Berliner Beauftragter für
Datenschutz und Informationsfreiheit

Privacy built-in rather than bolted-on – a mere vision or first use cases ?

Dr. Alexander Dix, LL.M.
Berlin Commissioner for Data Protection
and Freedom of Information

10th Privacy Enhancing Technologies Symposium

23 July 2010

Berlin, Germany

Overview

- The regulators‘ traditional vs. the new approach
- Social networks
- Road pricing
- Distribution of digital media content
- Electronic health records in hospitals

The regulators‘ traditional vs. the new approach

- *Locking the stable door after the horse has bolted*
- Regulators have traditionally exclusively reacted to violations of rules trying to bolt-on privacy to existing products and processes
- This is no longer sufficient (although violations of rules still have to be sanctioned)
- What is needed is a more preventative, systemic approach to privacy protection

Social Networks

- Social Networks have been the subject of three major studies recently
- The Rome Memorandum by the International Working Group on Data Protection in Telecommunications – *Berlin Group* (March 2008)
- Working Paper 163 by the Art. 29 Working Party (June 2009)
- Findings by the Privacy Commissioner of Canada in CIPPIC v. Facebook Inc. (1st Inquiry July 2009, 2nd Inquiry pending since January 2010)

The default is key

- In all major social communities the default used to be that new accounts are visible to all members of the community.
- Ann Cavoukian‘s Privacy by Design Principle No. 2: „If we can all be certain of one thing – the default rules !“
- Rome Memorandum: „Privacy-friendly default settings play a key role in protecting user privacy.“
- Although most social networks allow for restrictive privacy settings they are rarely used or only after something really bad has happened.
- Therefore: **The default should be privacy, not openness !**

Some get the message, others don‘t

- The VZ Netzwerke (Berlin) had restrictive default settings only in their platform schülerVZ, later extended these to their platforms studiVZ and meinVZ.

- Facebook still maintains privacy unfriendly default settings but is facing increasing opposition (Quit Facebook Day).

Real names vs. nicknames

- A option to use pseudonyms (nicknames) on social networks is prescribed in certain jurisdictions (e.g. Germany)
- But most social network services insist on registering with real names and using these names in the networks
- *Rome Memorandum* strongly recommends not only to allow for nicknames to be used but also to encourage their use

Third party applications

- More and more third parties seek access to social networks to offer additional services, functionalities, games etc. and to harvest personal data simultaneously

- Therefore it is vital that the user has the choice to allow third party access only to the extent that is just sufficient to perform a certain task *(user-mediated third party access implemented by studiVZ)*

- *„Where is the Privacy App ?“ (Peter Schaar)*

Necessary research and development

- Berlin Group called for strengthening research activities in this field
- From „policy-aware web“ to „privacy-aware web“
- Encrypting user profiles
- Decentralised storage of such profiles (under user control – see *Diaspora*)
- Watermarking technologies for photos
- Use of graphics instead of text for displaying information
- Introduction of an expiration date to be set by users for their profiles
- Protection against spiders, crawlers, bulk downloads

Mark Zuckerberg‘s errors and their consequence

- Zuckerberg is wrong when he suggests that privacy is outdated and Facebook merely responds to a change in social values.
- Users don‘t like to be considered „dumbfucked“.
- The Hamburg Data Protection Commissioner has launched proceedings against Facebook with regard to the illegal use of contact data of non-users after the upload and matching of phone books of Facebook users.

Road pricing

- People using vehicles normally travel anonymously
- They – just as pedestrians – have a *right to locational privacy*, to move freely without being registered or tracked
- This could change fundamentally with the advent of automatic road pricing systems („pay as you go“)
- But here again: much depends on the design of such systems

Recent studies and recommendations

- Information and Privacy Commissioners from various jurisdictions (Ontario/Canada, Netherlands, Victoria/Australia, Norway, Slovenia) have addressed the issue
- So has the U.S. National Surface Infrastructure Financing Commission (February 2009)
- The Berlin Group in their Sofia Memorandum of March 2009 dealt with the issue in detail and made a number of recommendations

Risks to privacy in road pricing systems

- Massive surveillance infrastructures possible if movements of inividuals (vehicle owners, drivers, employees) are tracked
- Central databases provoke secondary uses even if initially ruled out by regulators and law
- Function creep unavoidable
- Therefore: a technical infrastructure should be installed from the start which strictly limits the processing of personal data and especially excludes the storage of detailed movement profiles

