Privacy, the Internet of Things and Smart Cities

Professor Lilian Edwards
– *University of Strathclyde*
Nijmegen 2016
Lilian.edwards@strath.ac.uk
@lilianedwards

CENTRE FOR INTERNET LAW AND POLICY

1. What is the Internet of Things?

Ubiquitous, pervasive computing (ubicomp)

- Smart meters
- Domestic and care robots
- Driverless or connected cars (legalised Nevada, soon UK)
- Apps/wearables measuring not just location but physical activity – FitBits, Jawbones, Apple watch etc
- Smart CCTV – image, sound and behaviour, gait, face recognition
- Chips in human body – health monitoring, data flow eg from pacemaker

Driverless lorries to be trialled in UK

5 March 2016 | UK Politics

Daimler's self-driving truck has been tested on the German autobahn

Driverless lorries are to be trialled in the UK, Chancellor George Osborne is expected to confirm in his Budget speech this month.


Home
What is Grindr?
Using Grindr
About
Gear
Contact
Help
Download
Join the Grindr Revolution
iPhone
3:23 PM
Back
David
More
Hey bud. I like your profile.
Thanks man. You too.
Where u at?
Let's meet. Here's a photo.
GRINDR
Meet Guys Near You
It's Here!
Grindr for
ANDROID
Download
Download
Grindr
for Android
Download
Grindr
for iPhone
XTRA
Download
Grindr
for iPhone

IoT fail

Google Glass: what you need to know

IN DEPTH Are Google's glasses more than just a gimmick?

By **James Rivington** February 15th

7 COMMENTS

Like 119 Send Tweet 31 +1 86 1

Does Project Glass represent the next big step in mobile communications?

Barcelona clubbers get chipped (2004)

BBC Science producer Simon Morton goes clubbing in Barcelona with a microchip implanted in his arm to pay for drinks.

Imagine having a glass capsule measuring 1.3mm by 1mm, about the size of a large grain of rice injected under your skin.

Last week I headed for the bright lights of the Catalan city of Barcelona to enter the exclusive VIP Baja Beach Club.

The night club offers its VIP clients the opportunity to have a syringe-injected microchip implanted in their upper arms that not only gives them special access to VIP lounges, but also acts as a debit account from which they can pay for drinks.

Epicenter Sweden 2015

29 January 2015 Last updated at 17:01

Share

Rory Cellan-Jones
Technology correspondent
More from Rory | Follow **Rory on Twitter**

Office puts chips under staff's skin

COMMENTS (635)

The chip allows employees to open doors and use the photocopier without a traditional pass card

