

Data Privacy, Data Sharing and the Internet of Things

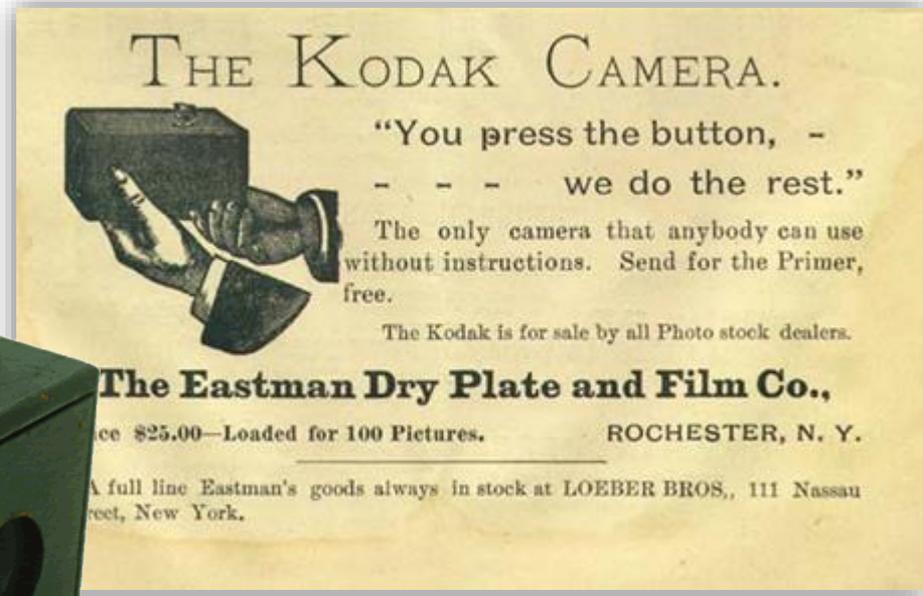
Jonathan Porter
Chief Economist's Team - Ofcom

UAE CCP Summer Conference - 19th June 2015

Topics

- The economics of personal data and data privacy
- Practical issues with informed consent in an on-line world
- Some potential implications for Ofcom's work on "The Internet of Things"

This is not the first time that advances in technology have led to privacy concerns...



The Economics of Privacy

Key economic features:

- The market for personal data and market for privacy can be thought of as two sides of the same coin leading to different trade-offs between costs and benefits.⁽¹⁾
- Also positive/negative externalities from data creation and transmission.

Consumers

- Want to avoid the negative consequences of privacy intrusions (spam, identity theft etc)
- But benefit from sharing their data more widely – reduced search costs:
 - More targeted product offerings, discounts etc;
 - Recommendations based on purchasing history;
- Consumers also benefit from *other* people sharing purchasing information
 - Reviews of movies, products, hotels, restaurants etc.

Firms

- As data users, benefit from access to more detailed information on consumer preferences, shopping habits, credit histories, as well as information to improve product quality.
- As intermediaries: gathering, aggregating, analysing, buying and selling consumer data.

(1) Following Acquisti: “*The Economics of Personal Data and the Economics of Privacy.*” Background Paper No.3. OECD Roundtable 2010.

Markets for personal data/Markets for privacy

- The work of the CMA highlights that there are already multiple markets in which personal data is being traded
- But it can be difficult for data subjects to participate in these markets, indeed they may not even be aware that their personal information is being traded.
- “If you’re not paying for the product – you are the product”

There is also scope for market failures other than as a result of market power:

- Information Asymmetries:
 - Consumers typically have little knowledge or understanding how their data will be used by the firm *before or after* transacting or indeed how it might be shared with 3rd parties.
- The Privacy “Paradox”
- Other behavioural biases, including: .
 - Loss aversion/endowment effects/self-control;
 - Myopia/over-confidence
- Externalities/network effects - e.g. social media sites
- Terms may be non-negotiable i.e. no choice but to accept

Informed Consent

- Informed consent is a key concept that has underpinned the legal framework for personal data processing in the context of data protection
- Informed consent plays a central role within the requirements for the processing of personal data set by the European Data Protection Directive.
- In the on-line world it is required for:
 - Placing cookies (and similar tracking devices)
 - Collection and processing of personal data
- However, informed consent is not always required as collection and processing of personal data can be based on another legal basis
 - If fulfilment of a service requires processing of personal data, consent is not (always) needed:
 - e.g. processing of address data to deliver magazine subscription
- There is an on-going debate as to whether *not* changing browser settings constitutes informed consent in relation to accepting “cookies”

Informed Consent in Practice

(1) Do consumers read privacy policies?

