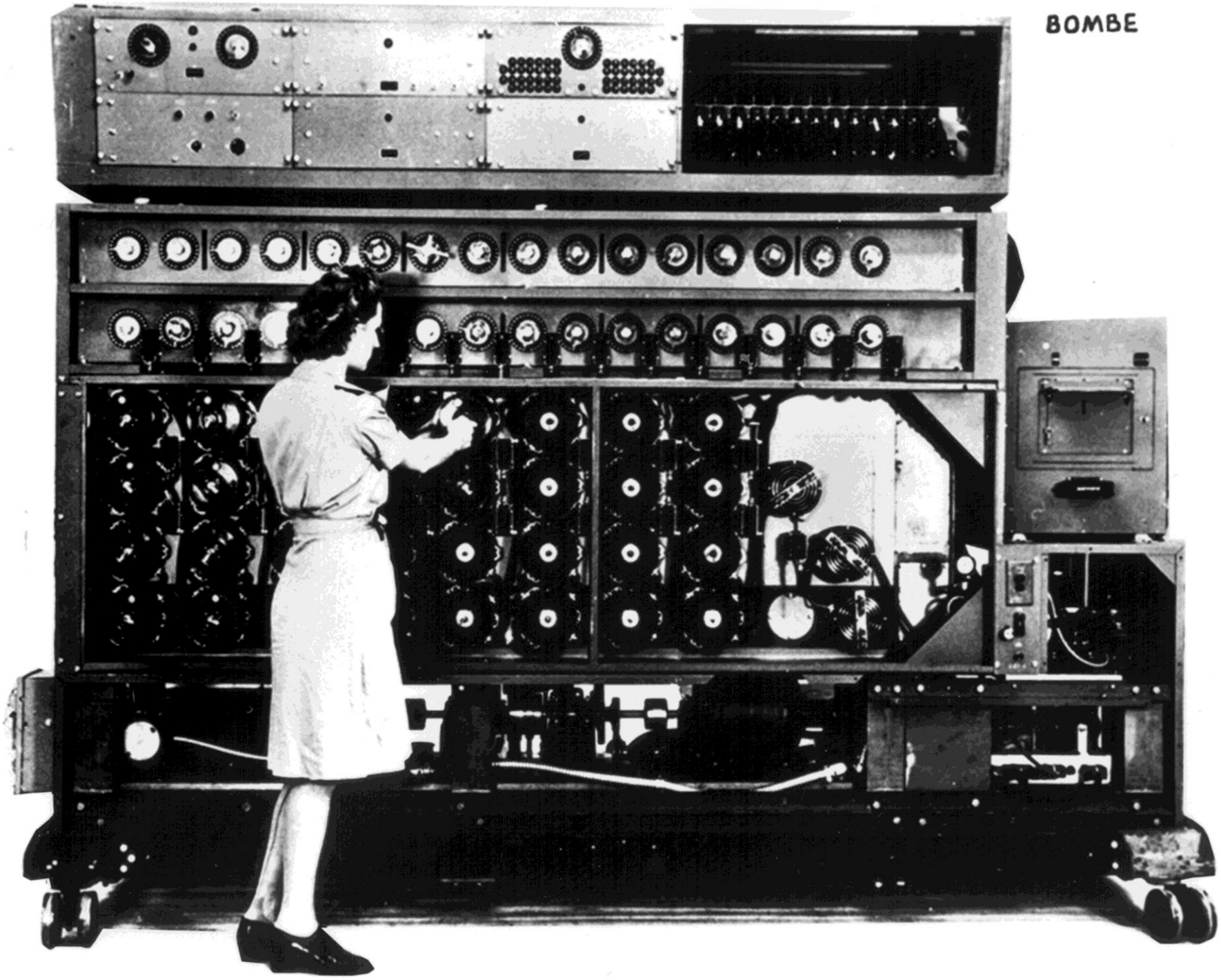
Privacy in a hyper-connected society

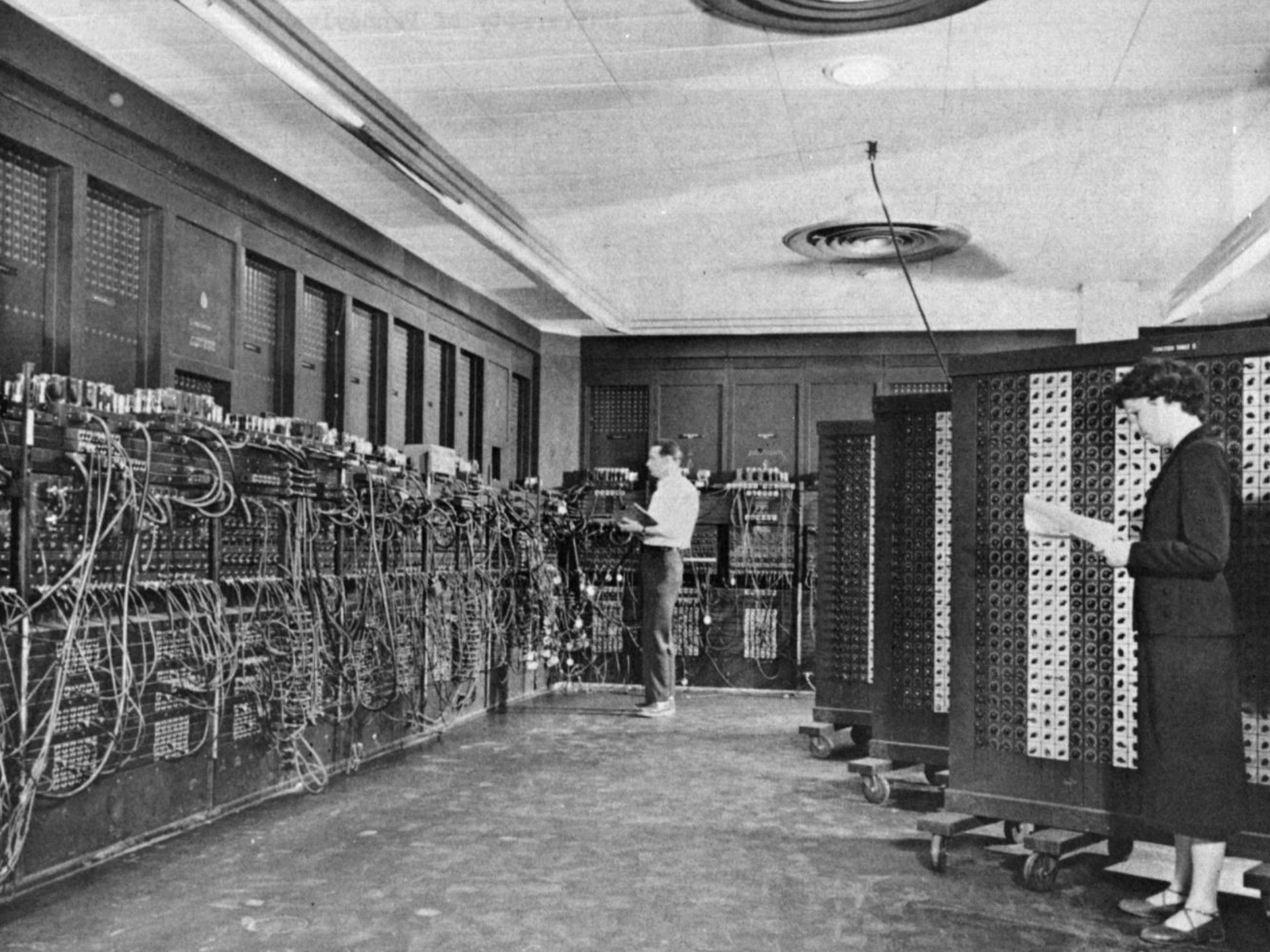
Prof. Ian Brown

Senior Research Fellow & Assoc. Professor, Oxford Internet Institute

Overview

1. **Challenges to privacy**
   1. **Technological development**
   2. **Market failure**
   3. **Authorised access**
2. Designing for privacy
3. Shaping technologies for the public good


