Public Report and

Proceedings

of the

Third
European Privacy Open Space

held at the

Europahaus in Vienna
26th and 27th October 2009

in conjunction with the
Austrian Big Brother Awards

PRIVACY

Project Acronym:	PrivacyOS
Project Title:	Privacy Open Space
Grant Agreement No:	225044
Starting date:	June 1, 2008
Ending date:	May 30, 2010
Deliverable Number:	D15
Title of the Deliverable:	Report 3rd European Privacy Open Space
Version	November 2009
Task/WP related to the Deliverable:	Results of the Conference
Type (Internal or Restricted or Public):	Public
Author(s):	Jan Schallaböck, Dr. Katalin Storf
Partner(s) Contributing:	All Partners
Contractual Date of Delivery:	November 2009
Actual Date of original Delivery:	November 2009

Project Co-ordinator:	Unabhaengiges Landeszentrum fuer Datenschutz/
Independent Centre for Privacy Protection	
Name of representative:	Jan Schallaböck, Dr. Katalin Storf
Address:	Holstenstr. 98, 24103 Kiel, Germany
Phone number:	+ 49 431 988 1283
Fax number:	+ 49 431 988 1223
E-mail: privacyos@datenschutzzentrum.de	
Project WEB site address:	www.privacyos.eu

The European Privacy Open Space (short:PrivacyOS) is a project supported by the European Commissions' ICT-Policy-Support-Programme under Contract No. 225044.

The Project is coordinated by the ULD:
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD)
Holstenstr. 98, D-24103 Kiel
privacyos@datenschutzzentrum.de

This publication is published by the ULD on behalf of the PrivacyOS Consortium.

Public Report and

Proceedings

of the

Third
European Privacy Open Space

held at the

Europahaus in Vienna
26th and 27th October 2009

in conjunction with the
Austrian Big Brother Awards

PRIVACY OS

ARGE DATEN - PRIVACY AUSTRIA
Hans G. Zeger, Chairman

PrivacyOS Conference
Wien October 2009

On the Way to Scoring Society

It's part of my daily job to deal with questions by the media whether a certain surveillance measure, a new register or a new technology will bring us closer to surveillance society. They have asked me such questions for the last twenty years. Even the longest path cannot have so many steps that you will not finally reach the destination.

We should therefore confront the awful truth, that we have long arrived at surveillance society in its classical sence. Never before citizens have left so many exploitable - mostly digital - marks be it through their travelling habits, their communication or their consumerhabits, in the workplace or in public. Never before was it so easy for public authorities and companies to retrace people's behavior. The examples are never-ending and in spite of this, the classical security-concept to ensure security through surveillance is not working at all. Nowadays we have more surveillance and more crime.

Classical surveillance does have a positive and comforting aspect. Surveillance and monitoring is attractiv to many people, implying that there is somebody who looks after them, who takes care of them. Surveillance brings order into a world that is becoming increasingly unclear and threatening.

The collapse of the concept "Security through Surveillance" has led to completely new approaches. No longer the concrete behavior is recorded and if necessary sanctioned, but expressions of daily routines are collected ahead (see Data-Retention, see Passenger Record Transfer). Lists and registers are created ahead of absolutly every move to score suspicios behaviour in advance, long before it becomes criminally relevant. Whoever does not have an adequate alibi is a suspect. Presumption of innocence is replaced by suspicion of guilt which needs to be averted through good conduct.

We are today on the cusp of a new era. We are at the beginning of an alibi- and scoring-society.

General characteristics, like marital status, age, type of employment contract, which street somebody lives on etc. are serving today to calculate an individual's scoring value. The values regulate access to economical, social and soon also to political life. Today these values are mainly significant in the economic sector but also politicians start wondering whether to restrict the access to jobs, to freedom of travelling, and of communication to invalid persons, persons with too low scoring. The "three-strike-out" idea to completely lock out peculiar ínternetusers from the internet points exactly in this direction.