RFID: enables IoT

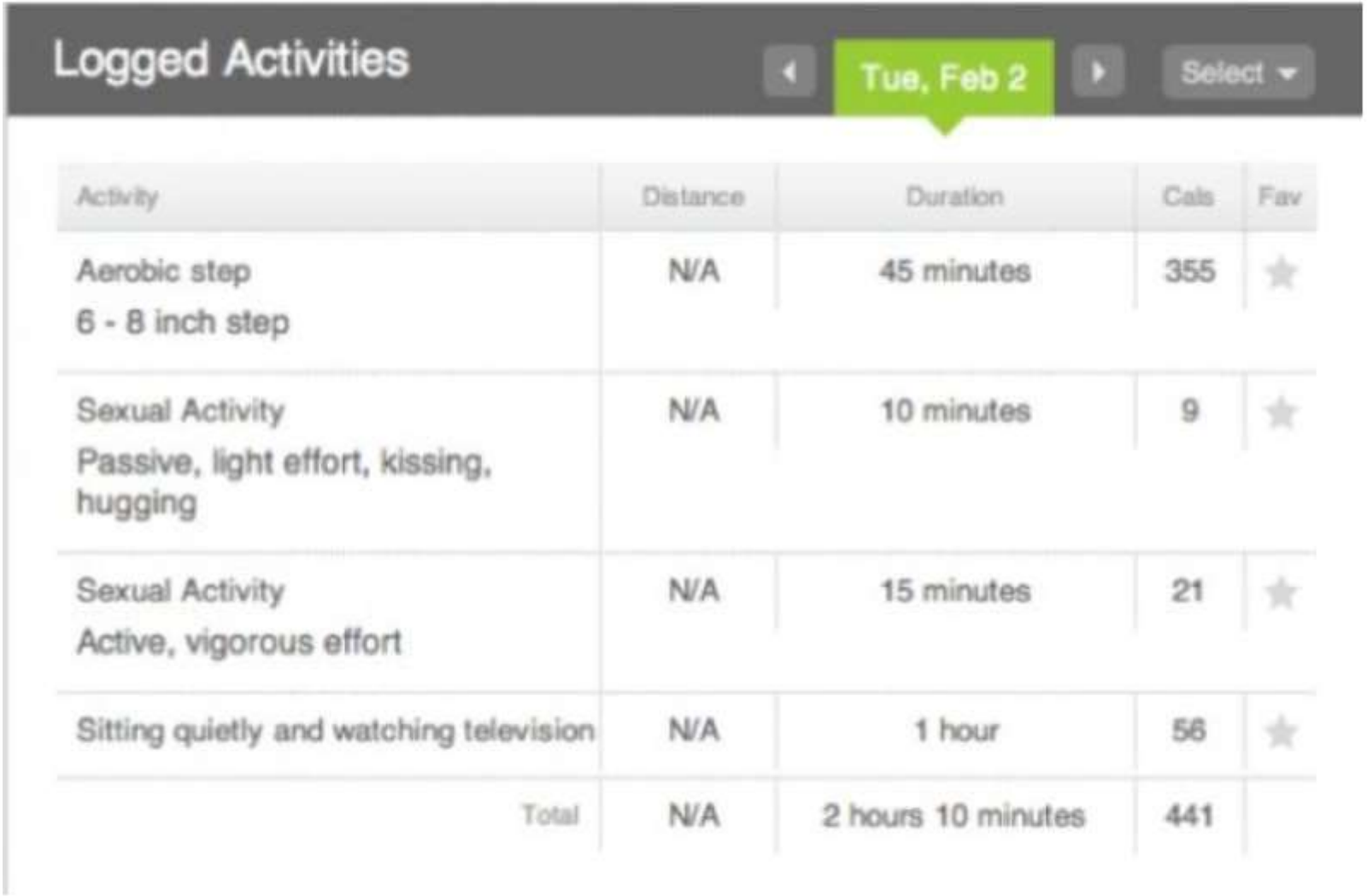
- What is RFID? Radio Frequency Identification chips. Initial main uses: inventory tags, retail chain barcoding, bag tracing, pets etc
- Transition to collecting data re humans? Passports, smart cards, transport cards, internal passes, library books, pupils, patients, prisoners?
- Identifies *things* not people. Early part of "The Internet of Things" or "ubiquitous computing" (ubicomp).
- Essentially collects the *location* of an object.
- Currently mainly cheap, *passive, low range*.
- Primary worries originally about **retail chain** use.


Pacemaker Chip Set

Surveillance via IoT data?

- Like all PD, IoT derived data can be **reused**
- "In 2006, the Guardian reported that police had requested access to the personal information of Oyster customers **243** times, and that access had been granted 229 times. Then in 2008, London's Evening Standard reported that over 3,000 requests had been made in under a year. Since then, **22,000** requests have been made by the Metropolitan Police, according to figures released by London's transport authority in February 2012, with 264 requests made in the first two months of 2012 alone."

.. Can be embarrassing..



Logged Activities

Tue, Feb 2

Select

Activity	Distance	Duration	Cals	Fav
Aerobic step 6 - 8 inch step	N/A	45 minutes	355	
Sexual Activity Passive, light effort, kissing, hugging	N/A	10 minutes	9	
Sexual Activity Active, vigorous effort	N/A	15 minutes	21	
Sitting quietly and watching television	N/A	1 hour	56	
Total	N/A	2 hours 10 minutes	441	

Fitbit users beware: The details of your sexual tryst last night—all vigorous, 15 minutes of it (21 calories burned!)—has probably been broadcast for all the Internet to see.

