Privacy by design

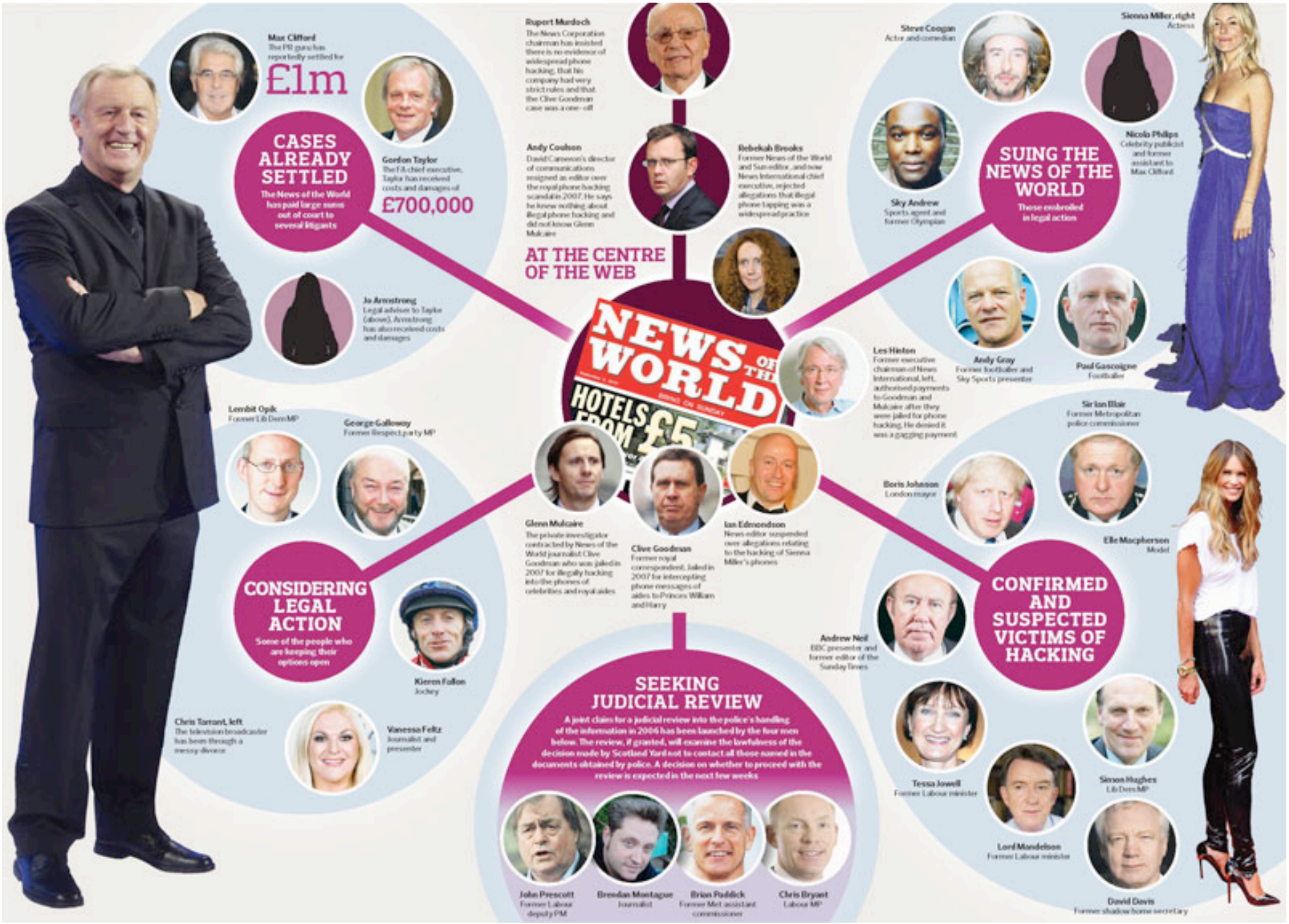
Dr Ian Brown, Oxford Internet Institute

Overview

- What is privacy by design?
- Privacy principles in sensor networks
- Privacy-friendly smart grids

Privacy

- "the right to be let alone – the most comprehensive of rights, and the right most valued by civilized men." – Supreme Court Justice Louis Brandeis, *Olmstead v US* 277 US 478 (1928)
- "A free and democratic society requires respect for the autonomy of individuals, and limits on the power of both state and private organisations to intrude on that autonomy... Privacy is a key value which underpins human dignity and other key values such as freedom of association and freedom of speech" –Australian Privacy Charter (1994)



Source: *The Guardian*, 16 January 2011

Privacy ≠ security

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)