This alibi- and scoring-society fundamentally challenges our core values und human rights. The issue is no longer the dispute with a state who controls more or less, but the defense of a direct attack on our human rights.

In this context it will be useful to remember some of our core values.

Article 1, 1st paragraph of the European Dataprotection Directive clearly states to the goals of our information society: "In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data".

Freedom, fundamental rights and privacy are central terms for the organisation of our information-society - not the other way round - we must not subordinate our fundamental rights and our private life to an omnipresent security-paranoia

Now I ask you, what value could privacy have if we no longer have the freedom to shape it ourselves and to decide which part of it to present, if we loose our freedom to speak out freely. Central to this freedom is also the liberty to act or speak callowly stupidly and controversially.

What value would our freedom have, if we could only say what is right and move along the mainstream? We would no longer live in a free society but rather in a labyrinthof walls of glass, where freedom is only pretended.

For the past 300 years our civilisation can look back at an unprecedented success-history, thanks to freedom, thanks to fundamental rights and also thanks to the possibility to explore new areas through trial and error. This successstory must not be destroyed by gererally suspecting all citizens, by deviding them into valids and in-valids, by thought control and placing bans on the expression of individual views.

The protection of privacy is directly linked to the protection of free speach and free expression in public. In my latest book about Web2.0 I have crossed out the danger that every restriction to free expression of opinion in these new social networks is a dangerous step towards a new censorship-society. Therefore we must develop concepts to secure freedom even in a new frightening technological landscape

In doing so, we will have to draw a categorical line between the freedom of individuals and actions set by institutions. What individuals rightly claim as part of their human rights, must be denied to authorities and companies. They need extensive control by our civil society, they must become much more transparent than today. They need precisely the kind of transparency for themselves, they impose on more and more people nowadys.

I wish this conference an intense exchange of ideas and many new concepts. May this conference contribute to securing our fundamental rights in our information society.

Hans G. Zeger, degree in philosophy, mathematics, social sciences, author of "MENSCH. NUMMER. DATENSATZ. Unsere Lust an totaler Kontrolle", Residenzverlag 2008, "Paralleluniversum Web2.0", Kremayr&Scheriau 2009 and numerous further case-publications, lecturer at Juridicum Vienna, member of the Data Protection Council at the Federal Chancellery of the Republic of Austria and chief executive officer of "e-commerce monitoring GmbH", chairman of "ARGE DATEN - PRIVACY AUSTRIA" (http://www.zeger.at)

Contents

Introduction

The Project European Privacy Open Space (PrivacyOS) aims at bringing together industry, SMEs, Government, Academia and Civil Society to foster development and deployment of privacy infrastructures for Europe. The general objectives of PrivacyOS are to create a long-term collaboration in the thematic network and establish collective interfaces with other EU projects. Participants exchange research and best practices, as well as develop strategies and joint projects following four core policy goals: Awareness-rising, enabling privacy on the Web, fostering privacy-friendly Identity Management, and stipulating research.

Over a two-year lifetime of the project four Open Space conferences will be held, possibly co-located with other events to extend the network further. So far, three conferences have been taken place.

The 1st PrivacyOS Conference was held on the 13th to 15th of October 2008 under the patronage of the Member of the European Parliament, Alexander Alvaro and co-located to the 30th International Privacy Conference in Strasbourg. The 36 participants from industry, SMEs, Government, Academia and Civil Society from 12 different EU countries autonomously developed the agenda corresponding to ongoing topics.

The 2nd European Privacy Open Space conference, held in Berlin, April 1st to 3rd, 2009 in co-location to the "re:publica" conference, brought together 77 participants from 11 different EU countries. Their self-set conference agenda included discussions and presentations covering Social Networks (Access Control, Netiquette, Human readable Privacy Policy), data protection among minors, eHealth and eGovernment as well as EU Projects like Fidis and PrimeLife.