2. "Ambient environments" and problems for privacy

- Ubiquity = "*invisible and seamlessly adaptive*" (Spiekerman and Pallas) . **Adaptive** – learn from ambient total data collection, data **not forgotten while** useful
- Weiser – weaving themselves "*into the fabric of everyday life until they are indistinguishable from it*"
- Eg ambient temperature control; lighting
- The more useful, **the less obvious** and the **less controlled by individual notice and choice**.

contd

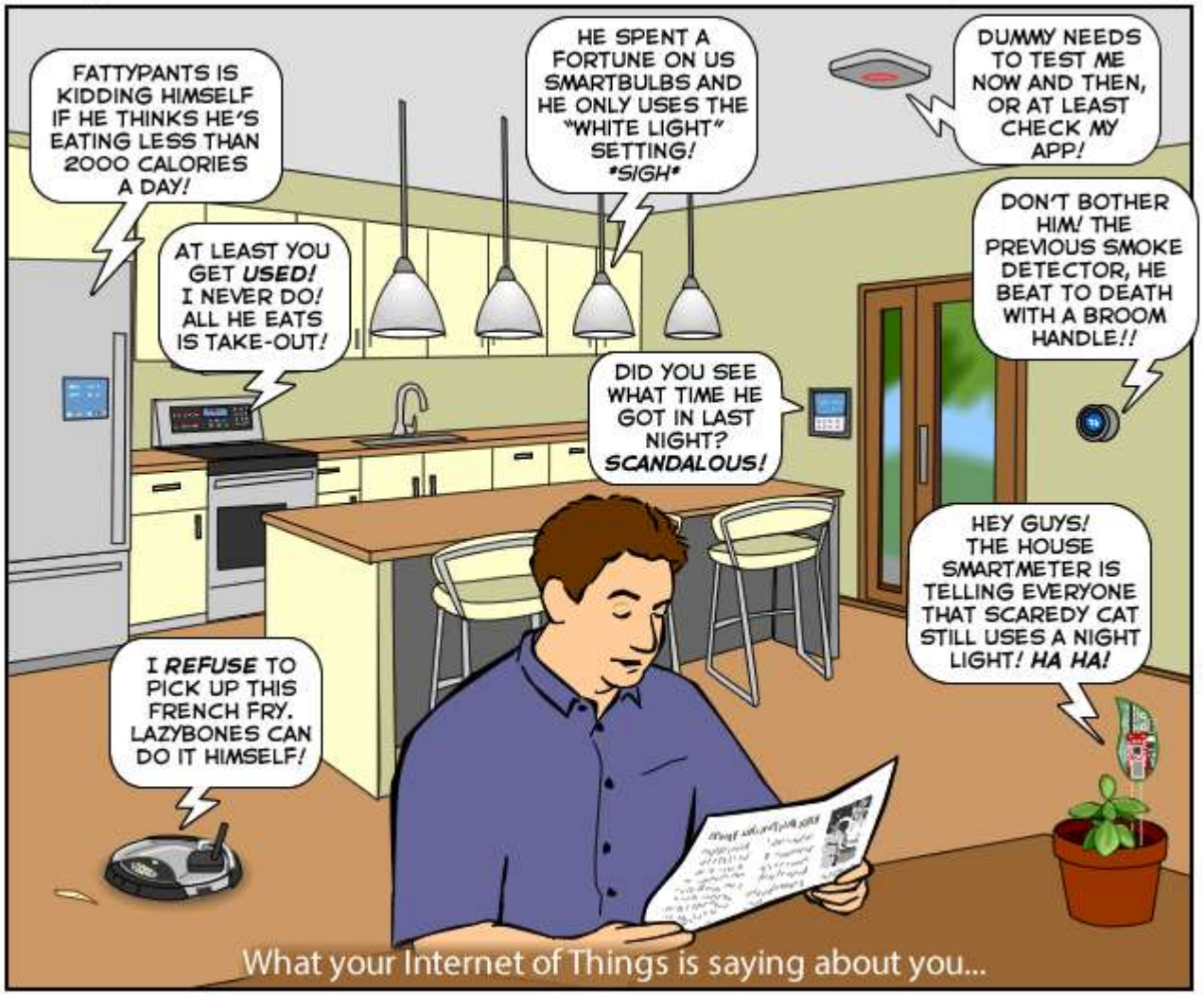
- How can this match DP ideal of privacy as *individual right to prior informed control of collection of data*?
- Problem expands when IoT installed in
  - **public** environments where no choice about sharing data except to entirely reject service– smart roads, smart transport
  - **public/private** environments eg smart malls where footfall measured from mobiles and possibly correlated with IDs via CCTV or credit card billing
  - **Private environments where choice removed** eg when smart meters **mandated** by EU to promote environmental goals?

