

# Personal Information Privacy, and Ubicomp



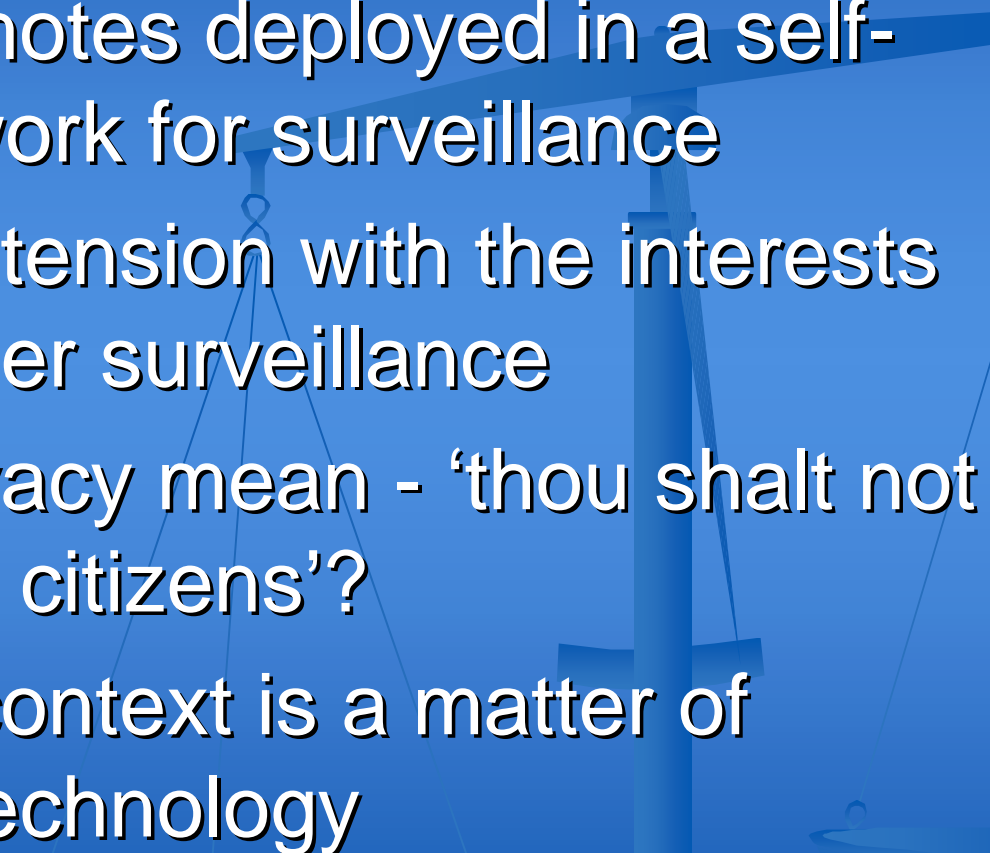
Ross Anderson  
Cambridge

# Privacy and Ubicomp



- What on earth might this mean?
- The definition of privacy that I'll use is the ability to control what happens to personal information
- Distinct from security, which covers a multitude of goals (both helpful and harmful to privacy)
- Let's look at some ubicomp platforms

# Ubicomp (1) - smart dust

- Thousands of motes deployed in a self-organising network for surveillance
  - This is in direct tension with the interests of the party under surveillance
  - What might privacy mean - 'thou shalt not monitor any US citizens'?
  - Privacy in this context is a matter of regulation not technology
- 

# Ubicomp (2) - RFID

- Big focus of US privacy concerns
- Passive tags returning 128-bit unique ID
- Argument about 'refilling your fridge' - but at heart about control of supply chains
- Can a third party scan not just what you're wearing but where you bought it, when and for how much?
- Triggered broad spectrum resistance from trade policy wonks to fundamentalist Christians
- Privacy? Maybe just kill it on purchase

# Ubicomp (3) - in the car

- Latest cars have 40-50 CPUs, CANBUS, bluetooth
- Closest to UbiComp ideal of computers embedded invisibly everywhere - serious attempt to make them usable, automatic etc
- Growing problem of feature interaction - multiple administrators / 'owners'
- Worries about platform vulnerability
- Privacy issues - combination of GSM, GPS, logging, road pricing and DRM is potentially lethal for customer control of personal data