This report focuses on the 3rd PrivacyOS conference, which was held in Vienna, October 26th and 27th 2009, co-located with the Austrian Big Brother Awards. 50 participants attended the conference and devised the agenda with 21 presentations in two parallel tracks. The topics of the presentations discussed included, amongst others: data protection awareness, data protection in healthcare, data protection in the Web 2.0, privacy-related technologies such as EnCoRe, TOR or Microformats as well as regulatory, cultural and sociological implications of data protection. Also at the 3rd PrivacyOS conference the software product "KiwiSecurity" was awarded the EuroPriSe Seal (European Privacy Seal, www.european-privacy-seal.eu). EuroPriSe is an initiative of the data protection authority Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD), Germany. It has been started as a European Project under the eTEN programme.

With participants from 10 EU countries (and one participant from the US) from different professional backgrounds, the talks given at PrivacyOS displayed a broad variety of views from a multidisciplinary perspective on privacy-related topics. Thus the goal of PrivacyOS to give partners and participants the opportunity to articulate and

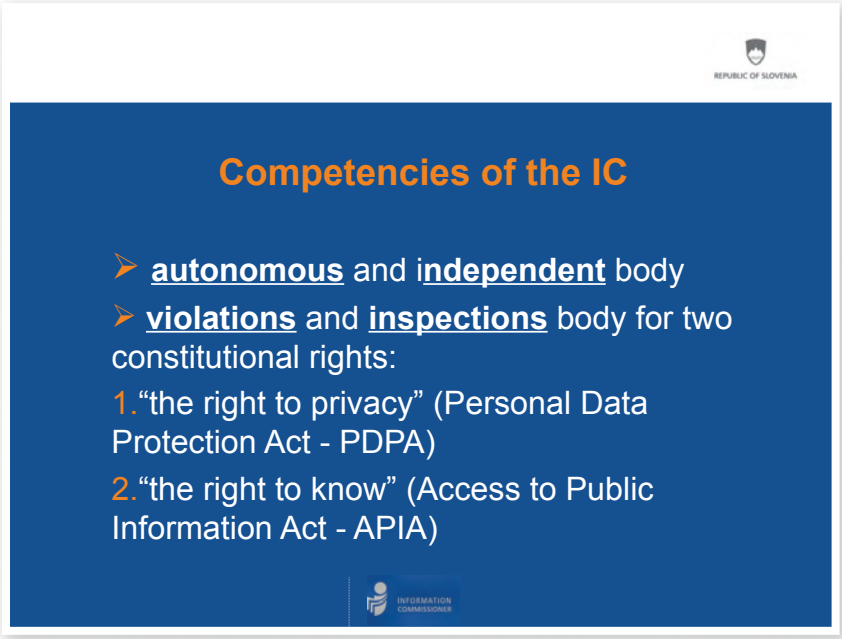
exchange best practices, challenges and solutions was achieved via presentations and discussions of the participants within and in between sessions.

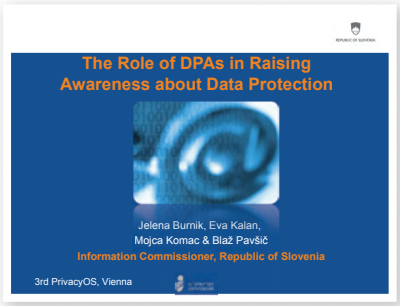
The 3rd PrivacyOS Conference started with an opening by its patron Hans G. Zeger. Zeger is chairman of Austria's most important privacy NGO, ARGE Daten. He focused "On the Way to Scoring Society". Zeger described how the growth of surveillance society challenges the classical "Security through Surveillance" paradigm and how we slightly shift towards an alibi and scoring society. He demanded extensive control of networks and enterprises by users and by civil society, stating that they "need precisely the kind of transparency for themselves [that] they impose on more and more people nowadays."

