Security for Society - Is any Technological Possibility a Desirable Solution for Democracy?

Gerhard Schneider IT centre / Dept of Informatics University of Freiburg gerhard.schneider@rz.uni-freiburg.de

Albert-Ludwigs-Universität Freiburg



9/11 and its aftermath

Use technology to control everybody's life

- CCTV, bank data (SWIFT), long term storage of telephone & internet connection data,...

Legally enforce the generation of more data Enable state agencies to correlate data

Latest example:

- 10 US\$ entrance fee to the USA
- Payable with your credit card

now they know where you are

- in the country, in the world $\ensuremath{\textcircled{}}$
- Note: they process your credit card data (world wide)

Unwareness of risks to society

Albert-Ludwigs-Universität Freiburg

Politicians use what is available even if they promised otherwise

- example: German TollCollect originally **only** for accounting – why not use it for prosecution?

Politicians openly question classical basics

in dubio pro reo:

- should this really hold in the digital world?
- is digital privacy really necessary?
 - it hampers the control mania
 - it does not please the music industry

Unwareness of risks to society

Albert-Ludwigs-Universität Freiburg

Lawyers still believe that we can hide in the enormous "sea of data"

- latest purchase in Freiburg: 8CPUs/512GB, 40K€
- enough to hold 80 bytes for every human on earth in main memory (fast access for indexing...)
- German Parliament tries to block the WWW to fight child pornography
 - in reality an ineffective, if not useless scheme
 - which does not even address the problem
 - Why ask specialists??
 - It sets up an infrastucture which can be used for all sorts of censorship (to support a crumbling old world)

Interdisciplinary cooperation

Albert-Ludwigs-Universität Freiburg

Nobody listens if technicians complain 😕

- They should stay in their labs

Team up with other disciplines:

- e.g. joint seminars
- Law and Computer Science
- Sociology and Microsystems Technology
- IT and Philosophy

Provide them with up-to-date insight

- Scare them ⁽²⁾ and discuss new theories
- Think about how to advance in your own field

Various task forces at Freiburg

Albert-Ludwigs-Universität Freiburg

Three major fields of interest have evolved:

- Thinking in security terms basic human behaviour and requirements
- New architectures for integrating security demands into society
- Technology for security vs. changes to society

Schizophrenic behaviour

Albert-Ludwigs-Universität Freiburg

Governments want to harvest data in social networks to identify terrorists

- And petty criminals (with a much higher success rate)

At the same time military warn their staff not to use social networks as classified information might leak out or may be deduced

- The Israeli army was the first to warn in public

The wife of the new MI6 boss publishes private information in facebook – jeopardizing national security

New paradigms

There is no anonymity

- if you keep data
- and do cross-correlation
- 80% of US citizens can be identified via ZIPcode, birthday and gender

Example: identify people via behavioural patterns in video recordings

- already used in court!
- Use face recognition to identify people in pictures on *flickr.com*
 - you may be on someone else's snapshot, proving you were in a certain location – and not where you claim to have been

EIBURG

Thinking security

Albert-Ludwigs-Universität Freiburg

In an emergency, will people behave the way the legal system expects them to behave?

- Looting, lyching,...
- Use computer simulation like computer games to study human behaviour
 - To get larger and more useful samples
- TV series influencing public view of security?
 - Cooperation of psychology, law, economy, humanities and IT

If you understand human behaviour – what are the right procedures / rules?

JNI FREIBURG

New architectures

Traditionally law experts only check the side effects of surveillance against individual paragraphs of the constitution

- The addition of various effects is not studied
- Is it clever to introduce a specific security measure?
 - Or should priority be given to the study of side effects and cumulative effects
- What is the price/cost of not installing counter measures to certain (criminal) offences?
 - E.g. is it worth it to fight any copyright violation?

New architectures

How do counter measures stop the evolution of society?

- breaking obsolete laws is part of progress
- e.g. shopping hours in Germany were once quite rigid
- scanning of books by Google may be illegal, but may be good for public knowledge
- Will surveillance also modify the target?
 - If a computer is hacked by a government agency, will the modified routines modify the evidence?
- If the state grants anonymity in the classical world, why not in the digital world?
 - I may use a public payphone without any ID, but not a mobile phone

Potential approaches / analysis

Albert-Ludwigs-Universität Freiburg



A department store may want to operate cameras to fight theft

- But why store the video for a long time?
- Or why allow security staff to monitor their girl friends?

Can we merge these contradicting requests?

- Why do we have to see the individual rather than the anonymous human on video in order to fight theft?

Potential approaches / solutions?

Albert-Ludwigs-Universität Freiburg

REIBURG

Digital stealth mode

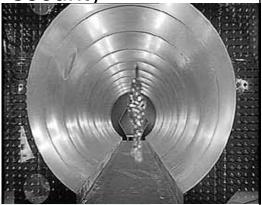
I carry a device (e.g. a mobile phone)

- When I enter a department store my device receives information on the store's policy w.r.t privacy

I may agree to a contract

- store security may monitor me if it does not process/store identifiable information
- e.g. only a shadow of me will be produced by the security camera, so that my actions may still be seen, but not my face nor my clothes.

or I do not enter the store



Potential approaches

How do we make sure that the camera will always adhere to the rules?

- Use hardware specification & verification technology from computer science
- So that my device can check whether it speaks to a verified (and unmodifiable) camera

How do we introduce such verifications into the legal process?

- e.g. have laws with attached hardware specifications
- Useful side effects: if politicians want new features, prior to a firmware update a new legal process is required
- And my device will detect the change I can then act accordingly.

International aspects

Security concerns are usually solved nationally

- Through legislation and politics
- This is pointless if we have strict rules on pro-cessing existing data but the CIA has not
- The Internet allows for international access to all available data
 - International legislation is quite difficult
 - Unless the legal systems do not differ too much (Japan/Germany??)

Rather than endangering its citizens should a state invest more in protecting its citizens against the curiosity of friendly states?

UNI FREIBURG



New threats call for new security measures

- Surveillance and storage of resulting data is seen as a security measure.
- The more data are accumulated the less secure the individual is
 - Society is formed by individuals!

What is the right balance?

- Introduce technical understanding in classical fields
- Common issue for the Japanese and the German society
 - Freiburg is looking forward to cooperating with the NII