

EPHR - Key Findings

January 26, 2011 by *pi*

Europe is the world's leader in privacy rights. But with leadership like this, we worry about the future. The Directive on Data Protection has been implemented across EU member states and beyond, but inconsistencies remain. Surveillance harmonisation that was once threatened is now in disarray. Yet there are so many loopholes and exemptions that it is increasingly challenging to get a full understanding of the privacy situations in European countries. The cloak of 'national security' enshrouds many practices, minimises authorisation safeguards and prevents oversight.

The primary conclusion? The situation is mixed. And for a world leader, this is unconvincing and untenable.

Good

- European democracies are in generally good health, with the majority of countries having constitutional protections.
- Surveillance policies have faced obstacles across Europe, including political challenges, policy implementation problems, and resistance from regulators, civil society, the general public and industry.
- European regulators are getting more and more complaints, which we take as a sign of increased awareness of privacy issues and awareness of the regulators' duties.
- Notification requirements for those placed under secret surveillance. (Luxembourg, Switzerland, Czech Republic)

Heroic

- Greece: in 2007 there was a collective resignation from the regulator in protest to the government's insistence of repurposing the Olympics' surveillance system.
- Germany: groups mounted a campaign against communications data retention where 34,000 people filed a case at the Constitutional Court appealing against the law.
- Netherlands: policy on mandatory smart meters had to be withdrawn after opposition.
- UK: NGOs mounted policy campaigns against the surveillance policies of the previous government, resulting in policy repeal on issues ranging from ID cards and biometric passports, to DNA practices, and large databases.

Awkward

- Many of the ambitious surveillance proposals have failed in implementation.
- Deployment of biometric passports and data retention is fragmented.
- Cutbacks have affected regulators' abilities to do their jobs, e.g. Latvia, Romania
- Ministerial warrants still exist in too many countries, i.e. Ireland, Malta, UK
- Access to financial data is on the rise, e.g. Belgium, Croatia, Czech Republic, France, Germany, Greece, Italy, Norway, Poland, Slovenia
- Failed oversight mechanisms, e.g. Sweden's commissioner over covert surveillance powers resigned in protest

Bad

- Inability to build safeguards into processes to gain access to information over new services, e.g. France, Germany, Switzerland seeking powers to conduct secret searches fo

computers, Ireland's ambiguous powers for unwarranted interception of VoIP; Italy building 'backdoors' into systems; Bulgaria's 'black boxes' at ISPs

- France: Attempt to ignore constitutional amendment proposals to include an explicit constitutional right to privacy.
- eHealth systems with security faults and/or centralised registries (France, Germany, Italy, Netherlands)
- Biometric registries and databases emerging and with more coming (Estonia, Italy, Lithuania, Netherlands,
- Few protections and safeguards for government access to data. (most countries)
- Illegal and warrantless surveillance still occurs.
- Journalists and dissident groups are under surveillance. (Lithuania, FYRM, Poland, Romania, Slovakia, Turkey)

Ugly

- Direct access to information held by third parties without warrants or oversight, conducted by unaccountable bodies. (e.g. Bulgaria, Croatia,)
- Inability to audit and review the actions of security services. (e.g. Lithuania, Croatia, Estonia, Hungary, Sweden)
- Medical databases are emerging with centralised registries. (e.g. Croatia, Czech Republic, Denmark, Sweden, Norway, UK).

This project was funded with the support of the Fundamental Rights and Citizenship Program of the European Commission.

<https://www.privacyinternational.org/article/ephr-key-findings>

Access on 04.05.2011