Presentations

1. The Role of DPAs in Raising Awareness about data Protection

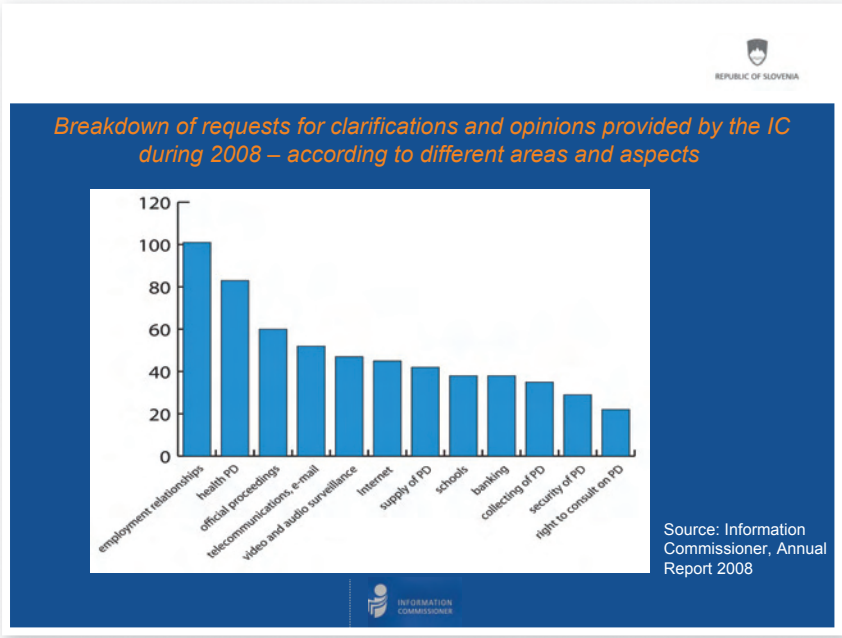
by Jelena Burnik, Eva Kalan, Mojca Komac and Blaz Pavsic (Information Commissioner of the Republic of Slovenia)





In this shared slot, two European Data Protection Agencies (DPAs), namely the Information Commissioner of Slovenia and the Spanish APDCM (Agencia de Protección de Datos de la Comunidad de Madrid), gave insights in their current activities and strategies.

The Slovenian delegation outlined the new challenges towards data and privacy protection and why these require further professionalization for DPAs especially in IT. Biometrics, road tolls and behavioural marketing/profiling pose current challenges to their DPA. The four speakers described their DPAs ambitious goal of answering every filed complaint or inquiry within 10 days.



Article 49 of the PDPA:

The IC may aiming at assuring publicity of its work and raising awareness:

- issue an internal journal and professional literature;
- publish its rulings, decisions, opinions; important courts' rulings and decisions; other important announcements;
- issue non-binding opinions on the compliance of codes of professional ethics, general terms of business or drafts thereof with regulations in the area of the protection of PD;

- issue and publish non-binding opinions, clarifications and positions on issues in the area of protection of PD;
- prepare and issue non-binding instructions and recommendations regarding protection of PD in individual fields;
- issue public statements on inspection supervision undertaken in individual cases;
- hold media conferences relating to its work.

Means of spreading public awareness

The IC is educating and informing:

- Individuals about their rights,
- Data controllers about their duties,
- General public on data protection issues,

USING THESE MEANS OF WORK:

- Communication with the media;
- Internet;
- Publications;
- Lectures, round tables, public debates (invited and self-initiated);

Communication with the media

- Crucial part of spreading public awareness!
- Interviews (important cases, impact of new tehnology on privacy, other privacy matters);
- Press releases (before/after important events, important IC and court decisions, international cases);
- Newspaper articles, professional articles, books, commentaries,..

INTERNET

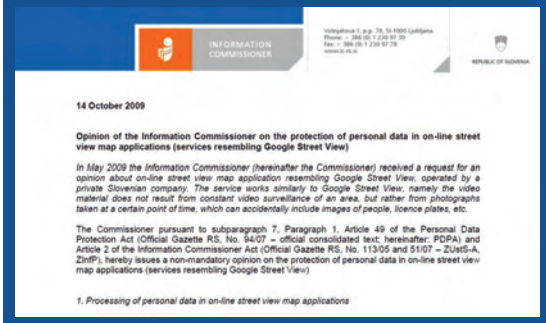
Content, dedicated to spreading awareness on personal data protection:

- Decisions, legal opinions and publication (guidelines, reports, articles, multimedia – special section for children);
- News and recommended reading;
- E-newsletter;
- Information technologies and personal data – special atterntion!!!

