Legal certainty as a tool for the spread of the Internet of Things
Overview

• IoT Law (issues and main regulations)
• Actors
• Contract Law
• Nest use case
• Product liability
• Privacy and data protection
INTERNET OF THINGS LAW

Certifications

Contract Law

Consumer protection

Privacy/data protection

Private International Law

Business Law

Criminal law

Civil liability

Public Law

Competition

Insurance Law

Standards

Security

Environmental law

Tax Law

IP

Legal Philosophy
IoT regulation in Europe

- WP29, Opinion 02/2013 on apps on smart devices, 27.2.2013
- ECJ, 11-12-2014, František Ryneš c. Úřad pro ochranu osobních údajů
- Commun. on “Future networks and the internet”, 29.9.2008 (s. Staff WD on Early Challenges regarding the “Internet of Things”)
- DG Connect, Europe’s policy options for a dynamic and trustworthy development of the Internet of Things, 31.5.2013
- ECOSOC, Opinion on ‘The Internet of Things’, 18.9.2008
- WP29, Opinion 02/2012 on facial recognition in online and mobile services, 22.3.2012
- WP29, Working document on data protection issues related to RFID technology, 19.1.2005
- WP29, Opinion 13/2011 on Geolocation services on smart mobile devices, 16.5.2011
- WP29, Opinion 04/2014 on surveillance of electronic communications for intelligence and national security purposes, 10.4.2014 (and WD of 5.12.2014)
- Council of Europe, The rule of law on the Internet and in the wider digital world, December 2014
- ENISA, Smartphone Secure Development Guidelines for App Developers, 25.11.2011
- ENISA, Appstore security, September 2011
- Parl. Res. on the Internet of Things, 15.6.2010
- EDPS, Internet of things. Ubiquitous monitoring in space and time, 29.4.2010
- EDPS, Opinion on Promoting Trust in the Information Society Fostering Data Protection and Privacy, 18.3.2010
- IERC-Internet of Things European Research Cluster (groups together the IoT projects like IoT-A and IoT-D)
- IoT experts group, Report on the Public Consultation on IoT Governance, 16.1.2013 (and other material from the IoT experts group)
- ISTAG, Scenarios for Ambient Intelligence in 2010, February 2001
ECJ, František Ryneš

- Art. 3.2 dir. 95/46 This Directive shall not apply to the processing of personal data...by a natural person in the course of a purely personal or household activity

- “The operation of a camera system, as a result of which a video recording of people is stored on a continuous recording device such as a hard disk drive, installed by an individual on his family home for the purposes of protecting the property, health and life of the home owners, but which also monitors a public space, does not amount to the processing of data in the course of a purely personal or household activity”

- i. The camera was in a fixed position and could not turn; ii. it recorded the entrance to his home, the public footpath and the entrance to the house opposite; iii. only a visual recording; iv. Stored on a hard disk drive; v. As soon as it reached full capacity, the device would record over the existing recording; vi. No monitor was installed on the recording equipment: no real time study; vii. Only Mr Ryneš had direct access to the system and the data.
IoT regulation: a comparative perspective


- **China**: reg. 19.4.2013 prevents manufacturers of mobile smart devices from preinstalling apps that raise privacy, security, or prohibited content concerns

- **India**: *Draft Policy on IoT*, 8.4.2015 (sensors for early defect detection)
International documents

• ITU, *The Internet of Things*, November 2005 (report)
• ITU-T, *Overview of the Internet of Things*, Y.2060, June 2012 (recommendation)
• Mauritius Declaration on IoT, 14.10.2014
Mauritius Declaration on IoT

- 36th Int’l Conference of DPAs
- Big Personal Data: sensor data are high in quantity, quality and sensitivity → inferences → identifiability
- Value not only in the devices, but in the new services and in the data
- Clear about what data they* collect, for what purposes and how long this data is retained
  *those who offer internet of things devices
- Privacy by design and by default should become a key selling point
- Firewall not sufficient: local processing or end-to-end encryption
IoT and contract law

• Contracts **difficult to understand** (opaque wording; born old; alien; multi-layer)

• **Chain** of contracts (hard to find/read/jointly interpret; fictitiously separate products)

• **Dependence** (economic d. supply chain; lock-in)

• Freedom of contract and asymmetric bargaining power: rid of **paternalistic consumer law**? (ubiquitous real-time access to information, but reality&contracts still too complex)

• **Things that sell things** (=coke machine: 1. Everywhere; 2. Autonomy; 3. Things can sell also themselves, s. Brad)

• Consent by design and **awareness by design**

• Private ordering (**hysteresis**: regulatory gaps)
Case Study: Nest

- One product, a thousand contracts!
- “With a smart system, the whole point is that when you use it, it learns about you over time. That learning intrinsically involves some sort of logging” (James Scott, 2015)
The contractual quagmire