IoT as 24/7 surveillance? Guardian, 2015

- "We may find ourselves interacting with thousands of little objects around us on a daily basis, each collecting seemingly innocuous bits of data 24/7, information **these things will report to the cloud**, where it will be processed, correlated, and reviewed.
- Your smart watch will reveal your lack of exercise to your health insurance company, your car will tell your insurer of your frequent speeding, and your dustbin will tell your local council that you are not following local recycling regulations. This is the **'internet of stool pigeons'**, and though it may sound far-fetched, it's already happening"

The Joy of Tech™

by Nitrozac & Snaggy



What your Internet of Things is saying about you...

joyoftech.com

From the "Internet of Things" to smart cities

Smart meters

Smart cities – features/gains/problems

- Based around
  - Networks of ***sensors attached to real world features*** (smart homes, roads, meters, telehealth etc) often processing in real time potentially personal data
  - Acquisition and exploitation of "***big data***" acquired via these sources and/or merged with other public and private datasets
  - Massive ***cloud infrastructure*** for such collection, processing, storage – often involving extra EU servers
  - Often financed by public private partnership -> outsourcing of "public" services – surveillance, health, waste? – to private cos along with the [big]data
- Yet – heavily promoted to achieve energy efficiency; sustainability; joined up transport; replacement of private by shared vehicles; waste management; govt, welfare and health savings; etc etc

3. Analysing DP law, consent and the IoT

- Do IoT systems collect "**personal data**"? If so DPD/GDPR applies. But in original conception (RFID chip) collected **location** of **thing**, not person? Do more advanced systems change this?
- DPD art 2 (c) : *"personal data' shall mean any information relating to an identified or identifiable natural person* ('data subject'); an identifiable person is one who can be *identified, directly or indirectly*, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;[unchanged GDPR]
- Many systems will claim either to collect non personal data or to **anonymise** eg O2 collection of location data from users of their system on London underground.
- Increasing ease of **reidentification** however?

If (a) personal data *is* collected via IoT?

Several options for lawful processing (art 7 DPD /art 6 GDPR)

- ***Consent*** of user (freely given, specific, informed, unambiguous and "indication") – v difficult?
  - Data may be gathered and shared with little or no transparency as to purpose of processing etc
  - Consent very difficult to give, IoT systems may not have traditional user interfaces
  - Apps may give opportunity to provide consent but *quality* of consent may be poor (and what if no contractual nexus? Eg smart mall)
  - What if no real poss to refuse sharing data in IoT system without refusing whole service? cf GDPR art 7(4)

.. Alt grounds to consent?