➤ Why not?

- Clicking-without-reading: the online equivalent of “not reading the small print”
- Opportunity costs are high:
 - Costs associated with reading Ts & Cs versus
 - Time actually spent on any one website.
- Overconfidence: what could go wrong?

(2) Do consumers understand?

➤ Why not?

- Legal jargon and “readability”
- Misinterpret what is meant by “privacy policy”
- Difficult to understand the consequences of their actions.

(3) Can consumers actually do anything about privacy policies?

➤ Why not?

- Limited scope to act: “take it or leave it”, browse-wrap contracts etc
- New technology means profiling/tracking is difficult to avoid
 - Device fingerprinting

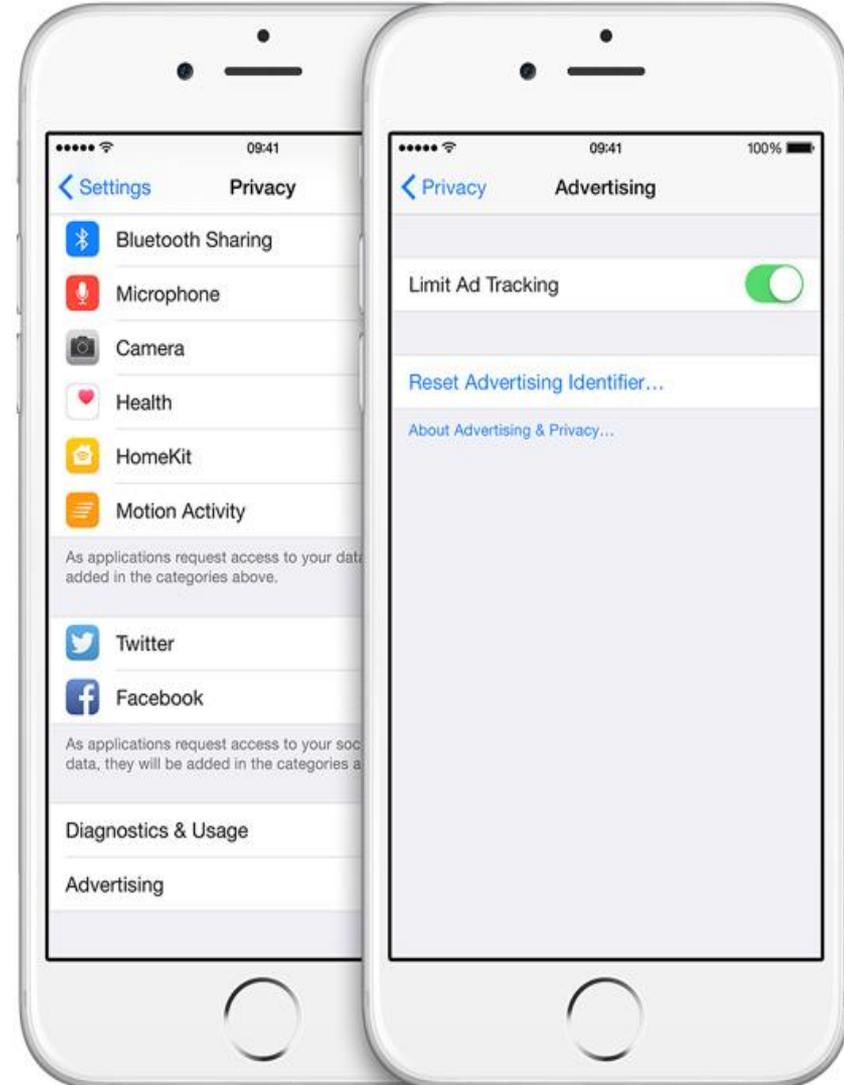
A quick straw poll?

- How many here have an iPhone?
- How many are aware that you can block ads from 3rd parties?

If you'd rather not see mobile ads tailored to your interests, you can choose to Limit Ad Tracking with a simple on/off switch. When Limit Ad Tracking is turned on, third-party apps are forbidden by Apple's guidelines from using the Advertising Identifier to serve you targeted ads. As part of submission to our App Store, Apple requires all developers to agree to abide by your choice to Limit Ad Tracking.

[Apple website accessed on 16th June 2015]

- So, how many of you have actually used
- the "Limit Ad tracking" function?



No “silver bullet” but lots of promising ideas

How might we improve readership/understanding?

