

Panel discussion: Security XOR Privacy

Andreas Pfitzmann

- My Motivation
- My Personal Aims and the Appropriate Architecture
- Discussion
- Conclusion

My Motivation

At school, I learned the very basics of ethics:

Do to others, what you want them to do to you!

--> Multilateral Security

--> Enabling Technologies

Later, I learned that even if people only fear that something like 1984 is happening, this means an end to democracy as we know it: People no longer dare to say what they really want, so the very basic mechanism of democracy, having all kinds of conversations and disputes at different fora, does not function anymore.

--> Prevent any tendency towards 1984

Starting in Sept. 2001, some terrorists tried to shock and change pluralistic democratic societies. They failed, but politicians (may be at their own discretion, may be driven by the media) in these democratic societies succeeded in doing the job intended by the terrorists.

--> Overcome political actions tending towards 1984 starting in 2001

So whatever Emerging Trends in Information and Communication Security might be, they should support Multilateral Security and at least not hinder to avoid 1984.

My Personal Aims and the Appropriate Architecture

Effective security *and* effective privacy !

If I have to choose between ineffective security and effective privacy, I clearly choose privacy, and vice versa.

Multilateral security helps to have both effective security and effective privacy:

application 1 application 2 application n

(privacy-enhancing) identity management

anonymous communication (e.g. by MIXes)

traceable and authenticated communications
(incl. data retention, if wanted)

Discussion

1. Underline what Sarah said: Privacy is NOT only a personal issue, it's an issue of the democratic society as well.
2. To Peter Raab: Pre-Paid eCommerce is very privacy friendly.
3. Detection of misuse of data is very hard to detect --> data avoidance where ever possible
4. To Seda: Fairness in communications can be bootstrapped from the bottom layer to higher layers
5. Fake of passport an issue sometimes --> digital signature under the contents of the passport is fine, but biometrics helps more the criminals than the good guys

(cf. Andreas Pfitzmann: Biometrics - how to put to use and how not at all? How to handle security problems of biometrics and how to handle security and privacy problems caused by biometrics? Security and Privacy in Information Society (ISC 2005), Düsseldorf, 27.10.2005. [Biometrics.pdf Düsseldorf 2005.10.27 \(PDF\)](http://www.inf.tu-dresden.de/index.php?node_id=703&ln=de); for download at http://www.inf.tu-dresden.de/index.php?node_id=703&ln=de)

Conclusion

Above all, our society demands safety.

Given the ever more dependence on ICT, we may write the fundamental equation as:

$$\mathbf{Safety = Security + Privacy}$$