BOMBE

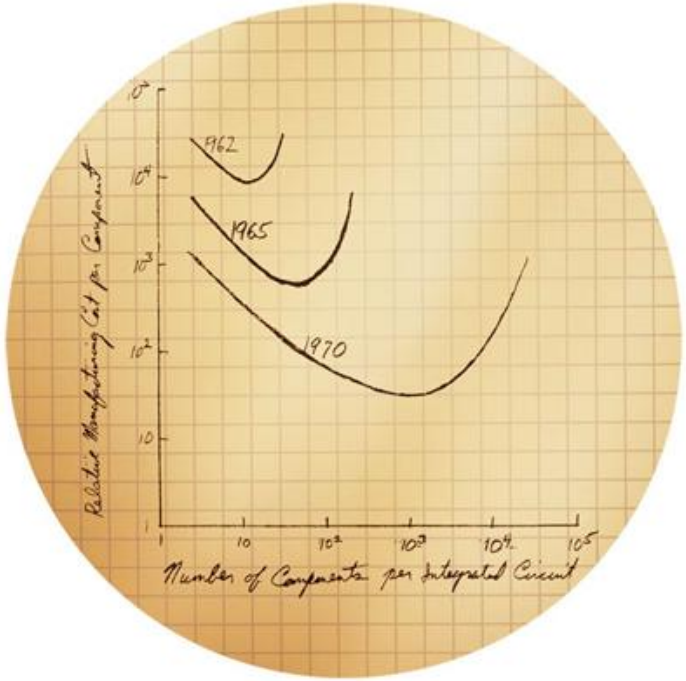



BRITISH BROADCASTING CORPORATION
MICROCOMPUTER SYSTEM
f0 f1 f2 f3 f4 f5 f6 f7 f8 f9
BREAK
ESCAPE
TAB
CAPS LOCK
CTRL
SHIFT LOCK
SHIFT
RETURN
SHIFT
DELETE
COPY
cassette motor
caps lock
shift lock

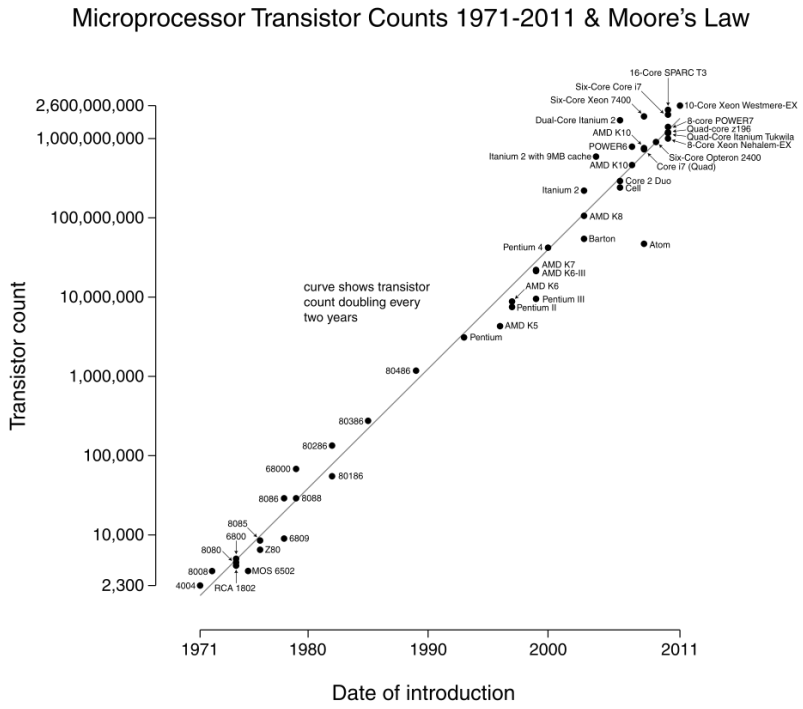
Kelvinsong/Wikimedia


Loic Le Meur

Moore's law



Gordon Moore (1964) Image courtesy of Computer History Museum



Google Research (2011)

Market failures

- Information asymmetry – data gathered ubiquitously and invisibly in a way few understand
  - Privacy policies unreadable and difficult to verify/enforce
- Most individuals bad at immediate benefit v deferred, uncertain cost decisions
  - Privacy risks are highly probabilistic, cumulative, and difficult to calculate
- Information industries highly concentrated

Brown (2014)

Commercial Big Brother

- Internet replaces broadcast TV, as a largely commercial channel for entertainment, retailing and advertising
- High-speed access is built to the home only with govt. subsidy and removal of regulatory constraints, strengthening large ISP dominance
- Immersive, interactive video content consumes most user time and 95% of bandwidth. Access is mainly through DRM-heavy proprietary hardware
- Merged ISPs/search engines/social networking sites offer walled gardens featuring high-quality access to video content and interactive services. They slowly merge with major entertainment conglomerates, with close links to retailers

Commercial Big Brother

- Tacit cooperation between governments and the providers of the new "opiate of the masses", who block access to politically controversial content. Internet becomes increasingly fragmented and nationalised
- Users are intensively profiled to support targeted advertising, with no effective global privacy regulation
- Security concerns used to justify lock-down of network, with e-ID requirements severely restricting anonymous speech and data retention laws squeezing user privacy

Insider threats

Information required	Price paid to 'blagger'	Price charged
Occupant search	not known	£17.50
Telephone reverse trace	£40	£75
Friends and Family	£60 – £80	not known
Vehicle check at DVLA	£70	£150 – £200
Criminal records check	not known	£500
Locating a named person	not known	£60
Ex-directory search	£40	£65 – £75
Mobile phone account	not known	£750
Licence check	not known	£250

"What price privacy?", Information Commissioner's Office (2006)

