Internet of Things privacy: risks, regulations - and solutions?

Kuan Hon
Senior Researcher, Cloud Legal Project & Microsoft Cloud Computing Research Centre, Centre for Commercial Law Studies, Queen Mary, University of London
w.k.hon@qmul.ac.uk
Introduction

- Self – 4 x 3 x 2 x

- CLP, MCCRC (IoT in 2015) & A4Cloud

- Questions – please leave till end or Panel session
IoT - & closely-related concepts

- **IoT “Things”** –
  - sense &/or actuate + connectivity; “ThingData” & “ThingActions”

- **IoT & cloud** (given Things’ limited storage / processing)
  - cloud to store / process ThingData; control / mediate Things & ThingActions - many IoT cloud platforms, incl. proprietary
  - “CloudData” = ThingData, data from analysing ThingData, etc
  - Therefore, “Clouds of Things” – CloudServices as ThingServices

- **IoT & cloud & big data**
  - ThingData often “big data”; cloud for big data processing of ThingData & related (e.g. derived) CloudData

- **European Commission** – IoT, cloud, big data “central” to EU competitiveness, innovation, jobs

@kuan0
Complex ecosystem >> cloud

- Many roles / relationships, e.g. Fitbit ThingServices
  - “online and mobile services, including, but not limited to the Fitbit website…, widgets, computer programs and mobile applications hosted by or on behalf of Fitbit” – & potentially third parties?

- ThingData volume / nature, players; so privacy risks:
  - Thing owner, Thing user – **others** whose data are captured by Things - Google Glass **fuores**; ( & employees etc. )

- Tension – privacy vs. benefits of open / shared ThingData

- Obligations, risks for many players (not just privacy):  
  - Thing maker (use other Things? ), distributor, vendor, lender etc; developer of OS, apps etc; ThingService provider, sub-contractors, CloudService providers, telcos, platform providers
Laws / regulations on privacy in IoT?

- Nothing IoT-specific
- But, sectoral laws / regulations - e.g.
  - EU eCall Regulation – mandatory in-vehicle emergency call service (privacy FAQ) – from 31 March 2018
- General laws on privacy / data protection apply to IoT / cloud / big data
- My focus – EU only

@kuan0
Concerns and consultations - EU


- Privacy / data protection regulators e.g. on
  - (Internationally) Profiling, IoT (Mauritius Decl.), cloud, big data
  - EU (Article 29 Working Party opinions)
    - IoT (WP223), cloud, big data
    - Also RFID, smart grids / meters, geolocation on mobile devices, facial recognition, biometrics, apps on smart devices, drones
  - National consultations e.g. Italy; guides e.g. ICO on big data

@kuan0
Common issues

- Trust & reputation
  - Example: my smart meter experience - health ?!
- Lack of transparency, loss of control (cloud also)
  - informed consent
- Monitoring, profiling, discrimination - & loss of control
- Interoperability, data portability
Data Protection Directive – recap

- “Personal data” (PD) as the trigger
  - Only “personal data” caught
- “Controller” must follow data protection (DP) principles when processing PD
  - Legal basis, fair processing, purpose limitation etc
  - Exemptions for national security etc., personal use
  - + Rules for “special category” sensitive data eg health
- May use “processor” – incl. cloud provider
  - Requirements on controller when using processor
- Myth re. “consent” (cf. US “notice+choice”)
  - “Legitimate interests” possible (if not too invasive)
E-Privacy Directive Art. 5(3) – recap

- In addition to DP Directive! (summary of “cookie law”)
- Store or access information stored in “terminal equipment” of subscriber or user iff (with exemptions):
  - consent given, after
  - “clear and comprehensive information”, incl. about purposes
- Often termed “cookie law”, but >> websites / cookies
  - any storage or access (network not always necessary! e.g. UK)
  - any stored information (not just “personal data”)
  - anyone (not just controllers)
- Things are probably “terminal equipment”
Key DP legal issues for IoT