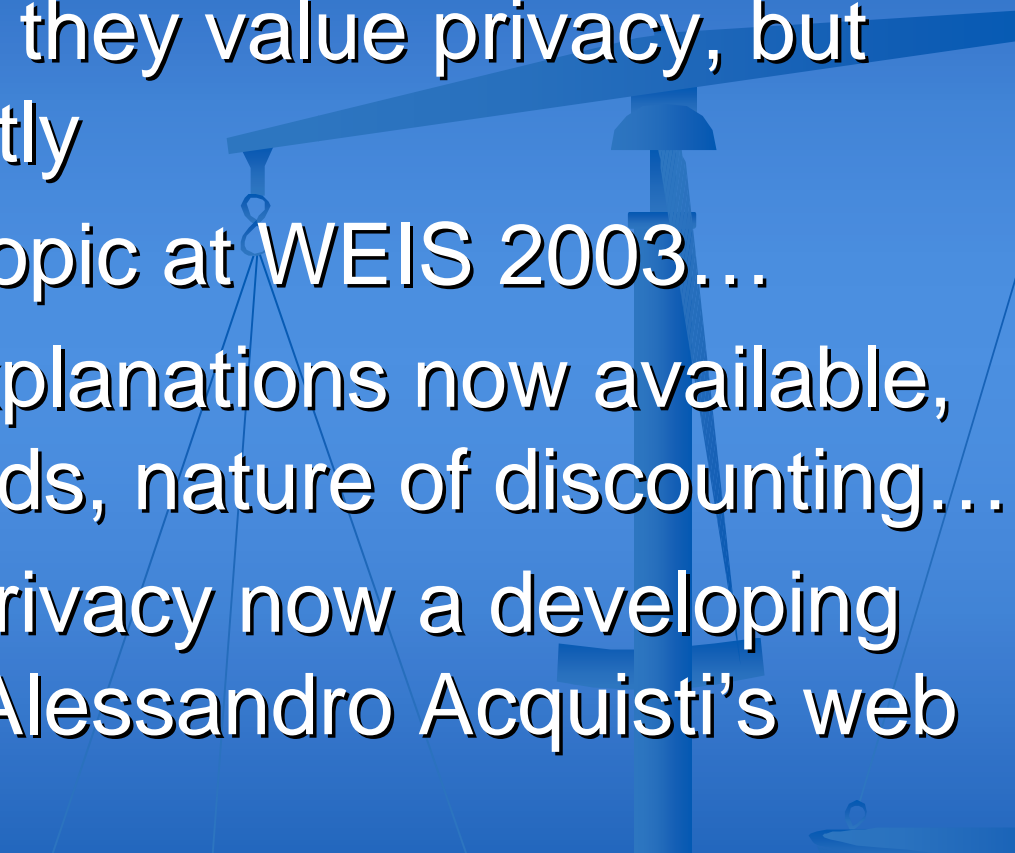
# Ubicomp (4) - the digital home

- Vision (e.g. Toshiba U-home) - appliances talk via UWB, 802.11, bluetooth, IR, RFID
- HGW talks broadband to outside world
- PKI provides universal identifiers. Could simplify using lighter-weight mechanisms, but, in any case...
- Trust management gets complex! E.g., Ellison's argument for compartmentation

# The Privacy Dilemma (1)

- Price discrimination is efficient in general! (e.g. if Barclays will pay 8K and Lloyds 4K for writing a report that costs me 10K)
- Technological progress deepens both the incentive and the opportunity for this
- Vendors demand ever more information
- Although PETs can be designed, firms can't sell them (ZK, Securicor, ...)

# The Privacy Dilemma (2)

- People say that they value privacy, but behave differently
  - Biggest paper topic at WEIS 2003...
  - Some partial explanations now available, e.g. type of goods, nature of discounting...
  - Economics of privacy now a developing discipline; see Alessandro Acquisti's web page at CMU
- 

# Odlyzko's warning

- Home environment is likely to be more complicated than the office environment today
- Home users generally less knowledgeable
- Will need to outsource the setup and maintenance of home appliances to experts - that is, remote administration
- Users given varying degrees of control, 'depending on skills and trustworthiness'
- We can already see the beginnings of this in mobile phone and car electronics markets

# Can we do better?

- We have ciphers, PKIs, ducklings and trust management engines galore
- The current bottleneck is security usability
- It's taken 30 years to come up with ways of managing the millions of bits of security state in a typical company
- The home is more complex still
- Meanwhile, consumers have difficulty with VCR programming and PC admin

# The right abstractions?

- Roles?
- Groups?
- Locations?
- Brands?
- People?
- File types?
- File creators?



# Ubicomp and Usability

- U-Vision - embedded devices will be easy to use, thus eliminating the PC's frustrations
- More sober view (Odlyzko) - trade-off between flexibility and ease of use is different for different users (and same user at different times/tasks)
- Norman's 'human-centered engineering' assumes mature products (a long way off!)
- 'We will still be frustrated, but at a higher level of functionality, and there will be more of us willing to be frustrated'

“Well, officer, the coffee pot at home tried to tell my PDA to buy some Colombian beans on the way home, but the car overheard the message and took it as a command to turn for the grocery store right away...”



# Market demand for usability?

- ‘Microsoft has triumphed because it has given us what we asked for: constant novelty coupled with acceptable stability, rather than the other way around. ... People talk simplicity but buy features and pay the consequences. Complex features multiply hidden costs and erode both efficiency and simplicity.’ (E Tenner, ‘The Microsoft We Deserve’, NYT)

# Usability and incentives

- User sees his phone banking app not as a Vodafone thing but a NatWest thing
- If it works, Natwest gets the credit
- If it doesn't, Vodafone gets the blame
- Incentives aren't right for the app vendor or the platform vendor
- Worse - there are half-a-dozen stages in the supply chain. Who'll do the work?

# Scientific challenge

- Computer scientists have spent the last 50 years building tools that help developers get a little bit further up the complexity mountain
- 'Risk thermostat' - the same proportion of projects fail, but they are bigger projects each year
- The complexity that now matters most, for building predictable dependable systems, is not from the CPU's viewpoint but the brain 's
- What should we design now instead of languages, compilers and CASE tools?

# Conclusion

- Privacy is a socio-technical system. We have to get incentives and policy right as well as mechanism and assurance
- Many of the incentives go the wrong way - and Ubicomp may make them worse
- To do better, we have a big bottleneck to deal with - security usability
- What should it mean for someone to 'lock the digital front door'?