User-Centric Regulation for the Domestic Internet of Things

Sensing & Privacy Workshop, QMUL, 20 June 2017

Dr Lachlan Urquhart - @mooseabyte
Research Fellow in IT Law
Horizon Digital Economy Research Institute
University of Nottingham
USER CENTRIC REGULATION (UCR)

- Complexity of regulating emerging tech
- Turn to creators of tech – e.g. PbD
- Problem: Situate role of IT designers in regulation
  - **Conceptual Perspectives** – turn to HCI & alignment with IT law
  - **Legal Perspectives** – what HCI concepts offer – case of IoT & PbD
  - **Expert Perspectives** – interviews with leading technologists & IT lawyers
  - **Design Perspectives** – developing & evaluating tool.

Source: INCTA.org
1A. CONCEPTUAL PERSPECTIVES: IT LAW

- Technology design = regulatory tool (Reidenberg; Lessig; Leenes; Brownsword etc)
- Broadening of actors/purposes of regulation - Black ‘post regulatory state’
  - Designers as new regulators shaping behaviour?
- Design in law – user?
  - Lessig - ‘pathetic dots’
  - Murray – ‘nodes’
- Inadequate engagement with how users interact with tech in practice?
  - Richer picture vs abstract notions of users
  - A role for HCI?
1B. CONCEPTUAL PERSPECTIVES: HCI

- **HCI and Society:**
  - Third wave of HCI (Bødker) cultural/emotional dimensions of computing; Reflective Design (Sengers); responsibility to users (Human Data Interaction)
  - Value sensitive design (Friedman)- Human values in the relationship between user, technology and designer
  - Extend to legal issues too?

- **User Centric Focus:**
  - HCI - range of tools and approaches to understand user interactions with technology in context
  - Design ethnography, participatory design with users – Scandinavian School
• Explicit Alignment of IT law and HCI:
  • Structuring reflection and action by designers
  • Sensitise to nature of legal and ethical responsibilities to users.
  • Earlier appreciation of legal dimension – requires mutual support.

• Legitimacy through User Proximity

• Legal Values, Ethics and Responsibility
  • From human values in HCI to legal values.
  • Beyond compliance - ethical concerns.
2A. CASE STUDY: UCR AND THE INTERNET OF THINGS

- **Trajectory:** from Ubicomp, Pervasive, Aml, AAL, Smart Homes, etc...now IoT

- **Risk of Visions:** Engineering challenges - neglect the present and interests of users...eg seamless networking

- **Applications:** energy...security...lighting...health e.g thermostats, smart meters, smoke alarms, lightbulbs, ; fridge?

- **Setting:** mundane, everyday, augment routines...complex social space of home vs invisible in use/seamlessness

- **Creative Dimensions of IoT:** experiences, tracking story of objects – guitars, books, Warhammer etc
2B. FUZZY PRINCIPLES

• **No Canonical Vision**— survey of reports eg ITU; Cisco; A29 WP; IETF etc
  
  • Remote controllability & automation (e.g. via apps)
  
  • **Constant connectivity** and networking - for data transmission & service provision (e.g. cloud backend, databases)
  
  • Ecosystem of stakeholders, incl. **third parties** & data **flows**
  
  • Physical objects **ambiently sensing** & **embedded** in social and physical the environment
  
  • With or without **human input** (lack of UI)
2C. REGULATORY CHALLENGES OF IOT

• Detailed inferences about everyday life
• Limited transparency of data flows
• International data transfer (cloud)
• Insufficient user control (lack of UX)
  • Heterogeneity of device interfaces
  • Control over access to data
• Data repurposing
2D. SOLUTION: PRIVACY BY DESIGN

- Legally: EU GDPR (2016) Article 25
- **Technical and organisational measures** of state of art; costs; severity of risks
- Historically?
  - Cavoukian; Usable Privacy; Privacy Engineering
- Practically - Tools to Support Designers?
  - “whereas for lawyers PbD seems an intuitive and sensible policy tool, for information systems developers and engineers it is anything but intuitive” (Birnhack, Toch and Hadar)
  - “Fostering the right mind-set of those responsible for developing and running data processing systems” (Jaap Koops and Leenes)
- Need cross disciplinary response...
2E. USER CENTRIC REGULATION FOR IOT

- 1) Right to be Forgotten and Object Provenance
  - Archiving - Carolan/W40K/TOTeM – object centric narrative
  - Balancing these interests - RTBF vs object memories
- 2) Trajectories and Consent
  - Benford et al (2011) – designing user experiences
  - Repurpose for obtaining user consent in IoT eg smart thermostat?
    - space (home – contested social space),
    - actors (third party flows and transient visitors),
    - interface (waves, beeps, feedback);
    - Time (longitudinal)
- 3) Seamful Design & Legal Uncertainty
3A. PRACTICAL PERSPECTIVES