- Software tools: browser add-ons
 - Extracting and condensing the most important parts of privacy policies into a reader-friendly format or ratings system.
- Different Formats
 - “Layering” of policies/standardising formats
- Visual prompts: Privacy Seals and Privacy Labels
- “Smarter” notifications
 - Personalised information based on different levels of knowledge (“KIPP”)
- Just-in-time “nudges”: pop-ups with information (and consent buttons)

How might we improve the chance that consumers act upon information?

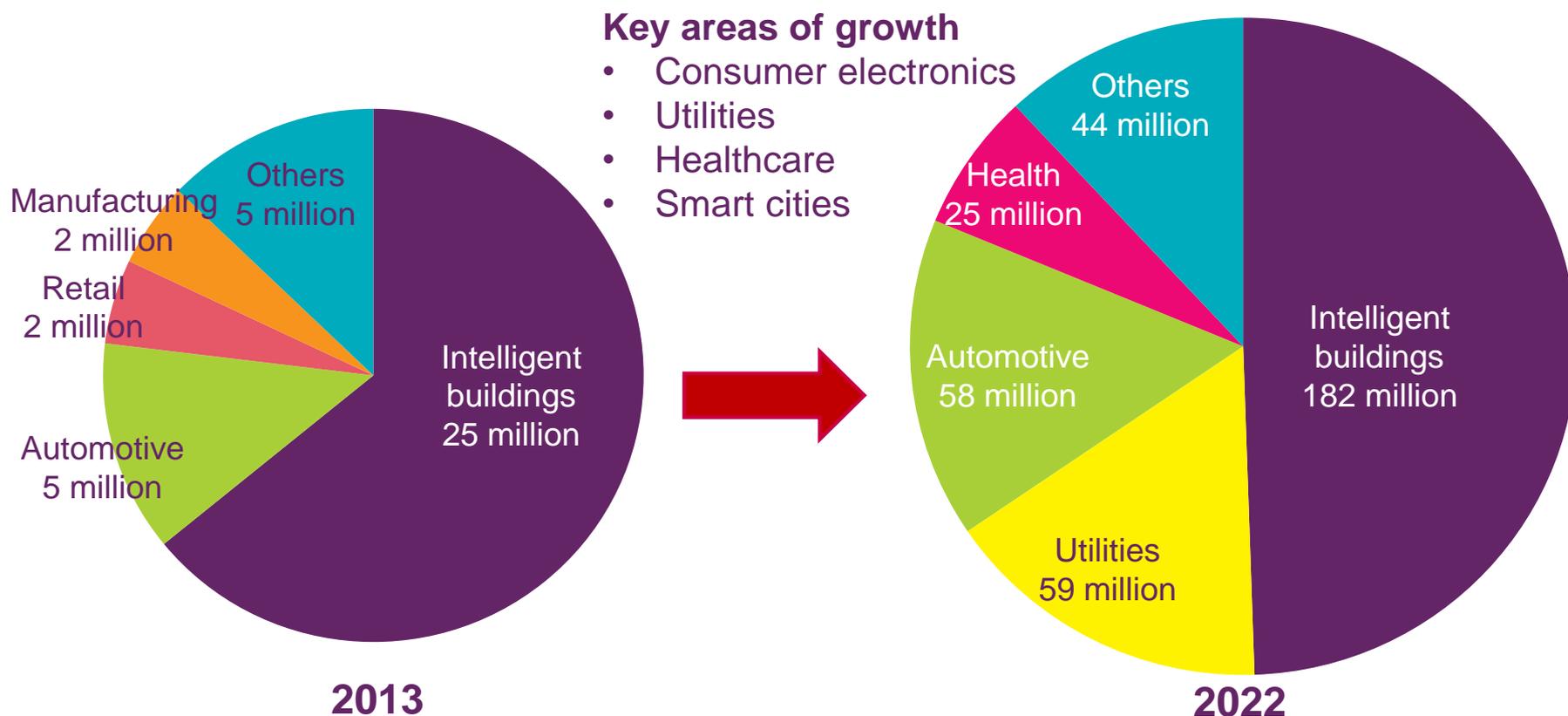
- Building awareness to increase engagement

Key Messages

- Effective communication: a process rather than a one-off act
- Privacy is a fluid concept – has changed and will change over time.

