



Select before you Collect



I. Background

Own involvement

- Professor of Computer Security since 2002
- Active in “public administration” topics, like:
 - Electronic voting
 - Biometric passports
 - Privacy
 - Open source software
- With occasional role in public debates in media.



Select before you Collect

Upcoming measures

- EU **data retention** initiative: make providers store traffic data (GSM, web, mail . . .) of all 450M EU citizens for 1–3 years
- NL initiative to make **biometric passport data** accessible via **central database** for law enforcement
(Original aim: only verification of biometric match between passport and individual)

Issue: large scale collection of privacy-sensitive data!

Jacobs – Govcert.nl Symposium, sept. 2005 – p.4/24



Select before you Collect

Privacy important for:

- Dignity
(the queen also has a bathroom)
- Protection against embarrassment / shame
(who admits having haemorrhoids?)
- Personal development
(eg. after misstep / conviction)
- Freedom / creativity
(eg. for dissidents; tight surveillance deadly)

Privacy is well-protected by law (in EU, not in US)

Jacobs – Govcert.nl Symposium, sept. 2005 – p.6/24



II. Privacy:

“the right to be left alone”

Jacobs – Govcert.nl Symposium, sept. 2005 – p.5/24



Select before you Collect

“Tough” politicians / police chiefs:

- Privacy is a safe haven for criminality
- If you have nothing to hide, you have nothing to fear
- We should sacrifice privacy for security
- Do you want to be responsible for the next terrorist attack?

Jacobs – Govcert.nl Symposium, sept. 2005 – p.7/24



Well ...

- I am a decent law-abiding citizen, and I have lots of things to hide.
- I want a government that guarantees both privacy and security!

But I am not a naive softy, and I do support tough actions / privacy violations, but **only selectively**, for suspects.

This is fundamental in a state of law.

Jacobs – Govcert.nl Symposium, sept. 2005 – p.8/24



III. Data collection

Jacobs – Govcert.nl Symposium, sept. 2005 – p.10/24



Privacy as technical challenge

- Designing with privacy requires focus on what is really essential (and nothing more)
- Road pricing example (NL, 2001):
 - All cars have GPS and GSM (sensitive!)
 - Cars send monthly report for road pricing
 - ... not of **locations**, but of:
 - 300 km on “green” road
 - 550 km on “red” road etc
- “Panic button” can always be added as **selective** override, with extensive logging

Jacobs – Govcert.nl Symposium, sept. 2005 – p.9/24



Trends

- Low price of digital storage and networking has led to huge digital archives
- **Profiling** highly profitable in marketeering & risk assessment, for precise targeting
- More and more input available: purchases, travel, websurfing, digital TV, RFID, etc.
- In the US largely private sector (ChoicePoint, LexisNexis, ...), but close cooperation with government after 9/11
- NL very active (VNU, Reed Elsevier, Versatel)

Jacobs – Govcert.nl Symposium, sept. 2005 – p.11/24



Risks of large scale data collection

- Data often wrong / out-of-date, with unpleasant consequences (Eg. Ted Kennedy kept out of airplane)
- Lower level access gives more misuse (police officers privately using databases)
- **Identity theft** easy with so much data (misuse from eg. credit card nr + birth date)
- Protection of databases against hackers is non-trivial, esp. when online (keeping up with all vulnerabilities + patches)

Jacobs – Govcert.nl Symposium, sept. 2005 – p.12/24



Profiling trend

- Data analysis leads to personal profiles
- May lead to denial-of-service (plane, train, bus, insurance, loans . . .)
- Criteria usually hidden: profiling has its own “laws”
- Enforces conformistic “average” behaviour & thinking, to prevent **bad profile**
- Limited independent control and monitoring
- Legal question: privacy laws apply to data, but also to information (like profiles)?

Jacobs – Govcert.nl Symposium, sept. 2005 – p.13/24



Catching terrorist with profiles?

- Not effective: profiles yield far too many **false positives** (find one in million with 1% error rate?!)
- IMHO: intelligence agencies better use “eyes-and-ears” for **selection** . . .
- . . . and concentrate their data collection powers on those selected individuals.

Jacobs – Govcert.nl Symposium, sept. 2005 – p.14/24



IV. My big fears

Jacobs – Govcert.nl Symposium, sept. 2005 – p.15/24



What I am really afraid of:

- Somehow getting a **bad profile**
- **Identity theft**
- The combination of these two!

Privacy protection is more than a personal concern



Privacy protection in the large

- Main point: no indiscriminate data collection, but only **after selection** (eg. as suspect)
- Profiling should be covered by laws
- Privacy enhancing technology (PET) should be more standard (pseudonyms, encryption, onion-routing etc)



Privacy protection in the small

What can we do ourselves, given the data-eagerness of companies and governments?

- Never give away more personal information than absolutely necessary
- Introduce noise (eg. swap loyalty cards)
- Use technical protection
- “flood” the system

In the end, these are only partial solutions



Technical protection

- Use **TOR** for anonymous websurfing
- Use **PGP** for confidential emailing
- Use a **cryptophone** for confidential mobile phoning *etc*



Privacy flooding

- Collectively put our fingerprints on the web (frustrating biometric identification)
- Continuously generate webtraffic (genuine page requests become hidden)
- *etc*

Sobering lessons (for governments):

- Don't push this too far
- You only catch stupid criminals/terrorists

Jacobs – Govcert.nl Symposium, sept. 2005 – p.20/24



Main developments

- Increasingly: data collection **before** (instead of **after**) selection
- Large scale data collection, with all its risks, generating new crimes
- Profiling, with decisions based on “virtual identities”
- Identity theft (fastest growing crime in US)

Jacobs – Govcert.nl Symposium, sept. 2005 – p.22/24



V. Conclusions

Jacobs – Govcert.nl Symposium, sept. 2005 – p.21/24



Issues / questions / thoughts

- Privacy has intrinsic value, but is easily taken for granted
- Should we all become shameless?
- Strength of our society: creative chaos within a state of law
- New privacy affecting measures effective and proportional?
- Terrorists defy us to undermine the very values that we claim to defend (freedom, privacy, no-torture, etc.)

Jacobs – Govcert.nl Symposium, sept. 2005 – p.23/24



Further reading

- Bruce Schneier, *Beyond Fear. Thinking Sensibly About Security in an Uncertain World*, 2003.
- Robert O'Harrow, *No Place to Hide*, 2005.

Slides soon available at:

www.cs.ru.nl/~bart/TALKS