- Terms of Service (sites, web apps, mobile apps)
- EULA (embedded software)
- Sales terms (hardware)
- Limited warranty
- Privacy statement (information collected via the devices)
- Website privacy policy
- The open-source compliance
- Intellectual Property and other notices
- Community Forum Agreement
- EU Declarations
- Installation ToS
- Developer ToS
- Does Google privacy policy apply?
- + Works with Nest
- + [US] FCC Compliance Notice, Customer Agreements for Rush Hour and “Silence the chirp”
Product Legals

+ "n" contracts * interoperable software/apps

+ "n" contracts * interoperable devices

= ∞
‘Product’ under the ToS

Professedly, the “ToS” apply only to the services and not to the hardware, but it affects the latter

“If you do not agree with any of the provisions of these terms, you should disconnect your products from your account and cease accessing or using the services”

1. The product is an inseparable mixture of hardware and software/service→ strict liability under the Product Liability Directive also for services/software/apps flaws

2. Standard contracts: little room for customisation (“You must accept this agreement as presented to you, without changes” (Community Forum Agreement))
‘Product’ under the Sales Terms

The ST **professedly** refer to the product as **hardware**, but:

> **“These Terms constitute the entire agreement between you and Nest regarding the use of the Services.”**

Confirmation in the “Privacy statement”: Nest Products include our mobile and web applications.
‘Product’ under the EULA

“If you do not agree with any of the provisions of these terms, you should cease accessing or using the product software.”

(customisability)

Is it feasible to use the device without using the embedded software? No (notion of product)

“Modifications...may be automatically installed without providing any additional notice or receiving any additional consent. (...) If you do not want such Updates, your remedy is to stop using the Product.” (asymmetry)
Product Liability

Product Liability Directive of 1985 and Consumer Protection Act 1987 apply also to flaws of services, software and apps→revival of this regime (liability without fault) forgotten for a lot of years

Immovables->movables->immaterial->IoT (hardware+software+service)

“The commercial sellers’ growing information about, access to and control over their products, product users, and product uses could expand their point of sale and post-sale obligations toward people endangered by these products” (Smith 2014)

Under this regime, the multi-layered nature of IoT market can’t act as a disclaimer

Are the contractual warranty disclaimers/liability limitations enforceable under dir. 85/374 and CPA 1987?
Directive on Defective Products

**Strict liability:** the injured has to prove only to prove the damage, the defect and the causal relationship between defect and damage (art. 4). And it is **not negotiable contractually:** the liability of the producer arising from this Directive may not be limited or excluded by a provision limiting his liability or exempting him from liability (art. 12)

‘**Damage**:’ death, personal injuries or damage to, or destruction of, any item of property other than the defective product itself (art. 9) → not a panacea

‘**Product**’ means all movables, with the exception of primary agricultural products and game, even though incorporated into another movable or into an immovable (art. 2) It encompasses IoT products **notwithstanding the fact that they are equipped with software** (s. above and, also, Dir. 2009/24 on protection of computer programs: nothing on liability)

‘**Producer**’ means the manufacturer of a finished product, the producer of any raw material or the manufacturer of a component part and any person who, by putting his name, trade mark or other distinguishing feature on the product presents himself as its producer (...) any person who imports into the Community (art. 3) **Compound things+complex supply chain**

A product is defective **when it does not provide the safety which a person is entitled to expect**, BUT the producer is **not responsible if the state of scientific and technical knowledge** at the time when he put the product into circulation was not such as to enable the existence of the defect to be discovered: the **case of the IoT?**
Consumer Protection Act 1987

Broader definition of ‘product’: “any goods or electricity” (and ‘safety’, in relation to a product, shall include safety with respect to products comprised in that product”)

Broader definition of ‘producer’: also the person who won or abstracted a substance used in the product and the person who carried out a process to which is attributable an essential characteristic
Privacy and data protection

“Every IoT-enabled device, whether an iron, vacuum, refrigerator, thermostat or lightbulb, will come with terms of service that grant manufacturers access to all your data.” (Goodman 2015)

- Things process big data
- Things communicate to things (SIoT) and persons
- Things are part of everyday life (everyware)
- Contractual quagmire: which protection is actually recognised?
- Multi-layer: “we have no control over and cannot confirm whether third parties honor the Do Not Track” (WPP)
- Processing lawful without consent if necessary “for the performance of a contract to which the data subject is a party”

Minimising privacy concerns requires:

- Ensuring only data critical to the functionality of the device are collected (data minimisation)
- Ensuring data collected are properly protected via technical protections (e.g. encryption).
- Ensuring the device and all of its components properly protect personal data. (privacy by design and by default)
IoT privacy in the UK


- More connected objects than people
- Breaches of security and privacy have the greatest potential for causing harm
- Legislation should be kept to the minimum required to facilitate the uptake of IoT
- The scale of personal information (locational and financial information), which is collected by existing technology, is huge: with IoT exponential growth
- Researchers carried out a cyber-attack that allowed them to control steering and braking of a car.
- Security vulnerabilities were exposed in a baby monitor device, enabling the hacker to shout at a sleeping child.