- BUT ALSO - "**Legitimate interests**" of data controller where not overridden by fundamental interests of data controller
- Necc for entering contract
- Necc to carry out task in public interest
- OR assert **anonymisatio**n

But – (b) special rules for location data

- Why?
- Beginning of ubiquity of collection of location data from cellphones then GPS chips in smartphones and other mobile gadgets eg tablets, smart cars etc
- Art 29 WP "*movement patterns of owners.. provide a very intimate insight into the private lives of owners*"
- US FTC 2013: "*mobile devices typically personal to individual, almost always on, and with the user*" -> highly sensitive data
- Cf Public reaction against Google "Glassholes" – essentially peer to peer *equiveillance* – very strongly negative

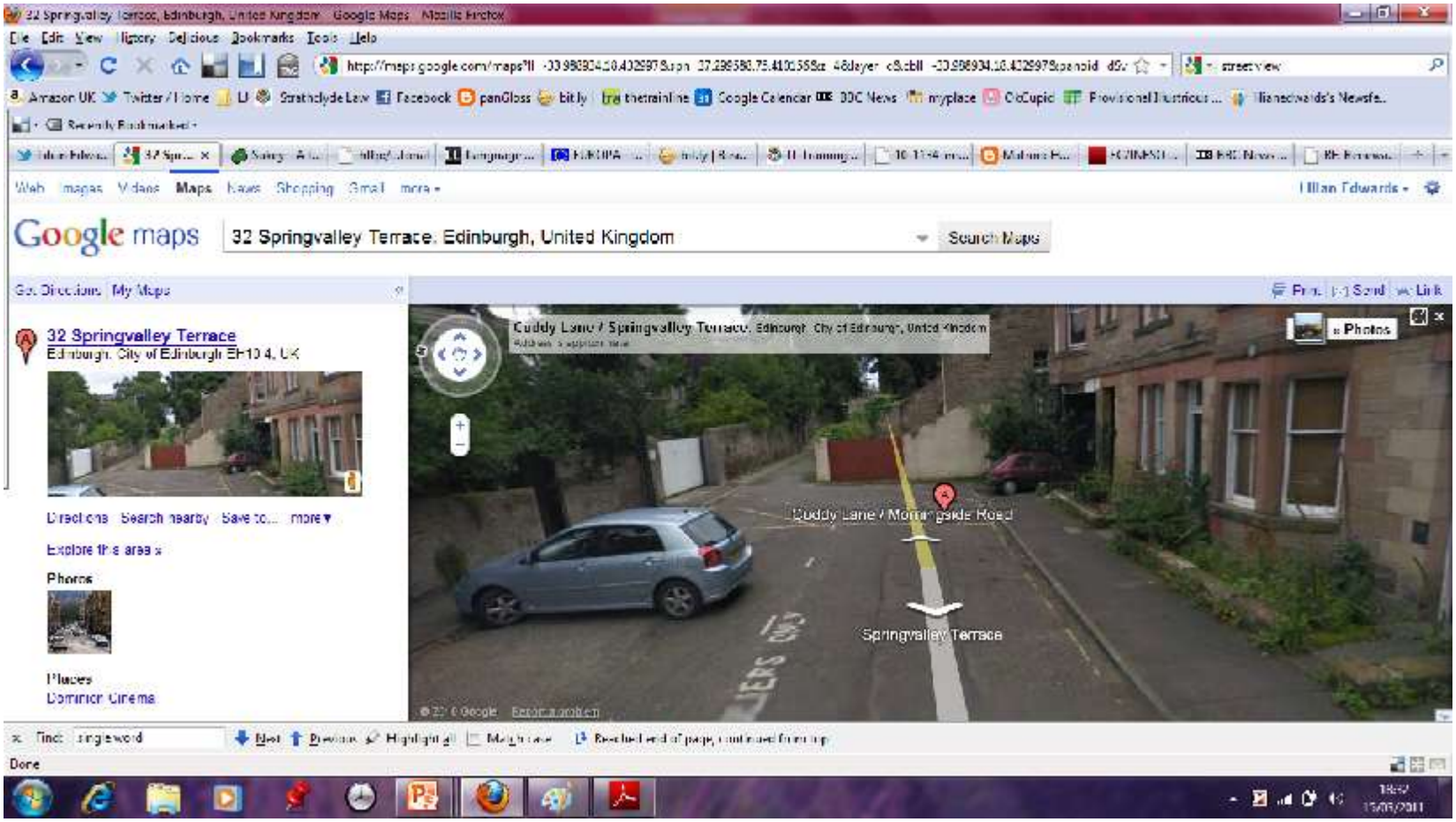
IoT and Location Data

Do IoT systems collect "location data" (LD)?