Thin client vs. smart client

- Thin clients (On Board Units) transmit all data concerning the location of the vehicle, the distance travelled and the roads used to the control centre where the toll charge is calculated - **least favourable design in terms of privacy protection !**

- Smart clients preserve the anonymity of the driver because they calculate the charges under his control and only send the total sum due to the control centre **– better privacy protection by design !**

Privacy-compliant enforcement

- The fact that some drivers may break the rules or try to evade the system does not justify identification and permanent tracking of all drivers
- **Only if there is evidence or suspicion based on facts that manipulation or evasion is taking place the identity of the driver may be ascertained**
- As a first step it has to be established if the toll system device is present in the vehicle and functioning faultlessly (principle of proportionality). If that is the case there is no need to identify the driver.

Main recommendation of the Sofia Memorandum

- **Centralized processing** of personal data (especially of movement profiles) is not necessary for road pricing and therefore **unjustified.**

- The Berlin Group in their Sofia Memorandum calls for strong privacy protection to be built into road pricing systems from the start. **Only bulk charges should be collected centrally**. This would offer better privacy protection than in mobile phone or credit card systems where detailed location and consumption data are being processed.

- Possible use case: the Netherlands ?

Distribution of Digital Media Content

- Working Paper adopted by the Berlin Group in September 2007
- **„The possibility of anonymous consumption of television and media content must be preserved in the digital age.“**
- This is called into question by the convergence of networks (triple- and quadruple-play, combination of TV and Internet access by providers, video on demand, peer-to-peer-communication etc.)
- The new digital interactive TV systems very often operate as a **„black box“** and give the user little or no control

Main recommendations by the Berlin Group

- Information systems set up to deliver digital TV have to be designed, built and configured to promote and assure anonymity (as with analogue TV consumption) or at least minimization of the use of personal data. A German company has already taken up this advice.

- If personal data are collected it may only be for legitimate reasons and to a legitimate extent. **Choice of channels does not justify identification of viewers.**

- Viewers‘ profiles may only be processed or communicated to third parties for marketing or other purposes with the viewers‘ explicit and free consent.

Electronic Health Records online and in hospitals

- The Berlin Group addressed the issues of web-based telemedicine in 2002 and 2006 recommending certain measures to be taken before health records can be made available online.

- But a recent judgment by the European Court of Human Rights (I.v.Finland – 2008) points to the fact that there are severe problems offline in hospitals.

So far: Lack of privacy design in hospital IT systems

- IT systems in hospitals which do not allow for checking and retroactive verification who has accessed a patient‘s file violate the human right to private life (Art. 8 ECHR).
- Problem: hardly any hospital IT systems are designed and manufactured to allow for checking and retroactive verification !
- Berlin Commissioner‘s office is coordinating the effort to draft guidelines to German manufacturers of hospital IT systems according to privacy by design.

The hard questions

- When do PETs get deployed in mass-markets and reach the break-even point ?
- What are the factors which prevent this happening or which could support such a development ?
- General legal obligations not enough
- Link to procurement rules is vital: if prices and conditions are equal products with in-built privacy are to be preferred

Better to build-in than to bolt-on privacy

- There is a strong business case for privacy by design:
- It is always much more expensive to bolt-on privacy to a product once it has left the production line than to build it in from the start
- Google has to spend a lot of money to implement the individual‘s right to object against publication on Street View („Data protection creates jobs !“)
- It would have been cheaper (and less damaging PR-wise) to get it right from the start

A coming use case: Smart Grids

- Smart meters are prescribed by law now in Europe and elsewhere
- They are the door-opener to smart grids which pose a number of tricky privacy questions
- If these are not solved in time, smart grids will not achieve their goal (sustainable environmental protection)
- We are examining the possibility for a joint initiative with our colleagues from Ontario (IPC)

Summary

- Privacy issues cannot be tackled solely in a reactive manner
- The best rules lead to nowhere if the technology in place is not privacy-compliant
- It is vital to focus on designers, manufacturers and standard-setting bodies to build privacy protection as fas as possible into the systems
- There will never be a magic „privacy button“, privacy by design is no panacea
- But: without privacy by design it will be difficult if not impossible to achieve meaningful privacy protection in the 21st century
- **The door should be locked before the horse bolts !**

Questions ?

dix@privacy.de