• Semi Structured Interviews
• 6 tech lawyers
  • 14 years average exp. – partners, associates
  • Expertise: contracts, data protection (DP), intellectual property, e-commerce etc.
• 7 technologists
• 32 years average exp. – CTOs, chief consultants, MDs
• Expertise: wireless networking, infosec, data science, telecoms, cloud computing, interaction design
3B. BUSINESS INSIGHTS

1) Differentiated resources
   - SMEs
     - investment – not compliance
     - Lack of resources
   - Multinational
     - systematic, resources available; internal advice

2) Business models and motivations for engagement (IoT market).
   - Cheap device - Monetise personal data - Stockpile data for later use
   - Protect Brand values... fear of hacks, scandals
   - Making a better product - fear of competitive disadvantage
3C. REGULATORY INSIGHTS

• **Contextualising Privacy by Design and Legal Values**
  - Technologists: Uncertainty of term – contested values – need to contextualise PbD for different sectors eg smart cars, energy etc

• **Regulatory Challenges in practice**
  - Smart phones as mediating devices for consent
  - Complexity of IoT ecosystems eg smart building vs fitbit

• **Managing Risk and the Realities of Enforcement**
  - Commercial mindedness to enable growth
  - Difficulties assessing risk of enforcement/sanctions
    - Pace of tech change vs law playing catch-up
    - A29 WP advice v valuable
3D. TECHNOLOGICAL INSIGHTS

• Application Led Framings of Technology
  • Move away from need to define what is or isn’t IoT – focus on applications, contexts of use...not visions

• Appreciating Conflicting Agendas
  • Technologists pulled many ways – business case, compliance, security, usability

• Communicating the Relevance of Law to Designers
  • Contextualise and translate law - internal codes of practice, standards, personal life/scenarios
4A. DESIGN PERSPECTIVES - PRIVACY BY DESIGN CARDS

- Raise awareness; Support engagement; Resource for reflection on legal concepts
- Ideation cards to surface and explore issues
- History of use value sensitive design, security, IDEO...
  - Structured approach to introduce new concepts into design process
- Translation of Legalese
- Original Deck - ACM CHI 2015
- Expansion to whole GDPR
  - Project: U of Nottingham, Microsoft Research Cambridge, U of Edinburgh
4b. Clusters

**Legal Principles**
- Informed, unambiguous consent
- Purpose limitation
- Data minimisation

**Rights:**
- To be forgotten
- Subject access
- To data portability

**Responsibilities**
- Data Security
- DP Impact assessment

**Global Data Flows**
- Adequate Protection
- Cloud Computing

**Definitions**
- Personal Data
- Data controller
- Data Processing
4C. TESTING THE CARDS

• 3 organisations:
  • Large media company (MOZ)
  • Innovation networking body for SME/Start-up (INC)
  • Small tech business trade association (SBA)
• 24 participants
  • Table opp.
• Findings: Regulatory Literacy

<table>
<thead>
<tr>
<th>Job Cluster</th>
<th>Example Jobs</th>
<th>Percentage of Overall Participants</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Business Strategy and Management</td>
<td>e.g. Managing Director; Facilitator; International Development; Auditor/Accountant; Marketing; Patent Attorney</td>
<td>33% (8)</td>
</tr>
<tr>
<td>2. Technology, Design and Creative</td>
<td>e.g. Software Engineer; IT Consultant; Programmer; Cyber Security and Privacy Consultant; Producer; Graphic Designer; UX Designer;</td>
<td>50% (12)</td>
</tr>
<tr>
<td>3. Research</td>
<td>e.g. Industry Research Scientist; Senior Lecturer; PhD Student</td>
<td>17% (4)</td>
</tr>
</tbody>
</table>
4D. THE DECK

1 System card + 1 Users card + 2 Constraints cards + 2 Legal Cards
4E. REGULATORY INTERACTION

- Motivations: A Spectrum of Values and Responsibilities
  - Protection of reputation, guarding against bad publicity, litigation or loss of public trust.
  - Necessity - SMEs
- Negotiating with the Law
  - Rich discussion of law – not using legal terms
  - Legal authority mandates action
  - MOZ - cards empower employees – knowledge engaging with internal advice giving bodies
  - SBA – easier entry point to law
4F. SENSE-MAKING STRATEGIES

- Support Mechanisms with Networks, Community and Leadership
  - SMEs - self help – face to face social network
  - Cards as Awareness Raising, but what next?
    - Concise, creative, fun, tool that prompts reflection
    - Desire from SMEs further resources – roadmap of further action
4G. MANAGING COMPLEXITY

• Designer Responses - Risk Management, Utility and Granularity of Data
  • Balance desire for more data, with legal compliance risks
  • Keen awareness of privacy – control granularity internal and external (occupants vs third parties)
  • Security big concern for SME
• Pragmatism and User Centricity
  • Difficulty reconciling commercial nature of consent and desire for consent to be better for users
    • Translation comprehension not just info
  • International Transfer - Local storage, avoid US cloud
QUESTIONS?

• Thanks for Listening
• lachlan.urquhart@nottingham.ac.uk
• @mooseabyte