.

Shneiderman, B. 2000. “Universal Usability.” *Communications of the ACM* 43 (5): 84–91.

Smithers, R. 2011. “Terms and Conditions: Not Reading Small Print Can Mean Big Problems.” *The Guardian*, 11/05/11.

Speed, C., D. Shingleton, S. Box, T. Cherrett, J. Dickinson, N. Davies, and S. Norgate. 2013. “An Internet of Cars.” *45th Annual UTSG Conference*, Oxford, UK.

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

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

Tene, O., and J. Polonetsky. 2013. “Big Data for All: Privacy and User Control in the Age of Analytics.” *NITIP* 11. 239–272.

Tolmie, P., J. Pycock, T. Diggins, A. MacLean, and A. Karsenty. 2002. “Unremarkable Computing.” *Proceedings CHI ’02*.

Tolmie, P., J. Pycock, T. Diggins, A. MacLean, and A. Karsenty. 2003. “Towards the Unremarkable Computer: Making Technology at Home in Domestic Routine.” In *Inside the Smart Home*, edited by R. Harper, 183–206. London: Springer-Verlag.

Ur, B., J. Jung, and S. Schechter. 2014. “Intruders Versus Intrusiveness: Teens’ and Parents’ Perspectives on Home-Entryway Surveillance.” *Proceedings Ubicomp ’14*, 129–139.

Urquhart, L. 2013. “The Persistence of Memory towards the Synchronic Society.” *Gikii* ’13.

Urquhart, L. 2016. “Towards User Centric Regulation: Exploring the Interface Between IT Law and HCI.” PhD thesis, University of Nottingham.

Urquhart, L., and T. Rodden. 2016. “A Legal Turn in Human Computer Interaction?” SSRN. *http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2746467*. 

---

L. URQUHART AND T. RODDEN
Vanhemert. 2014. “Needy Robotic Toaster Sells Itself If Neglected.” Wired.com, 18/03/14 http://www.wired.co.uk/article/addicted-toaster.

Von Hirsch, A., D. Garland, and A. Wakefield. 2004. Ethical and Social Perspectives on Situational Crime Prevention. Oxford: Hart. http://www.hartpub.co.uk/BookDetails.aspx?ISBN=9781841135533.

Walport, M. 2014. Internet of Things: Making the Most of the Second Digital Revolution. London: UK Government Office of Science.

Weiser, M. 1993. “Some Computer Science Issues in Ubiquitous Computing.” Communications of the ACM 36 (7): 75–84.

Weiser, M., and J. S. Brown. 1997. “The Coming Age of Calm Technology.” In Beyond Calculation, edited by Denning, and Metcalfe, 75–85. New York: Copernicus.

Winner, L. 1980. “Do Artifacts Have Politics?” Daedalus 109 (1): 121–136.

Yang, R., and M. Newman. 2013. “Learning from a Learning Thermostat: Lessons for Intelligent Systems for the Home.” Proceedings Ubicomp ‘13.