Bridging the Gap Between Law & HCI: Designing Effective Regulation of Human Autonomy in Everyday Ubicomp Systems

Lachlan Urquhart

Mixed Reality Lab & Horizon

University of Nottingham, Jubilee

Campus, Nottingham, UK,

NG8 1BB

lachlan.urquhart@gmail.com

Abstract

Ubicomp technologies pose challenges to human agency, and legal rights reliant on individual autonomy, for example informed consent to data processing. Existing regulatory measures designed to address these issues are working less adequately, and increased dialogue between design and law communities is necessary to decide how best to ensure effective regulation of human autonomy. This thesis seeks to understand the various regulatory issues posed by ubicomp technologies, through specific case studies, with the overall aim of creating legal and technological solutions that work in practice.

Author Keywords

Privacy; Regulation; Law; Policy; Design

ACM Classification Keywords

K.4.1 Public Policy Issues (Regulation)

Introduction

Broadly, Ubicomp research largely seeks to create contextually aware, 'invisible' technology operating in the background, seamlessly monitoring human behaviour and using embedded sensing devices to

engage, observe and respond to various stimuli in a range of routine, everyday practices. These processes pose fundamental challenges to human agency and many established legal principles reliant on notions of human autonomy & individual control over individual affairs. These concerns are particularly pronounced in the realm of privacy law and governance, for example. With ubicomp, regulators and businesses are posed with questions around regulating user trust in autonomous decision making infrastructures, ensuring legally valid consent is obtained from users and ensuring adequate control over use, collection, & sharing of human data. Already a number of law & policy measures are attempting to tackle these issues, through mechanisms like privacy impact assessments, privacy/ethics by design frameworks, and wholesale reform of EU Data Protection in the proposed General Data Protection Reform package. However, the efficacy of these approaches is often challenged by lack of implementable guidelines and solutions. This Ph.D seeks to address this by narrowing the gap between the design and law communities involved in creation and regulation of ubicomp systems, respectively. It will broadly increase capacity for co-operation between the communities by creating legally informed solutions that are grounded in real life design perspectives, and which ensure adequate legal protection of autonomy within ubicomp systems.

The thesis is considering examples of everyday ubicomp technologies situated in their real life context to understand what regulatory issues they pose, particularly from a legal perspective. Bridging the gap between these two communities by translating legal concepts and approaches for design that assists effective regulation is essential. A fundamental tension

for law and ethics posed by ubicomp is that individual rights are predicated on exercising human autonomy, yet ubicomp systems are becoming increasingly autonomous, less visible to the user, and have increased levels of agency [2,9,10]. The individual's reliance on fundamental rights and legal concepts such as the reasonable expectation to privacy or contractual responsibility for harm are challenged by such systems. This Ph.D research will understand issues highlighted by emerging ubicomp technologies, through grounded case studies of specific ubicomp system artefacts. This will allow the author to design regulatory solutions for a toolbox of approaches that address concerns around trust, consent, and autonomy much earlier in the system design and innovation process. This will draw on and incorporate legal perspectives into pre-existing frameworks, such as those on responsible innovation in ICTs [11], value sensitive design [4] and Privacy by Design [3].

In terms of background, Rouvray has highlighted that the law needs to balance enabling individual autonomy and agency against the benefit of these new technologies [9]. Cas has gone further, stating "*ubiquitous computing will erode all central pillars of current privacy protectio*n" and finding the tools that reconcile the benefits of ubicomp with the risks to privacy governance will continue to be a complex task [2]. Spiekermann and Pallas have questioned the automatic nature of machine responses using non-negotiable binary rules and the impact of automatic compliance that limits the autonomy of the human subject [10]. The thesis is also exploring challenges of obtaining legally valid consent and compliance with legal concepts of agency in ubicomp systems, building

on perspectives of Luger & Rodden [7], Camp & Connelly [1] and Langheinrich [6].

