

Privacy and Ubiquitous Network Societies

Gordon A. Gow

Department of Media and Communications
London School of Economics and Political Science



MEDIA@LSE
Department of Media and Communications

Overview

- Working definition of 'ubiquitous network society'
- Generic privacy concerns
- Three domains of information privacy
- Emerging issues in R&D
- Questions and conclusion



Ubiquitous Network Society

- Widespread interconnection of computing and communication devices
- Pervasive networks that include both wireline and wireless segments
- Mobile-to-fixed; mobile-to-mobile architectures
- Includes public and private information spaces
- Embedded intelligence, anywhere anytime



Generic privacy concerns

- Increase in quantity of personal information in circulation
- Qualitative changes through perceptual and biometric interfaces
- Personalized services may require tracking of everyday activities



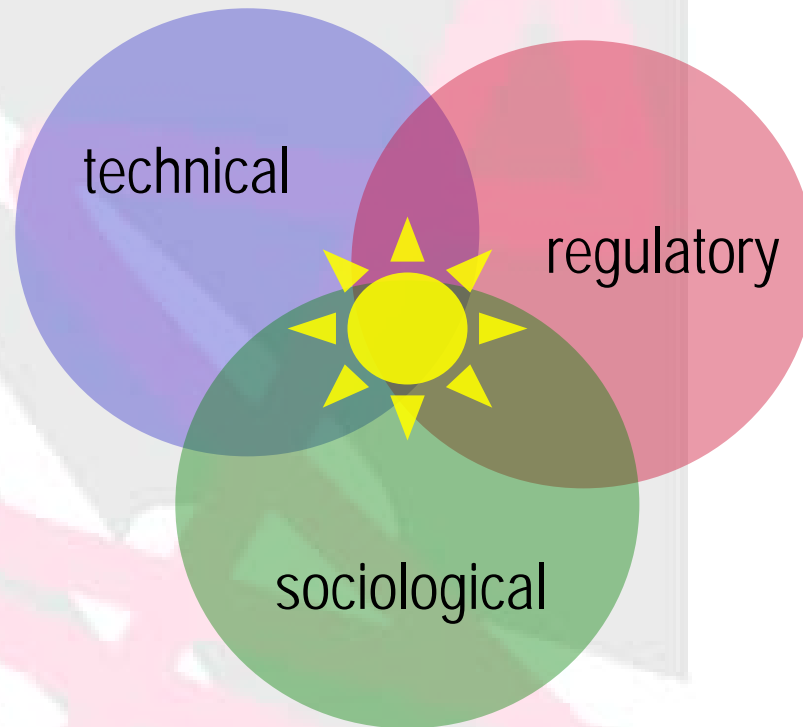
Privacy Paradox

'By virtue of its very definition, the vision of ambient intelligence has the potential to create an invisible and comprehensive surveillance network, covering an unprecedented share of our public and private life...'

Bohn, Jurgen, *et al.* (2004). 'Social, Economic, and Ethical Implications of Ambient Intelligence and Ubiquitous Computing' <http://www.vs.inf.ethz.ch/publ/papers/socialambient.pdf>



Three domains



Subdomains

- Technical
 - Encryption, anonymizers, cookies, spyware
- Regulatory
 - Collection, use, disclosure, preservation, retention
- Sociological
 - Public v. private, power, education and awareness



Consent

- Multiple contexts of use
- Memory
 - Forgotten permissions, old profiles
- Passive data collection (e.g., biometrics)
- Identity theft
- User attitudes
 - Privacy pragmatists v. fundamentalists



Data matching

- Added value comes from data matching
 - Profiles created from multiple sources of data
 - Location-base services
- Autonomic computing
 - Decentralized computing with local decisions
 - Data retention and unintended disclosure
- Social sorting and risk profiling



PETs

- Privacy Enhancing Technologies
 - Enable greater control over unauthorized collection of personal information
- Challenges in a UNS:
 - Contextual aspects of information privacy
 - Disruption of work flow
 - techno-literacy of users
 - Organisational power issues



Questions

- Will privacy become a commodity that is achieved through paying a premium?
- How will we balance privacy rights with public safety and national security concerns?
- Are the current policy and regulatory measures sufficient for the future?
- Will basic ideas about privacy rights change across generations and cultures?



Conclusion

- UNS introduces a privacy paradox
- Three domains of information privacy
- A number of emerging issues:
 - Consent
 - Data matching
 - PETs
- Questions remain:
 - Exclusivity, safety/security, institutions, cultural values