(TS//SI//NF) FAA702 Operations

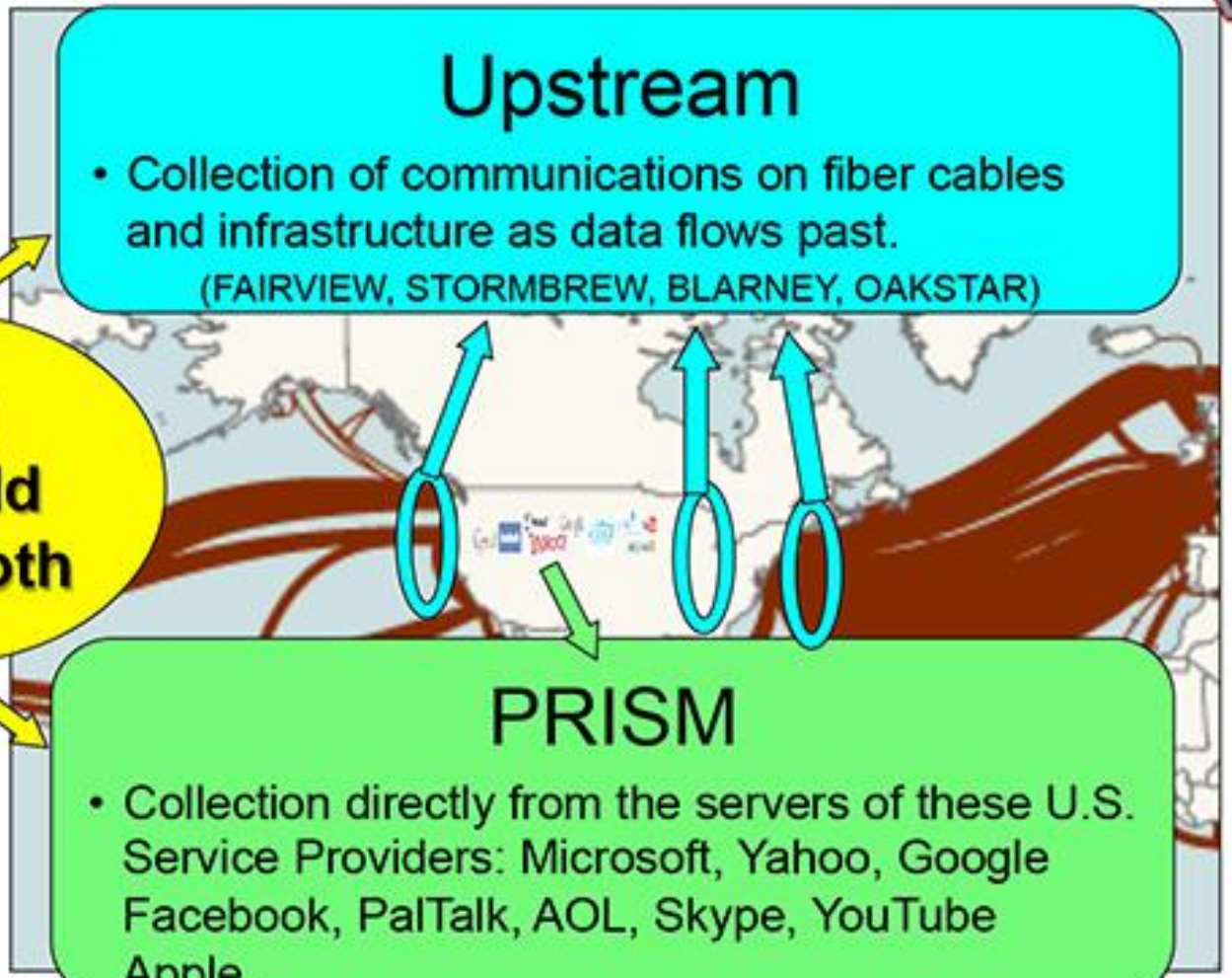
Two Types of Collection

Upstream

- Collection of communications on fiber cables and infrastructure as data flows past.

(FAIRVIEW, STORMBREW, BLARNEY, OAKSTAR)

You Should Use Both



PRISM

- Collection directly from the servers of these U.S. Service Providers: Microsoft, Yahoo, Google Facebook, PalTalk, AOL, Skype, YouTube Apple.