- What ThingData ( & associated CloudData) are “personal data”, even sensitive PD? - anonymisation problems

- Personal “household” use – Ryneš
  - attacks; CCTV video; entrance to home, public footpath, opposite house’s entrance; suspects prosecuted; “controller”! partially public

- Legal basis, e.g. informed consent – cf. study for Ofcom

- Purpose limitation; profiling (automated decision making), data minimisation; data retention; data quality

- Security (DPD “security“)

- Others e.g. applicable law (equipment), RTBF, “transfer” restriction

@kuan0
WP223 on IoT

- Very strict view > current law - impossible? (cloud too)
- Lack of control and information asymmetry
- Quality of user’s consent
  - can’t rely on consent as legal basis! (NB. not binding)
    - especially third parties. Signpost?
  - can’t disable certain features – not true consent?
- Purpose limitation – risk of repurposing, profiling incl. inferencing; combining data from different Things
- Security – energy-efficiency prioritised over security
- Recommendations for:
  - OS & Thing makers, app developers, social / data platforms, Thing owners / users, standards bodies

@kuan0
Key GDPR areas affecting IoT

- “Personal data” definition & anon. / pseudonymous data
- “Exclusively” personal use ? ( Council would delete )
- Transparency, notice – expanded; ( Parl ) info policies
- Consent – explicit, specific, limited, revocable
  - how to get / prove consent ? but e.g. legitimate interests ( though must disclose, strong right to object )
- Data minimisation, purpose limitation – Council could relax ? ( legit. interests ); data retention / deletion
- Profiling - consent, object; notice, threshold ? Pseud. data
- Security ( incl. processors ) - & breach notifications
- Risk analysis ( Parl ), DPIA, prior consultation
Other relevant GDPR areas

- Direct processor obligations & liability allocation
  - broad view of “processors”, more players caught?

- Certifications, codes etc
  - Council – “an element” to show compliance; Parl – regulator-awarded seal a “shield” absent negligence / intention

- Fines etc.; on-site audits

- Territorial scope
  - “offering” instead of equipment

- One-stop shop

@kuan0
Solutions?

- Too early for solutions but -
  - Regulators emphasise DPIA / risk assessment + PbD
    - selling point / competitive advantage / trust
    - continuous governance programme; accountability & documentation
  - Insurance?

- Consider legal risk (holistically)
  - get caught, big fine? e.g. media & celebs – business decision to ignore data protection laws
  - but the tide is turning – UK cases; GDPR fines; and increasing international cooperation between privacy / data protection regulators
    - e.g. mobile apps “sweep” 2014
Practical issues

- Legal analysis of specific situation (incl. cloud elements)
  - which player(s), which processing (incl. storage) – who’s controller, processor?
  - based on early risk assessment & DPIA – false economy to delay!
    - information on aims, data type, real life intended use; explanation of tech / model & 2-way communication (NB. mindsets, terminology, different countries)

- DPIA + PbD (all players!)
  - transparency / notice (incl. third parties), data minimisation, user-friendly methods to get user consent, pseudonymisation / anonymisation “ASAP”, granular user control, allow user monitoring, security by design, local processing, deletion, data portability, 2nd hand Things (WP223; ENISA, OASIS)

- Contract - processor obligations, liability allocation
- Certifications, codes, seals?

@kuan0
Broader issues

- EU Charter of Fundamental Rights
  - Privacy and data protection – separate rights
  - EU and national laws overturned for incompatibility
- European Convention of Human Rights - privacy
- Other laws – e.g. confidentiality, misuse of private info
- Not just privacy…
  - Consumer protection – standard contract terms
  - Standards - e.g. connected TVs – both interop & security
  - IP – licensing etc
  - Liability for ThingActions… product liability etc
  - Spectrum use – interference, fair allocation etc

@kuan0
Thanks for listening!

w.k.hon@qmul.ac.uk

cloudlegalproject.org
mccrc.eu

@kuan0 | kuan0.com
blog.kuan0.com