Agenda

- Building an IoT legal framework: the EU angle
  - Cyber security
  - Data protection
  - Terms and conditions and liability
- For each area
  - Why particularly a challenge for IoT
  - Key legal challenges for any framework to resolve
Internet of Things in the EU

- Market value of the IoT in the EU expected to exceed **one trillion** Euros in 2020

- Key focus of the European Commission: 3 pillars:
  - Single market for IoT: devices and services should work seamlessly across the EU
  - Develop a thriving IoT ecosystem including use of open platforms where possible
  - Human-centred IoT: high and trusted standards of protection of personal data and security
Leading EU IoT provider
Real world examples

- Hive smart heating controller
Real world examples

- AGFEO - German smart home provider
  - smart home controller
Real world examples

- Miele web connected dishwasher
Real world examples

- Purple wifi
  - Manchester based firm Purple added a “Community Service” clause to their usual wifi terms and conditions
Real world examples

The user may be required, at Purple’s discretion, to carry out 1,000 hours of community service. This may include the following:

- Cleansing local parks of animal waste
- Providing hugs to stray cats and dogs
- Manually relieving sewer blockages
- Cleaning portable lavatories at local festivals and events
- Painting snail shells to brighten up their existence
- Scraping chewing gum off the streets
Real world examples

- 22,000 people signed up for the free wifi over a two week period
- A prize was on offer to anyone who spotted the “Community Service” clause
- Only one individual claimed the prize
Cybersecurity and IoT

- Key issue given real world impact of IoT
- Common themes
  - Lack of testing of consumer products
  - Security not prioritised over time to market
  - Users lack awareness of the risks and will not pay a premium for security
  - Vendors not geared up to respond quickly when issues are identified
Cybersecurity: EU position

- Network and Information Systems Directive
  - In force in EU from 9 May 2018 (at the latest)
  - Member states consulting now
  - Restricted to “essential services” (water, energy, healthcare etc) and larger digital service providers
Cybersecurity: EU position

- ENISA (EU Cyber Security Agency)
  - December 2015 report:
    “the need for security in Smart Home Environments is still underestimated and vendors lack incentives toward this goal”
  - July 2017: plans for New EU Cybersecurity Strategy
Data protection and IoT

- Key to develop trust in use of data by multiple internet connected devices

- Common themes
  - Consent issues
  - Lack of clarity on “ownership” of data / risk of vendor “lock-in”
  - Multiple entities involved in processing data
  - Cross border issues
Data protection: EU position

- General Data Protection Regulation
  - Increased requirements around consent and associated information provision
  - Applies across supply chain to processors
  - Enhanced user rights: withdrawal of consent; deletion; porting to a new provider
  - Extra territorial
  - Substantial potential fines
Data protection: EU position

- Privacy and Electronic Communications Regulations
  - Specific rights in relation to electronic communications
  - Supplement GDPR
  - Under review to take into account IoT issues
Ts and Cs and IoT

- Key to be confident that terms are understood and enforceable

- Common themes
  - Multiple sets of terms and conditions
  - Terms written for one jurisdiction and not reviewed for local law compliance
  - Consumer law protections not always taken into account potentially impacting enforceability
Ts and Cs and liability

- Consumer protection for IoT
  - Clarity of terms and conditions vs click to agree
  - Onerous provisions for consumers eg “bricked” devices

- Determining liability for unsafe technology
  - Given interdependencies, who is responsible

- Liability limitations
  - Consumer legislation
  - Unfair contracting provisions
Q and A?