Privacy, Ethics and Society: Implications of Pervasive Computing

Frank Stajano

University of Cambridge
Computer Laboratory

From RFID to the Internet of Things
European Commission, Brussels, Belgium
2006-03-06

PGP 0xE52D19AC: A600 AC13 0511 91EB C128 :: D3A4 6526 3E25 E52D 19AC

Denied oblivion

Gathering of experts, so I'll skip the ubicomp intro

- Cost of HD storage now < 1 nano€/byte
  No economical reason ever to delete anything
- Data, once acquired, is stored forever. . .
  - *. . . including URLs of all the web pages you visit*
  - *. . . including anything you buy at the supermarket*
  - *. . . including your fingerprints held for US-VISIT*
  - *. . . including the personal data demanded by EU bureaucrats to process a travel reimbursement*

Data shadow much sharper, and never fades:
denied oblivion

UNIVERSITY OF CAMBRIDGE

Digital butlers

Your gadgets are designed to learn your habits
so as to anticipate your requests and serve you better.

- smart phone
- smart car
- smart hifi
- smart fridge. . .

Discretion fundamental for human butlers.
Do digital butlers care as much?

UNIVERSITY OF CAMBRIDGE

RFID is X-ray vision

- Lechers can check their victims' underwear
- Robbers can wear VR goggles that place € signs over worthy victims
- Burglars and child molesters can check whether parents are in
- Big Brother can track people's whereabouts by constellations of objects
- Terrorists can program bombs to recognize favourite politicians
- Competing supermarkets can automate corporate espionage

Location Privacy

- One of the first concerns as soon as we developed the Active Badge
- Our early start: Jackson (PhD 1993–1998), Beresford (PhD 2000–2004). Now problem made ubiquitous by cellphones, Bluetooth, Wi-Fi, RFID...
- Executive summary: some anonymization possible, but:
  - It's a lot of work
  - It's very hard to do it robustly
  - It can only work if infrastructure is designed for it
- Today, commercial services let Alice allow Bob to track her phone. *Bob can also allow himself without Alice knowing, as people have started to realize...*

UNIVERSITY OF CAMBRIDGE

Is privacy a goal?

- RFID proponents *say* they support privacy.
- "You can always kill the tag!" *(Smart house stops working.)*
- Strong anti-privacy incentive for merchants: price discrimination. Charge each customer as much as they are prepared to pay. *(Anti-counterfeit is a cover story.)*
- For governments: better surveillance.
  - Airport: not just X-ray scanned. All items in suitcase in outgoing trip are identified. *And logged. And compared with those in return trip.*
  - Scanning RFID passports from a distance: "helps to spot terrorists!". *As well as peaceful, law-abiding dissidents.*
  - Could put RFID in every bullet! Surely safer for all.
- Many privacy-protecting countermeasures...
  All useless if incentives are misaligned.

UNIVERSITY OF CAMBRIDGE

Fairness to non-techies

- With the “Internet of things” we are building a new world. But side effect: everything we do is traceable.
- So many laws that, strictly, all of us did something illegal this week. Currently, balanced by unobservability and unenforceability. But if all actions traced and never forgotten, we will always be guilty and under threat. A major unintended consequence for society. Will the legal system be rebooted to match?
- Remember that non-techies will have to live in it too. *As Spiderman’s uncle said,* “With great power comes great responsibility”.
- But do they care? *Apparently no.*
- Do they *understand*?

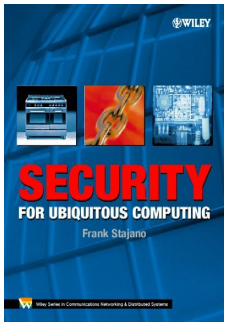
UNIVERSITY OF CAMBRIDGE

- Denied oblivion + universal observability = constant blackmail threat
- Frankenstein syndrome: building new technology is too exciting to waste time looking at long term consequences
- Technical countermeasures won't go far if the real motives are *against* privacy.

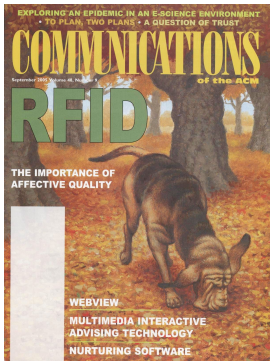
UNIVERSITY OF CAMBRIDGE

I wrote more on this…

Security for Ubiquitous Computing
Wiley, February 2002



"Will your digital butlers betray you?"
Proc. Workshop on Privacy in Electronic Society
ACM Press, October 2004



"RFID is X-ray vision"
Comms. ACM 48(9):31–33
ACM Press, September 2005

PDFs at `http://www.cl.cam.ac.uk/~fms27/`

Also: technical papers on ubicomp authentication, location privacy, breaking and repairing Bluetooth etc.

UNIVERSITY OF CAMBRIDGE