Overview

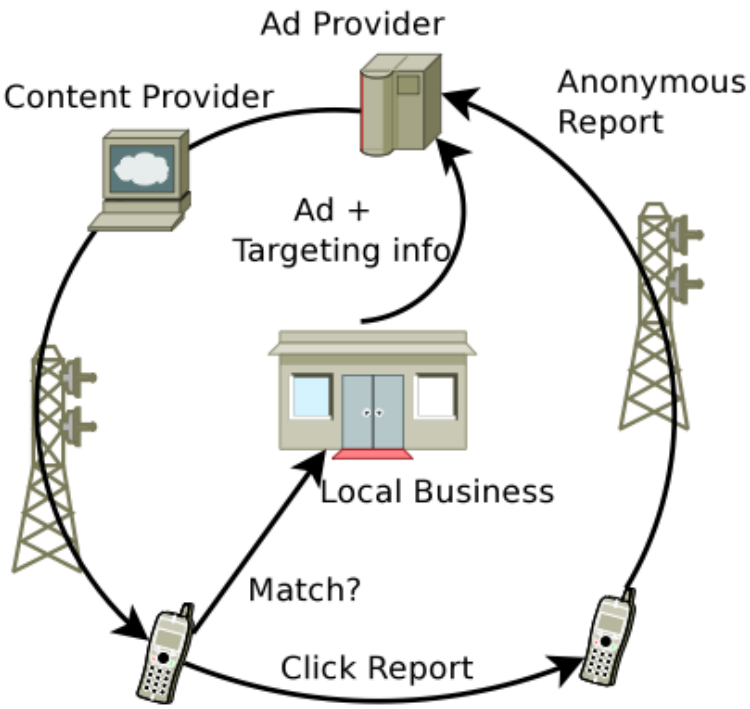
1. Challenges to privacy
2. **Designing for privacy**
    1. **Principles**
    2. **Targeted advertising**
    3. **Smart meters**
    4. **Congestion charging**
3. Shaping technologies for the public good

Designing for privacy

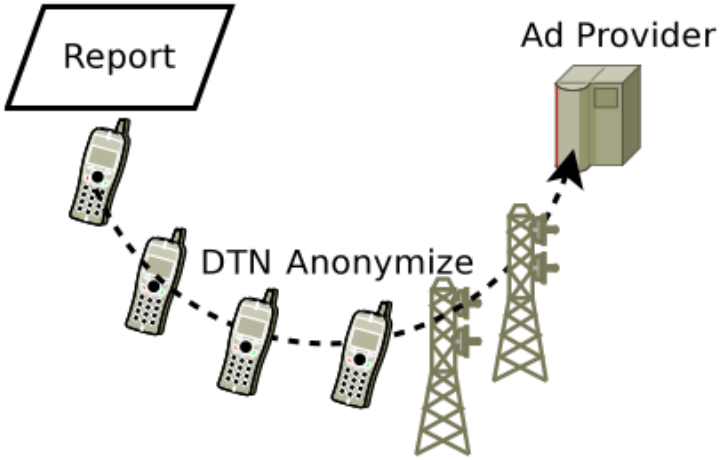
- Data **minimisation** key: is your personal data really necessary? Limit & decentralise personal data collection, storage, access and usage – enforced using cryptography
  - Protects against hackers, corrupt insiders, and function creep
- Users should also be **notified** and **consent** to the processing of data – easy-to-use interfaces are critical. What are defaults?

Jedrzejczyk et al. (2010)