The IoT is diverse, growing rapidly, and expected to deliver substantial economic benefits

Numbers of Connected devices



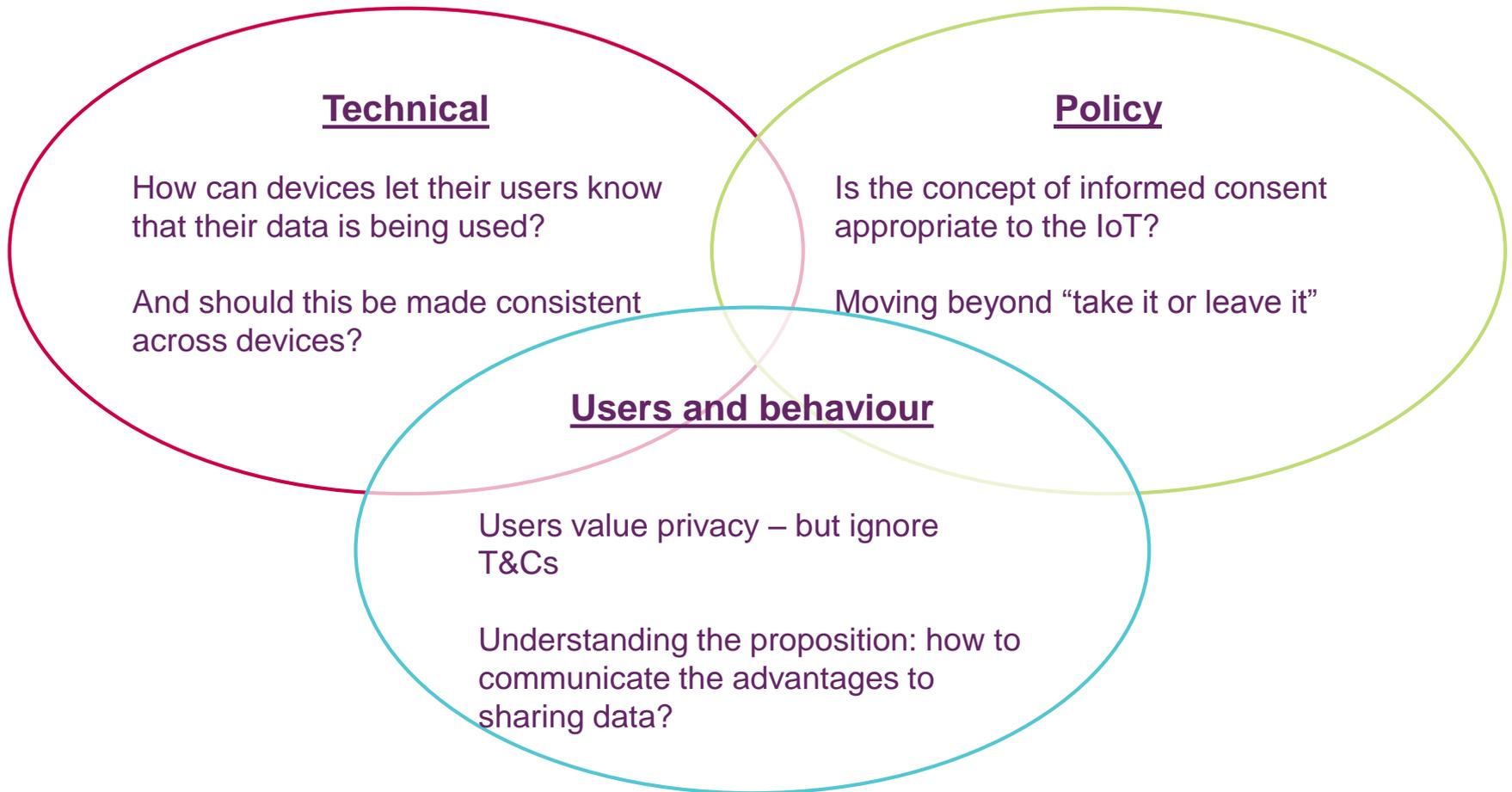
But it will make things more complicated



The Internet of Things is likely to aggravate the issues around informed consent

- More devices, more data
 - More contracts about different types of personal data usage will be necessary
 - Interaction between devices becomes more sophisticated and complex
- More subtle/sophisticated data collection, aggregation and analysis will be possible
 - Benefits from more seamless tracking across all aspects of day to day life
- But at the same time it increases the challenges:
 - Contracts may need to become more complex
 - Even less consumer awareness about data usage practices
 - Consumers may not even be aware that a specific device is connected to the Internet
- Some of promising solutions may not work so well for the Internet of Things
 - No displays
 - Possibly little direct human interaction means that “nudges” may not work as well.
- Building awareness likely to be key

Part of the challenge will be managing the different dimensions to the issue of data privacy



“Personal Data and Data Privacy” by WIK Consult

Available at:

<http://stakeholders.ofcom.org.uk/internet/personal-data-and-privacy/>