Opinion on services resembling Google Street View

Source: The Commissioner's website

http://www.iprs.si/fileadmin/user_upload/Pdf/razno/Opinion_of_the_Information_Commissioner_on_the_protection_of_pers



14 October 2009

Opinion of the Information Commissioner on the protection of personal data in on-line street view map applications (services resembling Google Street View)

In May 2009 the Information Commissioner (hereinafter the Commissioner) received a request for an opinion about on-line street view map application resembling Google Street View, operated by a private Slovenian company. The service works similarly to Google Street View, namely the video material does not result from constant video surveillance of an area, but rather from photographs taken at a certain point of time, which can accidentally include images of people, licence plates, etc.

The Commissioner pursuant to subparagraph 7, Paragraph 1, Article 49 of the Personal Data Protection Act (Official Gazette RS, No. 94/07 – official consolidated text; hereinafter: PDPA) and Article 2 of the Information Commissioner Act (Official Gazette RS, No. 113/05 and 51/07 – ZUstS-A, ZInfP), hereby issues a non-mandatory opinion on the protection of personal data in on-line street view map applications (services resembling Google Street View)

1. Processing of personal data in on-line street view map applications

- The service is likely to involve personal data processing
- Controllers must erase or anonymize (blur) personal data in the photographs in a way that the individuals won't be identifiable anymore

Information Commissioner's Website

www.ip-rs.si

Guidelines regarding privacy policies

Source: The Commissioner's website

Guidelines regarding introduction of biometric measures

Source: The Commissioner's website

Guidelines regarding identity theft prevention

Source: The Commissioner's website

Guidelines regarding data protection in the context of digital TV

Source: The Commissioner's website

Guidelines regarding protection against cyber bullying

Source: The Commissioner's website

PUBLICATIONS OF THE IC

- **Handbooks, brochures, guidelines**
- On crucial questions in the field of data protection
- Handbooks and brochures: 12 (some of them also in other languages beside Slovene: English, French, Russian, Croatian)
- A guide through data protection for parents and teachers;
- You decide! – a guide through data protection for youth;
- Schengen and your personal data;
- Access to my Privacy Denied!
- Guidelines: 15 published, 4 in the making
- Annual reports: 2005 – 2008

DECISIONS AND OPINIONS

- IC issue non-binding opinions, clarifications and positions on issues in the area of protection of personal data and publish them on the website;
- IC issued and published on website over 1700 opinions;
- Most opinions in the areas of data protection in
  enployment relationships,
  telecommunications,
  video surveillance,
  health data.

Results of wide activities for raising awareness

Rising number of applications and requests for the Commissioner's action

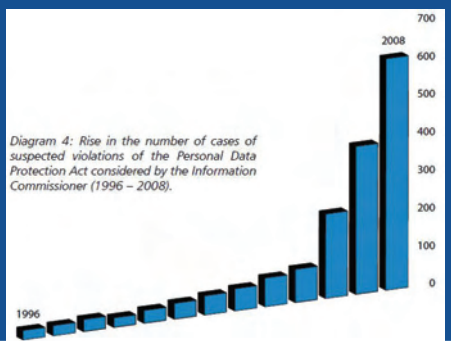


Diagram 4: Rise in the number of cases of suspected violations of the Personal Data Protection Act considered by the Information Commissioner (1996 – 2008).