Location-based services

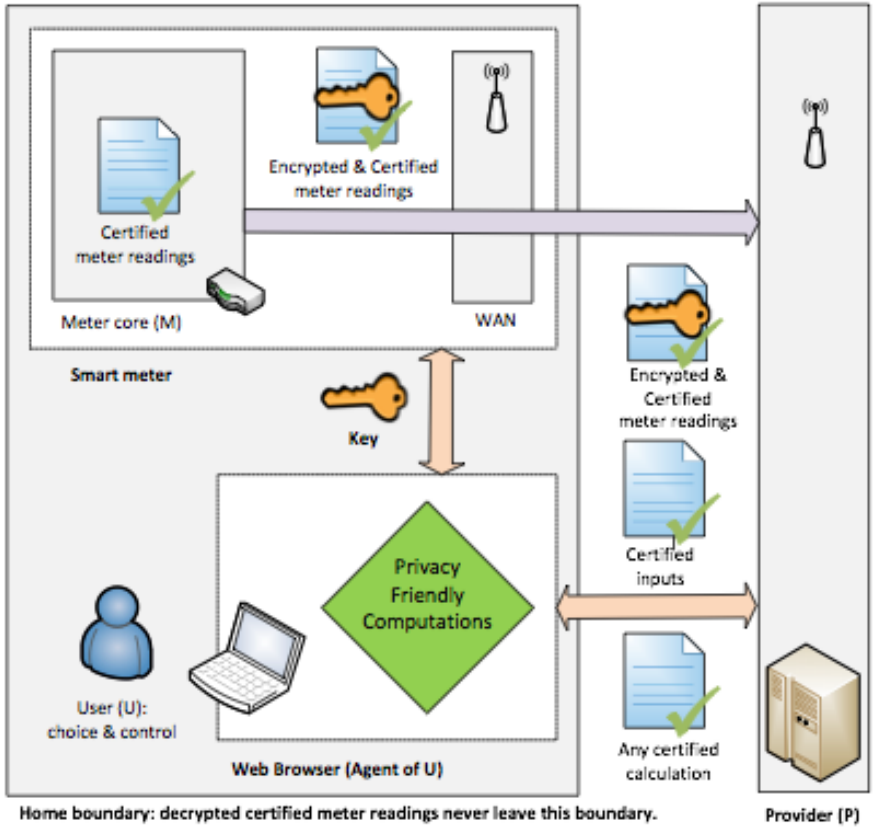


- Can we use features of mobile phone networks to supply anonymous, targeted adverts?



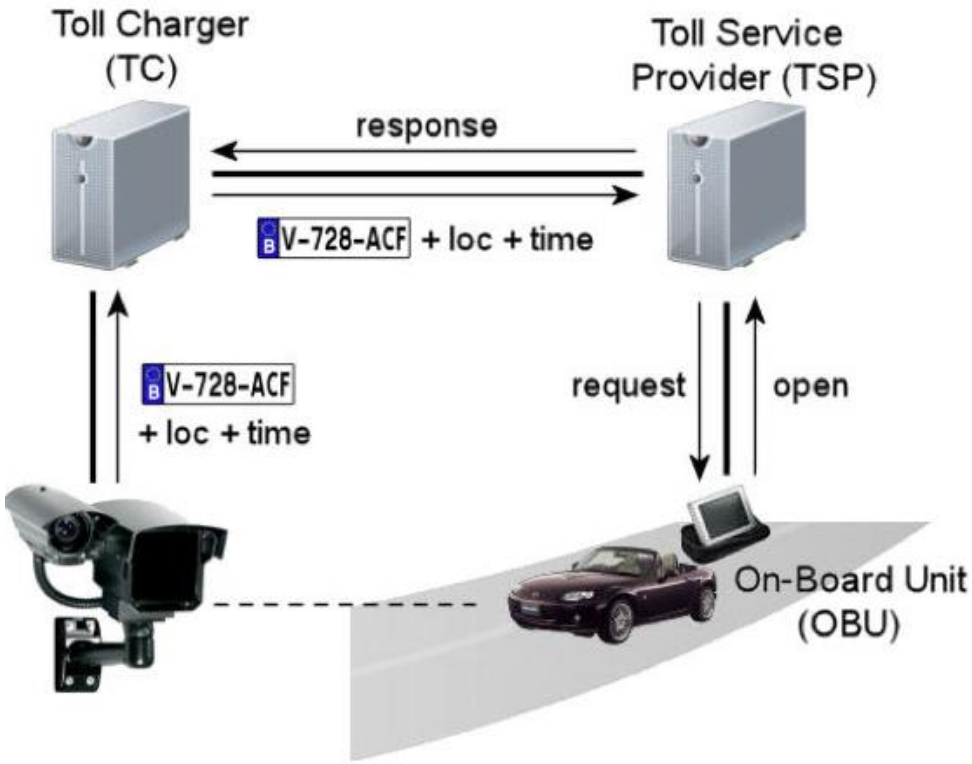
Haddadi, Hui, Henderson and Brown (2011)

Privacy-friendly smart meters



Rial and Danezis (2011)