Data protection instruments

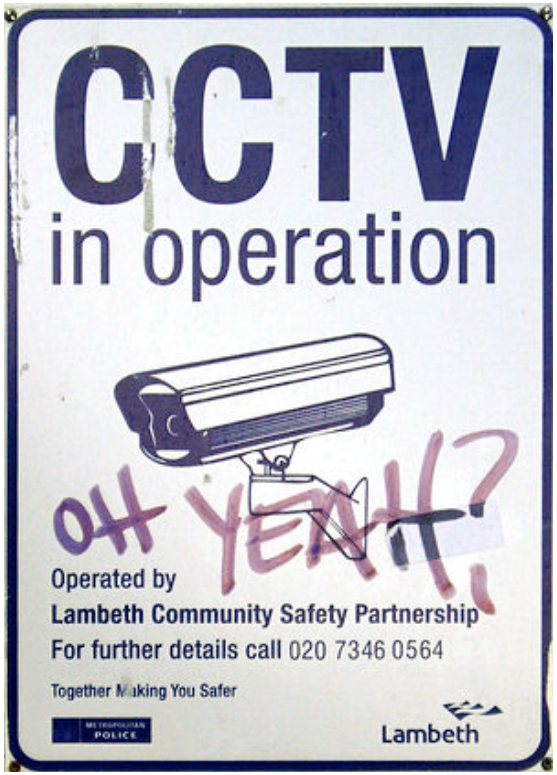
- OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980)
- Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981)
- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
- Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector
- EU Charter of Fundamental Rights (2007)

Privacy by design

- "businesses must use their power of innovation to improve the protection of privacy and personal data from the very beginning of the development cycle… Privacy by Design will lead to better protection for individuals, as well as to trust and confidence in new services and products" –EU Justice Commissioner, Viviane Reding
- "The quantity of personal data collected and processed can be very significantly affected by details decided long before system architects and programmers start building new database applications." (Korff and Brown, 2010)

Designing for privacy

- Data **minimisation** key: is your personal data really necessary? Limit personal data collection, storage, access and usage
- Users must also be **notified** and **consent** to the processing of data – user interfaces?
- §3(3) 1995/5/EC: "the Commission may decide that apparatus … shall be so constructed that: … it incorporates safeguards to ensure that the personal data and privacy of the user and of the subscriber are protected"



Ade Rowbotham (2005)

