

The German Federal Constitutional Court - closer to ICT and Technology Assessment than German Government

Andreas Pfitzmann

Technische Universität Dresden, Faculty of Computer Science, D-01062 Dresden
Nöthnitzer Str. 46, Room 3071

Phone: +49 351 463-38277, e-mail: pfitza@inf.tu-dresden.de, <http://dud.inf.tu-dresden.de/>

Abstract

- **German government** usually does not understand information and communication technology (ICT) and therefore, often they do not understand possible uses of ICT they try to regulate (and some politicians are even proud of not understanding ICT). So, German government, e.g., assumes terrorists will connect their computers to the Internet in an insecure fashion to enable the German Federal Police to search their hard drives.
- In spite of this attitude of German government, the **German Federal Constitutional Court** did a remarkable job in Winter and Spring 2008 to decide on regulations of ICT.
- My talk shortly explains why and how.

Actors and their Knowledge

Average knowledge

Average knowledge
about ICT

German Government

- Understanding ICT is not sexy
- Assume ICT does what it shall do
- If you don't understand and there is no experience to rely on, do something and pretend you are certain to do the right things

Society at large

Experts in ICT

German Federal Police

- Pretend to only serve the well-being of society at large
- Never mention self-interests, e.g., more money for and employees working in ICT

German Federal Constitutional Court

- Understand ICT
- Listen to and understand all arguments
- Form an own opinion

Actors and their Knowledge

Strategies
Counterstrategies

Average knowledge

Average knowledge about ICT

German Government

- ~~Understanding ICT is not sexy~~
- ~~Assume ICT does what it shall do~~
- ~~If you don't understand and there is no experience to rely on, do something and pretend you are certain to do the right things~~

Some training in ICT

Own judgement and so capability to sort out contradictions, listen to all experts

Since no own judgement and so no capability to sort out contradictions, listen to German Federal Police only shifting the responsibility on to them

Society at large

Experts in ICT

German Federal Police

In-depth training in ICT

- Pretend to only serve the well-being of society at large
- Never mention self-interests, e.g., more money for and employees working in ICT

Make self-interests known

German Federal Constitutional Court

- Understand ICT
- Listen to and understand all arguments
- Form an own opinion

A chain of arguments

- Knowledge in ICT of the German government is much weaker than the knowledge the German Federal Constitutional Court acquired within months.
- Specific to ICT?
 - Experience in physical life does not continue in the digital space
 - No knowledge in ICT is socially accepted (and convenient)
- Part of a strategy?
 - Institutional necessity: Fight for resources at the cost of freedom
- Counterstrategies
 - Government needs training in ICT
 - Disclose self-interests in an open debate

Answers to the three questions

- If you were politically in charge of privacy and data-protection, what would your first advice or regulation be? *Requiring everyone, including politicians and data protection officers, to get some in depth training about ICT in general and data security in particular. Without at least thorough basic understanding of ICT and data security, a fruitful discussion about privacy and data security is impossible - not to speak about helpful decisions how to approach and solve issues.*
- Are you personally concerned about profiling? In what sense? *I am not much concerned about my country doing profiling of me (which of course should be restricted to stay within reasonable limits), but I am pretty much concerned about other countries and their secret services. In addition, organized crime will do profiling where ever technically possible, e.g. gathering biometric fingerprints exploiting the carelessness with biometric data induced by the new generation of European passports. So infrastructures supporting profiling are no good idea as long as ICT is as insecure as it is today. Particularly bad are infrastructures, where the bad guys can avoid being trapped, but the good guys are profiled: Neither terrorism nor organized crime require communication such that data retention can serve its stated purpose.*
- On what privacy topic should we organize a panel next year?
 - Biometrics, e.g. in e-passports, and privacy
 - Valid privacy policies in a world where nearly all ICT is pretty insecure