With autonomy, law plays a key role in protecting the ability of citizens to rely on their human agency and control/protect their own interests. This can be seen with human rights like Article 8 of the European Convention on Human Rights (which puts limitations and obligations on the state to protect the Right to Private and Family Life); contract law (where the state regulates rights and responsibilities of private actors) and consumer protection law (state protecting private actors). A key issues is that when law regulates technologies, it often provides ex poste solutions (i.e. after the fact), and instead a more proactive a priori approach where solutions are incorporated further up design chain is preferable. This is especially pronounced with ambient ubicomp systems because they have many attributes that are problematic from an ex poste regulatory perspective. They are intimate, due to being embedded in our daily routine; designed to be "unremarkable" & "invisible in use" [12]; reliant on human data to provide contextually appropriate services; and are obtaining progressively higher levels of agency. The relationship between individual user and technology becomes difficult to navigate, especially in the normalised, everyday life context. The dynamic relationships of agency that ubicomp technologies facilitate often prevent legal clarity for the risks.

Consequently, the original contribution of this research will be to:

- Understand how users negotiate ambient technologies in different everyday contexts, the perceived impacts on their autonomy, and how legal protections might address issues raised?

- Translate broad, abstract legal concepts, policy and guidelines into accessible tools that can assist ubicomp system design on a real life, practical level.

- Design socio-technical solutions that ensure effective regulation of autonomy in everyday, ubiquitous computing systems.

Current Work & Methodological Approach
Even the most ordinary, everyday technologies can give rise to a large range of legal, social and public policy problems. Framing the first part of the Ph.D discussion is an analysis of the NEST learning thermostat system. This device replaces a conventional thermostat in the home, and monitors the behaviour of occupants to learn and manage energy use in their environment. The sources for this analysis include empirical work from a longitudinal study conducted in the US, user concerns detailed in online forums, self designed storyboards and analysis of the various NEST legal contracts. The storyboards were created using insights from the longitudinal study and other users concerns, and helped to situate the technology in homes of fictitious characters, where different scenarios unfold and surface a range of legal questions from different areas of law. For example can tortious liability exist for harm caused by the system and who is contractually

responsible for the costs of bills where the system has acted outside the bounds of agency defined by the user? More broadly, this process led to creation of a range of legal questions that were then mapped and clustered with relevant areas of law doctrinally analysed (i.e. assessment of concepts, principles and terminology from case law, legislation etc). Particular focus was given to unfair contract terms, tort law, consumer protection law, data protection and privacy law, agency and product liability.

The process of mapping the range of strengths and weakness in current legal governance of autonomy is not exclusive to the NEST study, and will be replicated in the context of three further ubicomp technologies (where specific stakeholder values may be challenged, uncertain aspects of legal governance could exist, and attributes of the specific technology being analysed might pull together these issues). This will involve situating the relevant technology in its social context, primarily through use of envisioning future scenarios/ narratives; pre-existing studies/datasets and self conducted qualitative empirical work (interviews, focus groups and design ethnography primarily).

Framing the discussions around specific system capabilities and limitations should providing greater clarity for the legal analysis. To narrow the scope of the legal resources used, the emphasis is restricted to examining effective regulation of autonomy in ubicomp systems.

Underpinning this overall procedure will be extensive translation of concepts, terminology and ideologies between legal and human computer interaction (HCI) design communities. Legal bodies like regulators and policymakers need far greater awareness of the challenges faced by designers in complying with the needs of the law. Equally, it is increasingly important for designers to understand the complex, fragmented state of law, and to interpret what it means for their work. This requires uncovering uncertainties inherent in the law, from the terminology used, the process of law (slow legislative progress), the ex poste nature of much legal regulation, and questions of ambiguity in interpretation of key legal concepts. Designers are not likely to be equipped with the skills to navigate this landscape, and part of the PhD will focus on understanding how to present this information in an accessible manner that highlights to what extent law provides clarity or uncertainty (i.e. does it create sufficiently clear guidelines/frameworks on what can and cannot do be done?)

The research will consider emerging concepts like 'Human Data Interaction' [5] for example. In the regulatory community, a lot of emphasis is placed on concepts like privacy/ethics by design and responsible innovation, to ensure legal and societal values are considered during the design of a new IT system. To realise the benefit of these concepts requires the uncertainty and ambiguity about the process to be addressed, with input from both communities. This PhD research will fit into that space, aiming to be an intermediary between law and design.