Source: Information Commissioner, Annual Report 2008

Results of wide activities for raising awareness

Slovenian public opinion poll **"Politbarometer"** – the Commissioner enjoys high level of trust

European public opinion poll **"Eurobarometer" –** Slovenia ranks at the top regarding awareness of data protection issues

Results of wide activities for raising awareness

National "**Netko 2008**" award for best business and administrative web page

Future data protection issues and the Commissioner's role

Invisible and invasive electronic surveillance practices as a side product of ICT development:

- Biometrics
- Road pricing
- Behavioural marketing (internet, digital TV)

The Commissioner's role – follow closely all developments and assess their implications on privacy and data protection at the EARLIEST possible stage.

Room for improvement

Privacy Impact Assessments

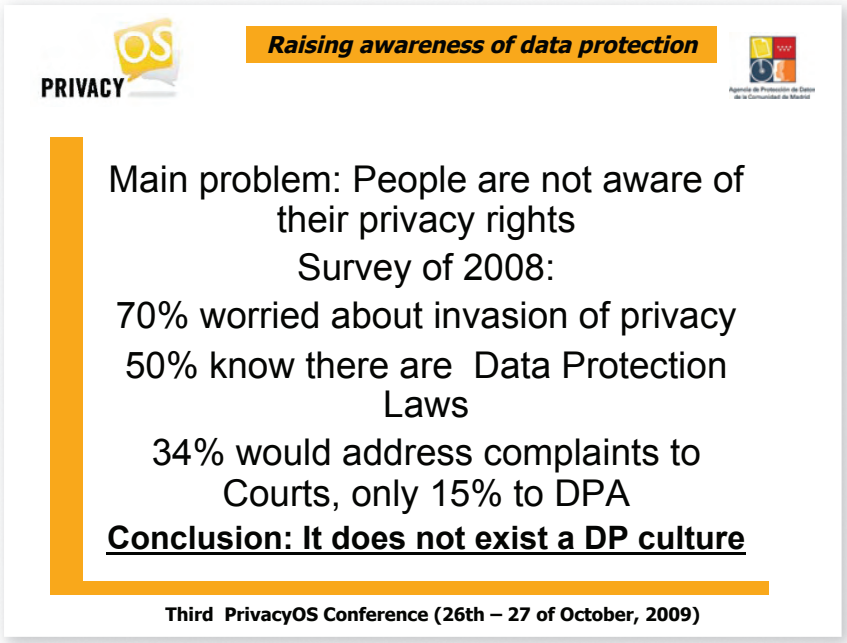
- Preventive action – care for privacy at all stages of a project which involves data processing
- Vital for IT products and services (case of Phorm)

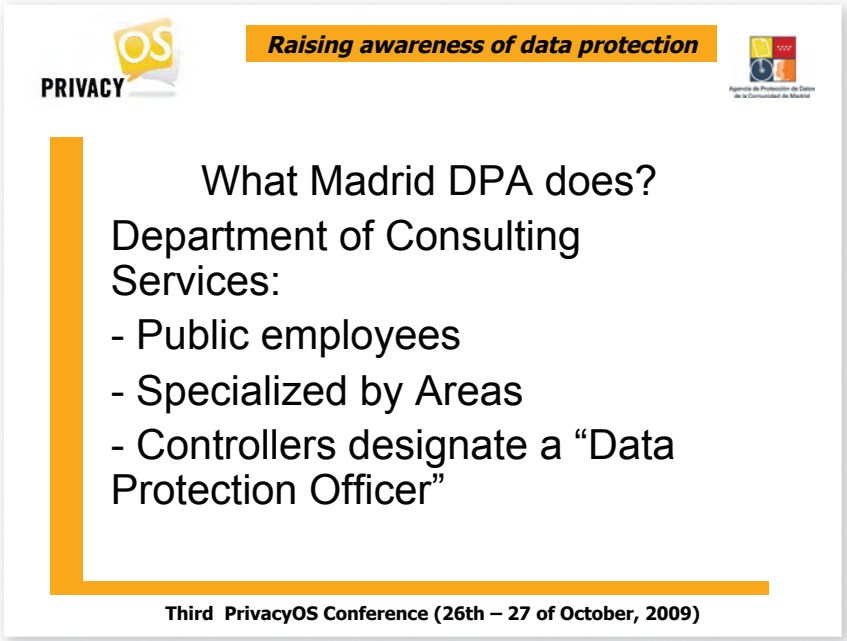
Certifying IT products and IT- based services