Congestion pricing

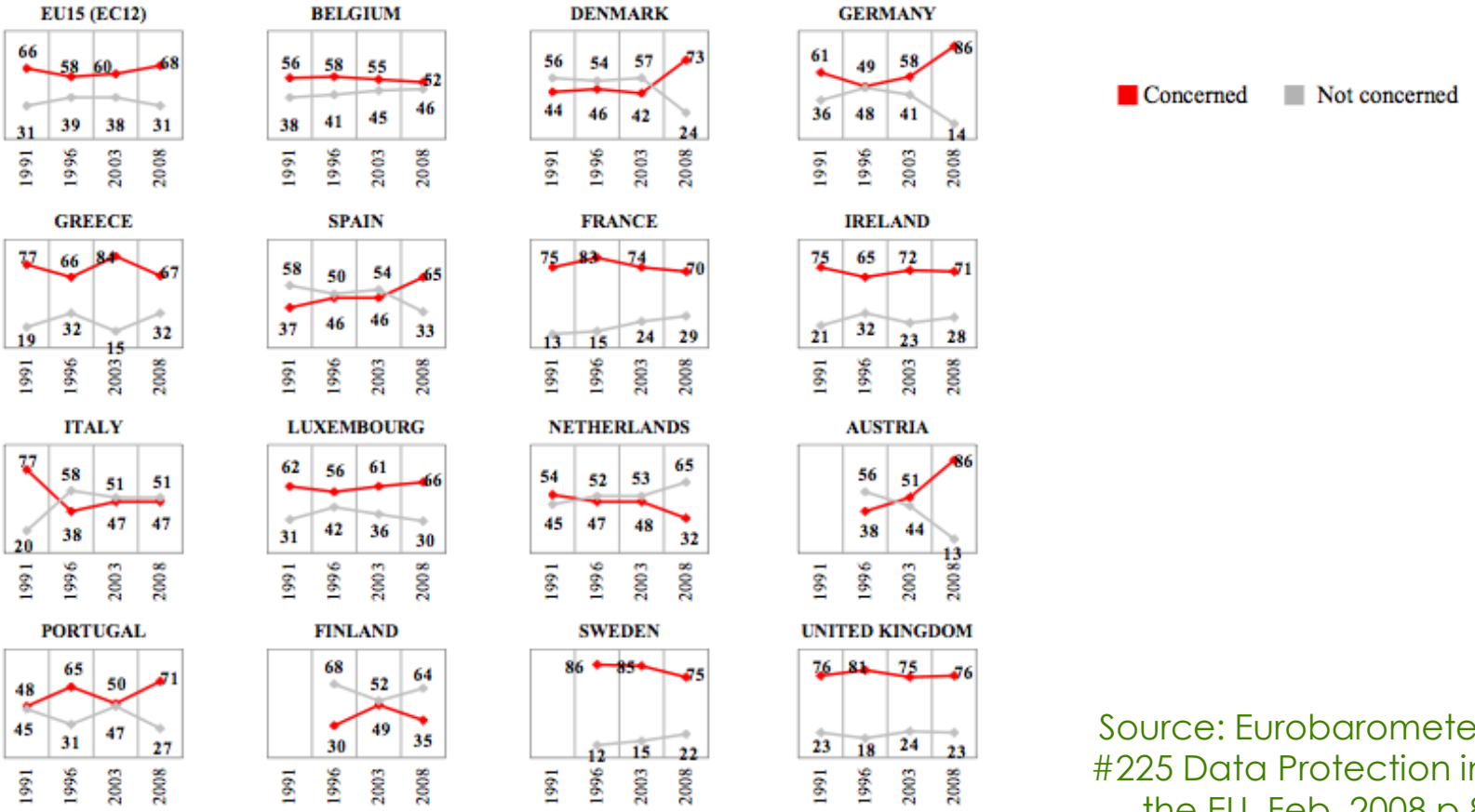


Source: Balasch et al. (2010) p.3

Overview

1. Challenges to privacy
2. Designing for privacy
3. **Shaping technologies for the public good**
    1. **Defining the public good**
    2. **Limits on government surveillance**
    3. **The General Data Protection Regulation**
    4. **Encouraging competition**

EU data privacy concerns



Source: Eurobarometer #225 Data Protection in the EU, Feb. 2008 p.8

Constitutional protections

ECHR, 1950

Reaffirming their profound belief in those fundamental freedoms which are the foundation of justice and peace in the world…

§8 Everyone has the right to respect for his private and family life, his home and his correspondence

§9 Everyone has the right to freedom of thought, conscience and religion

§10 Everyone has the right to freedom of expression

§11 Everyone has the right to freedom of peaceful assembly and to freedom of association with others

US Bill of Rights, ratified 1791

…extending the ground of public confidence in the Government, will best insure the beneficent ends of its institution…

I: Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble

IV: The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated

Bulk vs. targeted surveillance

- President Obama's NSA Review Panel :

  "Although we might be safer if the government had ready access to a massive storehouse of information about every detail of our lives, the impact of such a program on the quality of life and on individual freedom would simply be too great… We recommend that the US Government should examine the feasibility of creating software that would allow the National Security Agency and other intelligence agencies more easily to conduct targeted information acquisition rather than bulk-data collection."

- Deputy Prime Minister, 4 Mar 2014 :

  "[O]ur current framework assumes that the collection of bulk data is uncontroversial as long as arrangements for accessing it are suitably stringent. I don't accept that... [S]trong access controls are vital to prevent employees from going on 'fishing expeditions' once a store of data exists. But the case for collection itself has to be made, not assumed."