- e-Privacy Directive 2002/2009 (PECD) Art 2(c) defines location data as:

  "*data processed **in** an electronic communications network or* **by** *an electronic communications service indicating the* geographic position *of the* **terminal equipment of a user** *of a* **publicly available** *electronic communications service"*

Q. When you use Google St View are you processing "location data"?



IoT = Location Data?

- Much early concern if definition matched RFID systems, implying requirements over and above basic DP
  - Are RFID tags the "*terminal equipment*" of user? (Not altered in main text in 2009 – however recital 56 after 2009 *explicitly* applies location and DP regime to RFID chips "and similar")
  - PECD now applies since 2009 reforms to *publicly available* networks or where use is made of "electronic communications services as a basic infrastructure" – most IoT systems now fit this (recital 56)

Location data : art 9 PECD (not revised)

- For the purpose of marketing electronic communications services **or** for the provision of "value added services "
- **..the provider of a publicly available electronic communications service [or someone they authorise] may** process location data to the extent and for the duration necessary for such services or marketing,
- *if the subscriber or user to whom the data relate has given his or /her consent*.. And
- "*prior* to obtaining their consent", **informed** re type of location data other than traffic data which will be processed, purposes and duration of the processing and whether the data will be transmitted to a third party for the purpose of providing the value added service
- Users or subscribers shall be given the possibility to **withdraw** their consent for the processing of traffic data at any time.

(c) Confidentiality and art 5(3), PECD

- Requires consent informed by prior "**clear and comprehensive information**" where
  - "information" is **stored** on "**terminal equipment of a user**"
- Intended to catch cookies or spyware placed on users hard disc or phone
- But how far applicable to IoT sensors eg smart thermostats, energy meters, connected cars?
- "*Storage*"? A29WP argue a Fitbit (eg) is "terminal equipt" where info stored (even though probably quickly transferred to cloud)
- Terminal equipment of "*user*"? Shared autonomous taxi? A connected smart transport system? A smart escalator?

In summary : re IoT and consent

- Basic DP law would probably accept non-consent grounds for processing lawfully eg legitimate interests of data controller
- Some data flows involving IoT sensors *may* be deemed "anonymised" and so exempt from DP or PECD controls.
- Art 9 PECD *may* apply if location data collected by *telco or their authorisee* via the "terminal equipment of a user" and on sufficiently "public" network
- Art 5(3) PECD may apply if information *stored* on terminal equipment user.
- ***If so*****,** prior informed consent needed ,plus ability to opt out afterwards (art 9 PECD) and no substitute grounds allowed
- Can such prior consent be sensibly given and collected in modern pervasive IoT eg smart homes, smart cities?
- More issues – rights to object to automated processing, to delete, subject access rights, RTBF?!

Solutions from Privacy by Design (PbD) and Human Computer Interaction (HCI)?

- *Privacy/DP impact assessments* - for IoT systems, for smart cities as organic whole?
  - 2009-2012 – negotiation of voluntary EU PIA framework for RFID (Spiekkerman). Extended to a PIA for Smart Meters since. Anecdotal low industry take up. But DPIAs will be mandated by GDPR..
- New *semi automated ways of giving consent* eg home dashboards; "pre" or "sticky" consent (consent by autonomous agents)
- New types of transparency eg *privacy icons*? EU RFID icon
- Greater *algorithmic transparency* inc extension of right now in GDPR (ex DPD art 12(a))

For more information --

- Edwards “Privacy, Security and Data Protection in Smart Cities: A Critical EU Law Perspective” (2016) European Data Protection Law Review 28-58