A working paper (written with co-authors at Nottingham) has already mapped the conceptual importance and the significant challenges inherent in integrating data protection law into the iterative, user centred HCI process.

The inadequacies or strengths in law can create new opportunities for designers to address legal shortcomings, and create solutions that actually work in practice.

Future Work

In order to unpack the impact for different stakeholders, the two upcoming pieces of work will focus on users and designers specifically. Firstly, focus groups and interviews will be conducted to understand the ethical and legal aspects of a privacy management tool that allows users to understand and alter data flows from smart metering data. By showing who controls, owns, collects, uses and shares the data the study will investigate the user perspectives on such a tool: from an individual data control/autonomy perspective - do they feel this technology is a solution that adequately protects their legal interests? What practical control would they like to see over their data use?

Secondly, there will be consideration of how the design process accounts for legal requirements such as data protection law or law of agency. This broadly looks at operationalising privacy by design [3] beyond policy rhetoric, and by understanding the processes of incorporating certain values into a technology via the framework of 'value sensitive design'[4]. This will involve qualitative work conducted alongside designers working on specific technologies to unpack their processes, concerns and what tools best ensure input from law in this space.

Contribution to the Field

From a law and policy perspective, this thesis will provide a valuable, empirically grounded insight into the range of issues that ubicomp technologies pose to the regulatory domain. Importantly, the output is to create solutions to these issues and the process of the research is to understand the problems to a suitable extent to be able to advise on solutions that truly meet the needs of the stakeholders (primarily users and designers). These may take the form of design and legal guidelines, conceptual frameworks, and technological tools.

More broadly, the process of understanding the legal aspects of ubicomp technologies through specific case studies should provide both the law and design communities with greater practical understanding of the problems they respectively face in addressing challenges like preserving human agency, consent and trust within emerging technologies. This research aims to take those insights and develop means that best facilitate increased dialogue between these two communities.

Acknowledgements

References

1. J. Camp & K. Connelly (2007) "Beyond Consent: Privacy in Ubicomp" in A Acquisti et al, *Digital Privacy: Theory, Technologies and Practices* (Taylor and Francis Group: 2007)

2. J. Cas (2009) "Ubiquitous Computing, Privacy and Data Protection" in S Gutwirth et al (2009) *Computers, Privacy and Data Protection: An Element of Choice* (Springer) p167

3. A. Cavoukian (2011) "Privacy by Design: The 7 Foundational Principles" *Information and Privacy Commissioner of Ontario*

4. B. Friedman (2012) "Envisioning Cards: A toolkit for catalysing humanistic and technical imaginations" *CHI 2012* http://www.vsdesign.org/publications/pdf/p1145-friedman.pdf

5. H. Haddadi, R. Mortier, D. MacAuley, & J. Crowcroft, (2013) "Human-Data Interaction" *Cambridge University Computer Lab Working Paper*

6. M. Langheinrich (2002) "A Privacy Awareness System for Ubiquitous Computing Environments" in *Lecture Notes in Computer Science 2498*, Springer (2002), 237–245

7. E. Luger, & T. Rodden, (2013) "An informed view on consent for UbiComp" *Proc. UbiComp '13*. ACM (2013), 529-538

8. H. Nissenbaum, *Privacy in Context.* (Stanford University Press, 2010)

9. A. Rouvray (2008) "Privacy, Data Protection and the Unprecedented Challenges of Ambient Intelligence" *Studies in Ethics Law and Technology*

10. S. Spiekermann and F Pallas (2005) "Wider Implications of Ubiquitous Computing" Poiesis & Praxis: International Journal of Ethics of Science and Technology Assessment

11. B. Stahl, G. Eden, M. Jirotka, and M. Coeckelbergh (2014) "From Computer Ethics to Responsible Research and Innovation in ICT: The transition of reference discourses informing ethics−related research in information systems" *Information and Management* http://www.cs.ox.ac.uk/publications/publication8475-abstract.html

12. P. Tolmie, J. Pycock, T. Diggins, A. MacLean, & A Karsenty, (2002) "Unremarkable computing" in *Proc. CHI '02. ACM Press* (2002), 399-406