GDPR Art. 23 Data protection by design and by default

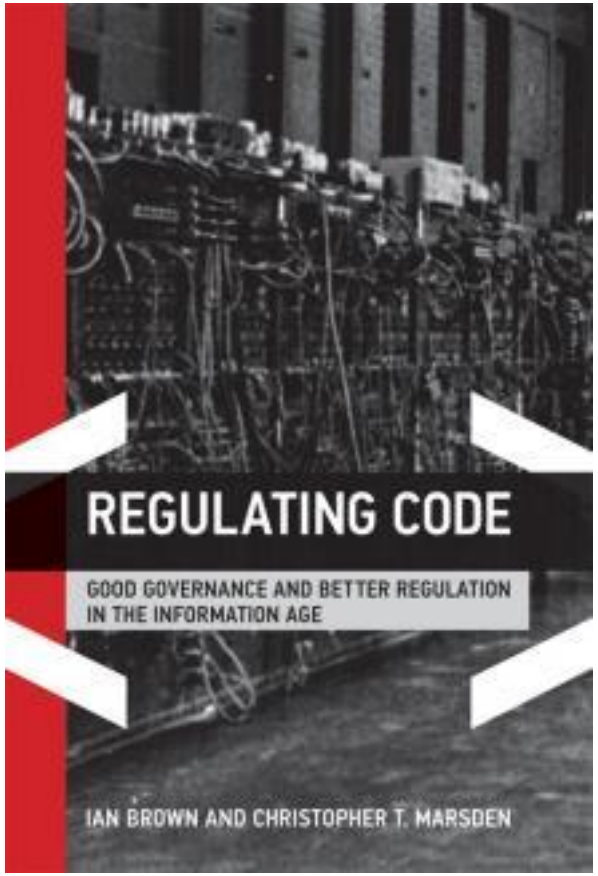
1. …the controller… shall…implement **appropriate and proportionate technical and organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation** and ensure the protection of the rights of the data subject… data protection by design shall be a prerequisite for **public procurement** tenders… [and] procurement by entities operating in the **water, energy, transport and postal services** sector

2. The controller shall ensure that, **by default, only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected, retained or disseminated beyond the minimum necessary for those purposes**, both in terms of the amount of the data and the time of their storage. In particular, those mechanisms shall ensure that **by default personal data are not made accessible to an indefinite number of individuals** and that data subjects are able to **control the distribution** of their personal data.

See Korff & Brown (2010)

Interoperability requirements

- Data portability may reduce switching costs, but network effects will still act as a barrier to entry
- Vertical integration could limit consumer choice
- To minimise network barriers, competition authorities *could* impose *ex ante* interoperability requirements:
  - upon dominant social utilities
  - between vertically integrated value chains



Conclusion

- Technology developments can have a significant social impact – societies can shape the values technologies embed if they wish (Brown, Clark & Trossen 2010)
- Privacy-protective technologies have been developed for a range of applications – how do we persuade companies and governments to use them?
- These are questions not just for computer scientists, but also lawyers, economists, sociologists – and citizens and their representatives

SEVENTH FRAMEWORK PROGRAMME

INTERNET-SCIENCE.EU

References

J. Balasch, A. Rial, C. Troncoso, C. Geuens, B. Preneel, and I. Verbauwhede (2010) PrETP: Privacy-Preserving Electronic Toll Pricing, In Proceedings of the 19th Usenix Security Symposium, pp. 63-78

I. Brown (2014) The economics of privacy, data protection and surveillance. In J.M. Bauer and M. Latzer (eds.) *Research Handbook on the Economics of the Internet*. Cheltenham: Edward Elgar

I. Brown, D. Clark and D. Trossen (2010) Should Specific Values Be Embedded In The Internet Architecture? *Re-Architecting the Internet*

I. Brown and C. Marsden (2013) *Regulating Code: Good Governance and Better* Regulation *in the Information Age*. Cambridge, MA: MIT Press.

I. Brown, C. Buckley and D. Harris (2014) *Data Protection: Redress mechanisms and their use in the UK*. EU Fundamental Rights Agency

L. Jedrzejczyk, B. A. Price, A. K. Bandara and B. Nuseibeh (2010) On The Impact of Real-Time Feedback on Users' Behaviour in Mobile Location-Sharing Applications, *Symposium on Usable Privacy and Security*, Redmond

H. Haddadi, P. Hui and I. Brown (2010) MobiAd: Private and Scalable Mobile Advertising, *ACM International Workshop on Mobility in the Evolving Internet Architecture*, Chicago)

D. Korff and I. Brown (2010) *New Challenges to Data Protection.* European Commission DG Freedom, Security and Justice.

A. McDonald and L.F. Cranor (2008) The Cost of Reading Privacy Policies. I/S 4 p.543