RFID tags & ambient, ubiquitous networks

Ewan Sutherland

Contents

- some principles
- some competition
- some fears
- some unavoidable words on roaming
- some conclusions and issues

Ubiquitous principles

- economic growth:
  - innovation
  - removal of barriers to adoption
  - achieving confidence in use
- horizontal legislation includes:
  - competition and contract law
  - privacy and data protection
  - health and consumer protection
- technological neutrality:
  - the issues are ubiquitous

Threats

- criminals are early adopters
- spam, spim, viruses, trojan horses, worms, hacking, phishing, pharming, etc.
- fraud and identity theft
- surveillance
- public fears of these threats
- weaknesses:
  - inadequate design
  - poor explanation

Some examples

- Reading RFID tags in the shops of competitors
- Zapping all the RFID tags in the university library or supermarket
- Writing graffiti on someone else's RFID tags
- Reading someone's trash without getting your hands dirty (teacher, celebrity, politician, etc.)
- Offering discounts to persons carrying EU official identities in nightclubs
- Offering a parent tracking service to children
- Exhibitionists wearing RFID tags so you know they are wearing and carrying
- Fake goods with authentic RFID tags
- The NSA will have a back door to read encrypted tags

Hype cycles

- perhaps the greatest risk
- vapourware
- unmet promises
- delays

Competition

- this and only this drives the benefits through to:
  - individual productivity gains
  - economic growth
  - social welfare
- but requires:
  - access
  - roaming
  - inter-operability
  - economies of scale

Access and roaming

- no operator has total coverage, so there must be access to and roaming on other networks
- which services will have access to your:
  - personal area network?
  - car network?
  - home network?
- where will the bottlenecks be?
- parallels with carrier (pre-)selection and local loop unbundling suggest difficult negotiations
- who will sort out disputes?

International roaming

- you will be in a different legal jurisdiction:
  - so there will be differences in:
    - consumer rights
    - service provider duties
    - opt in and opt out for commercial communications
  - split/overlapping responsibilities
- severe legal problems in complying with cross-border data protection obligations
- potentially greater value of information when abroad
- there is a long history of over-charging based on abuse of market power

Beyond 3G

- 3G is far from a “big bang”
- Little chance of large-scale funding for nG
- Incremental addition of:
  - networks
  - features
- But what is the ROI for:
  - suppliers?
  - Enterprises?

The inter-working of services

- will the service you want be available on the networks you have access to?
- will the devices and networks interwork?
- how will the network be selected?
  - the cheapest? (for the user or the provider?)
  - the best quality?
- what happens if you have no billing relationship?
- will all services be available on all networks?

The question of liability

- multiplicity of:
  - networks, devices and sensors
  - network operators and service providers
  - third parties (aggregators, portals, etc)
- we need to be clear about:
  - who controls and manages the service
  - who ensures security to minimise misuse
- ultimately, if something goes wrong, who is it that goes to gaol?
- in criminal cases there needs to be a high standard of proof

Traffic data retention

- a new directive
- “limited” to Electronic Communication Services(ECS)
- likely to capture many services using RFID tags
- boundary line is unclear
- potentially vast amounts of data, perhaps several times

Conclusions

- threats and risks are everywhere
- devices are smaller and weaker
  - every device will have an IP capability
- responsibilities can be equally diffuse
- we must avoid a repetition of spam:
  - vast scale of the problem
  - long delay in its suppression
- we must act quickly to get economies of scale to enable widespread adoption

Issues

- how do we ensure competition?
- how do we avoid decades of arguments on access to networks?
- how do we ensure service portability?
- how do we ensure customer confidence?
- can integrity really be maintained across several networks?
- can vendors keep up with the hackers?
  - they innovate very rapidly
- can the law keep up?
  - where will they find evidence to show in court?

thank you

Ewan Sutherland

http://3wan.net/

http://www.gstit.edu.et/

3wan [at] 3wan.net

+44 141 416 0666