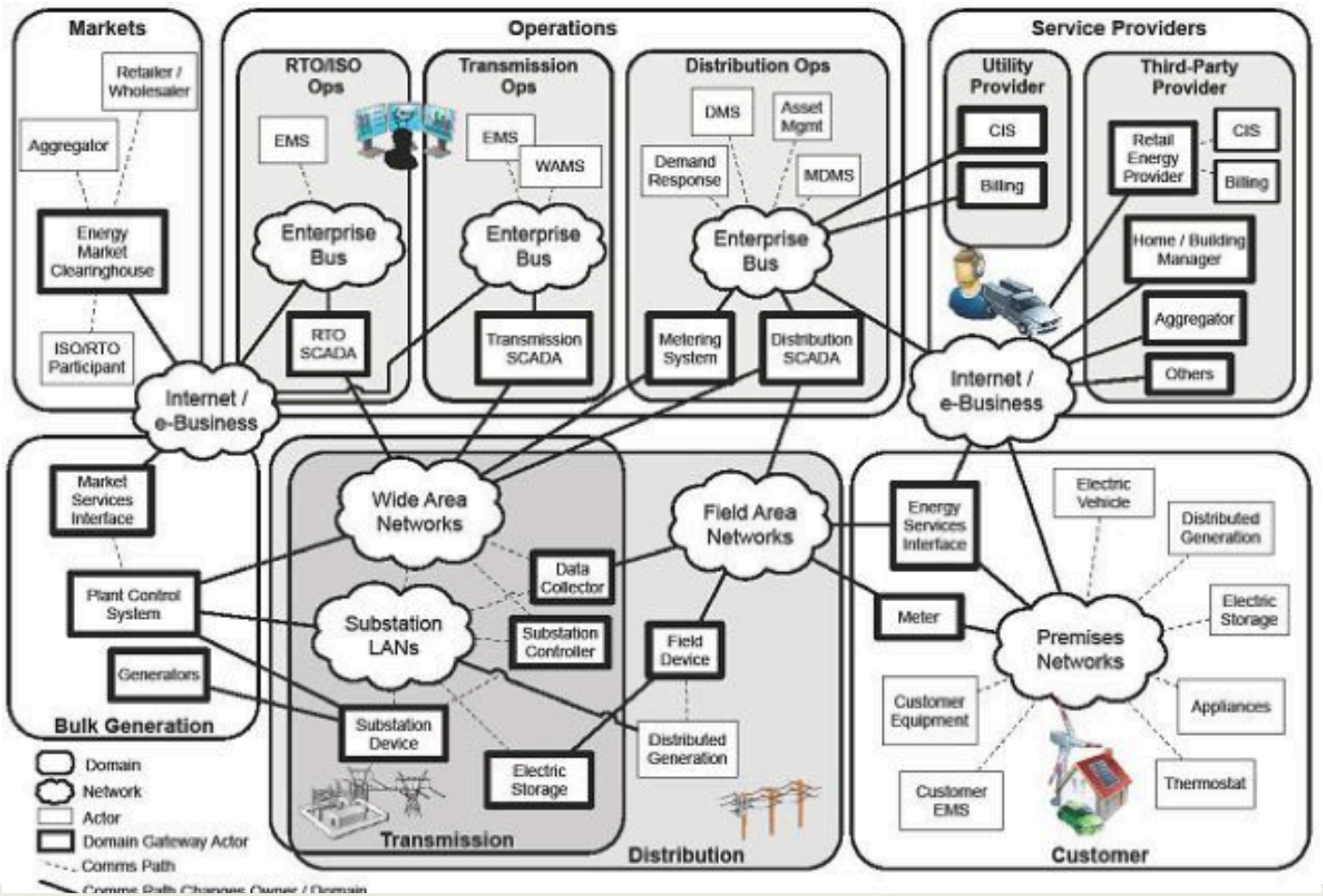
Mobile data

- Is communication uni- or bi-directional or broadcast? Oblivious transfer, MobiAd
- Does sensor, user agent or network carry out triangulation and processing? What resolution data can network access?
- How long-lived and linkable are identifiers? IMSIs, TMSIs and location patterns

Sensor mix networks

- Restricted Mix Networks in DTNs (Wright and Brown, 2010)
  - Network-wide routing is infeasible; isolated network partitions may still provide opportunistic mixing amongst local networks.
  - As messages enter zones, local mixing within the local network.
  - Local communication gateways can still act as powerful attackers against local network.
- Can we use encrypted broadcast to further conceal path of messages?

Privacy-friendly smart grids



NIST conceptual model

Information revealed by meters

- When are you usually away from home?
- Is your household protected with an electronic alarm system? How often do you arm it?
- How often do you arrive home around the time the bars close? How often do you get a full night's sleep vs. drive sleep deprived?
- How often are you late to work, or rushing to get there on time? Does the time it takes you to get from your home to your workplace require that you break the speed limit?
- On what days and during what times do you watch TV? How much home time do you spend in front of your computer?
- How often do you eat in? Do you tend to eat hot or cold breakfasts? What's the relative frequency of microwave dinners to three-pot feasts in your home? How often do you entertain?
- Are any of your household appliances failing or operating below optimal efficiency? Do you own lots of gadgets? Are you a Laundromat person, or do you have your own washer and drier?
- Are you a restless sleeper, getting up frequently throughout the night?
- In a custody battle: Have you ever left your child home alone? How often, and for how long?
- In a worker's compensation hearing: With your disabled back, how were you able to turn on the TV upstairs less than a minute after turning off the lights downstairs?
- Alabama tax provision requires obese state employees to pay for health insurance unless they actively work to reduce their body mass index. So: why haven't you used your treadmill at home any time in the last week? You clearly have not been away from a computer or TV long enough for aerobic exercise.
- Do depressed or bipolar individuals have distinctive energy profiles? People with behavioral disorders? Could you tell if someone hadn't been taking their medication?

Source: Quinn (2008) pp. 30-1

NIST privacy principles

- **Associate energy data with individuals only when and where required,** e.g. only link equipment data with a location or customer account when needed for billing, service restoration, or other operational needs
- **De-identify information** Usage data and any resulting information, such as monthly charges for service, collected as a result of Smart Grid operations should be aggregated and anonymised by removing personal information elements wherever possible
- **Safeguard personal information** All information collected and subsequently created about the recipients of services should be appropriately protected in all forms from *loss, theft, unauthorized access, disclosure, copying, use or modification*
- **Don't use personal information for research purposes**

Privacy-friendly smart grids

- Personal data should almost always remain at customer premises under their direct control
- Network broadcasts tariff data to meters, which control appliances
- Heavily aggregated information used for billing and price comparison
- Central Communication Provider should set interoperability standards but store no personal data

References

- E. L. Quinn (2008) Privacy and the New Energy Infrastructure, *Center for Energy and Environmental Security, University of Colorado*
- NIST (2010) Smart Grid Cyber Security Strategy and Requirements, *DRAFT NISTIR 7628*
- D. Korff and I. Brown (2010) New Challenges to Data Protection, *European Commission DG Justice*
- J. Wright and I. Brown (2010) Privacy Challenges in Delay-Tolerant and Restricted-Route Networks, *Extreme Communications*, Dharamsala
- 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
- I. Brown, D. Clark and D. Trossen (2010) Architecture Design: Embedding Inherent Values or Being Value-Neutral? *Re-Architecting the Internet*, Philadelphia