

Counter Terrorism and Privacy The German Case

European Pluridisciplinary Seminar

"The Role of ICTs in the Evolution of Security Policies in Europe"

27 January 2006, Laboratoire de Informatique des Paris 6

Dipl. Pol. Ralf Bendrath

University of Bremen

Overview

- Security vs. Privacy over time
- A New “Security” Paradigm



Security vs. Privacy over time

German Privacy History

- **1945: defeat of Nazi regime**
 - genocide, secret police (GeStaPo), terror rule
- **1949: West German Constitution**
 - human dignity as cornerstone (Art. 1)
 - privacy of communications and home (Art. 10,13)
- **1971: first data protection law in Hessen**
 - protection against computers in administrations
- **1983: Constitutional Court Census Ruling**
 - "informational self-determination"
- **Repeated Constitutional Court Rulings**
 - stopped some of the worst laws, but not all

German Counter-Terror History

- 1951: paragraph 129 in criminal code
 - „support of criminal organization“ – worse than 1871
- 1968: „state of emergency“ laws
 - phone interception by intelligence agencies
- 1976: paragraph 129a in criminal code
 - „support of terrorist organization“
- 1998: „organized crime“ law
 - „big eavesdropping attack“
- 2001 / 2002: „counter-terror“ laws I&II
 - „foreign terrorist organizations“ (EU 1998)
 - secret searches in private databases
 - easy access to traffic data

Good Beginnings...

- Strong protection for Privacy and Human Rights in Constitution
- Privacy Protection since 1971
 - enforcement still weak
 - elephants & mice, exceptions
 - public awareness had peak in 1980s
 - good network of privacy professionals
 - NGO community fragmented

Bad Developments...

- Steady assaults on privacy in the name of security
- 1950s-60s: Communism
- 1970s: Left-Wing Terrorists
- 1980s: Neo-Nazis
- 1990s: Organized Crime
- 2000s: Islamist Terrorism

Who is Winning?

- Braking / Breaking the Securitization?
- No political majorities
- Repeated Constitutional Court rulings
- Technological measures (defensive)
- CCC, December 2005
 - “We lost the war”
 - defend anonymous use of ICTs

The Use of Technology

- First: only specific searches
 - eavesdropping
- Later: profiling, computer searches
 - Horst Herold, Federal Police Director
- Now: everybody is a potential suspect
 - data retention
 - biometrics
 - toll collect
 - 2006 soccer world cup as major test bed



A New “Security” Paradigm

The “Balance” Discourse

- “Balancing” Security and Privacy?
 - constitutional human rights protection as stronghold against “security”
 - security politicians: “balance of weapons”
- Paradigm shift
 - public interest in law enforcement vs. human rights protection
 - → security and privacy on same level

A Special German Invention

- **”Human Right to Security”**
 - Josef Isensee / Rupert Scholz (1984)
- reaction to census ruling
- no longer defense against,
but demand towards government
- government has to provide security
- security policy as human rights protection
- prevention of insecurities (“risks”)

“Human Right to Security”

- **“super human right”**
- basis of other human rights
- “no human rights without security”

- more security → more human rights protection
- surveillance necessary to save privacy

- part of political discourse now

"Prevention" Logic is Spreading

- **German Police**
 - from "repression" to "prevention"
 - "preventive state protection" since 1976
 - preventive arrests since 1989
- **NATO Strategy 1991**
 - from "balancing threats" to "preventing risks"
- **"War on Terror"**
 - acceleration
 - "prevention" as hegemonic doctrine

Prevention and Technology

- **“Prevention” as hegemonic doctrine**
 - Who is or can become a risk?
 - prediction of behaviour needed
- **Remember CRM?**
 - prediction of potential purchasing behaviour
 - not just business tool, but social sorting
- **Terrorist Risk Management (TRM)**
 - convergence of CRM and security measures
 - technology in favour of this

Questions?

- Dipl. Pol. Ralf Bendrath
 - ralf.bendrath@sfb597.uni-bremen.de

Technological Aspects

Technological Aspects I

- **Security: Computers tell Intentions**
 - Storing, Matching
 - Profiling, Data-mining
- **Privacy: Protection against Profiling**
 - What am I? What do I want?
 - personal ID number illegal
 - “Humans can not be reduced to a set of computer data”

Technological Aspects II

- **Security: Eavesdropping tells words**
 - Bugs, Interception devices
 - Infrastructural design (ISP nodes)
- **Privacy: Protection of personal zone**
 - What do I tell whom?
 - home, communication

Technological Aspects III

- **Security: Tracking tells Locations**
 - Passports, Biometrics, CCTV, Tolls
- **Privacy: Freedom of movement**
 - Where can I go?
 - public places, travel infrastructures