No panic! The owner failed to change the default password
IoT privacy in the UK

ICO, *Response to Ofcom's consultation 'Promoting investment and innovation in the Internet of Things'* , October 2014

• With ‘personal’ electronic devices (smartphone) “the *organisation* collecting and using the information is a ‘data controller’ and is therefore fully subject to data protection law”

• With less ‘personal’ devices (TV), the application is uncertain
IoT privacy in the UK

The rule: unless a particular individual is identified - or is reasonably likely to be identified - by the organisation collecting the information from the device, the information will *not* constitute personal data” (multi-tenancy devices ≠ individual ones).

True, but beware to “linking or matching data with other datasets” (not only datasets).

If the DPA doesn’t apply-*de iure condendo* introduction of industry *codes of practice* or other *soft-law* instruments that would address this.
IoT privacy in the UK

The 1<sup>st</sup> of the 8 DPA principles on **good information handling**: any personal data processing is both lawful and fair→information also about the **purpose** of any processing.

IoT devices may have **no physical interface** at all with which an individual can interact! Valid informed consent? (crucial especially in medical liability).

On the other hand, things talk and augmented reality: **overload** of information?

No/small interface → 1) connect to a **separate computer** → the configuration software running on the computer will need to be **coded** securely; 2) limited physical interface+complicated underlying technical (and relational) situation = **privacy by design**.
IoT privacy in the UK

The end-user has little chance to modify both the object and the service—privacy by default.

A device can have privacy features available, and yet may not be as privacy-friendly as it could be because those features are not enabled by default.
IoT privacy in the UK

• The DPA's 7th data protection principle requires organisations to take appropriate technical and organisational measures against unlawful/unauthorised processing and loss/destruction of personal data.

• **IoT organisational complexity** - if someone discovers a security flaw in the device's software, whose responsibility to fix it? How will this fix be applied. If no action is taken, such a flaw could allow an attacker to compromise the device.
IoT privacy in the UK

• “It will generally be appropriate to use an SSL / TLS connection where it is necessary to transmit any sensitive personal data, user login credentials or unique identifiers”.

• HAVE USERS CONTROL ON THE CONNECTION AND ON ITS DEGREE OF SECURITY?
IoT privacy in the UK

• **Software lifecycles** are potentially **shorter** than the expected lifetime of an IoT device

• Software projects become soon **unsupported** → **security updates** are no longer provided→**increasing security risk**+stop of functioning.

• Specifications of the hardware openly available, so that **FOSS** could be written and maintained for the lifetime of the device
IoT privacy in the UK

FROM IPV4 TO IPV6.

• The widespread adoption of IPv6 \((2^{124})\) would ease the problem of limited IPv4 addresses and how they should be allocated...

• ...however, it would make IP addresses much more likely to be personal data in any given case (every device in the world a unique address in space and time).
IoT privacy in the EU


• Caveats: unclear 1) the possible convergence and synergies of the IoT with other technological developments such as cloud computing and predictive analytics; 2) how to transform all the data possibly collected in the IoT into something value sensitive. $1+2=$ focus only on wearable computing, quantified self and domotics
IoT privacy in the EU

Fundamental assumptions

• “The IoT usually implies the processing of data that relate to identified or identifiable natural persons, and therefore qualifies as personal data in the sense of art. 2 DPD”.

• The processing of such data in this context relies on the coordinated intervention of a significant number of stakeholders.
These different stakeholders may be involved for various reasons: “once the data is (sic!) remotely stored, it may be shared with other parties, sometimes without the individual concerned being aware of it” = the further transmission of his/her data are thus imposed on the user who cannot prevent it without disabling most of the functionalities of the device.
IoT privacy in the EU

IoT privacy and data protection challenges:
1) Lack of control and information asymmetry
2) Quality of the user’s consent
3) Inferences derived from data and repurposing of original processing
4) Intrusive bringing out of behaviour patterns and profiling
5) Limitations on the possibility to remain anonymous when using services
6) Security risks: security vs. efficiency
Final remarks

• Contractual quagmire
• No time to overturn the paternalistic approach of consumer law
• Revival of product liability regulations
• By design (privacy, consent, awareness)
• Need for comprehensive and international regulations
• Need for interdisciplinary research groups
THANK YOU!

Guido Noto La Diega

noto.la.diega@gmail.com