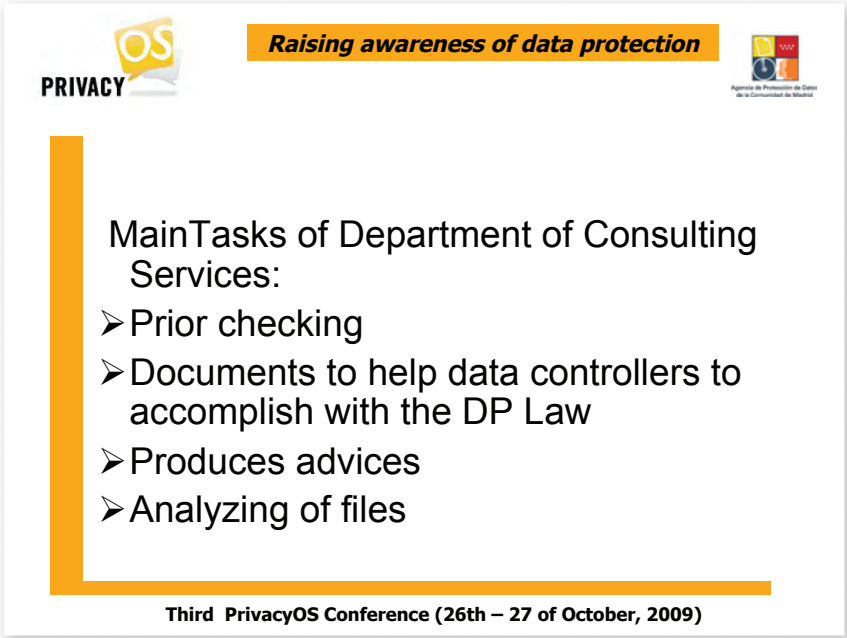
- Increased market transparency, trust in IT products and services

Thank you!

http://www.ip-rs.si







The Madrid DPA is working towards the establishment of a Data Protection Culture. Within the last 12 years, 40,000 public employees have been trained by them. The APDCM also provides an on-line support and e-learning platform for data controllers. This is well-grounded by a variety of classic dissemination channels, for example the production of several print and audiovisual publications, free digital reviews or such a yearly prize competition for Best Practice initiatives.

Both DPAs once more stressed the role of trans-European co-operation of DPAs, especially as regards awareness raising.

PRIVACY OS

Raising awareness of data protection

CUMPLE: a tool for helping controllers

PRIVACY OS

Raising awareness of data protection

Training courses:

- General and specific
- More than 40.000 civil servants trained in 12 years
- Linked to Sector Specific one day Seminars:

  - Education, Social Services, Health Services, Profesionnal Associations, City Councils, Security Measures

PRIVACY OS

Raising awareness of data protection

Attendance:
Social Services Day #272
Health Services Day #336
City Councils Day #129
Professional Association Day #147
Universities Day #129
Education Day #500 + #500

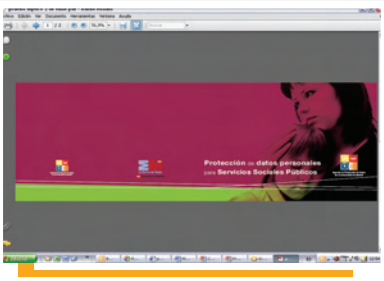
PRIVACY OS

Raising awareness of data protection

Publications:

- **Public employees guides**
- **Sector Handbooks on data protection**
- **Posters**
- **Brochures for health services and social services**

Third PrivacyOS Conference (26th – 27 of October, 2009)



Third PrivacyOS Conference (26th – 27 of October, 2009)

PRIVACY OS

Raising awareness of data protection

Publications (2):

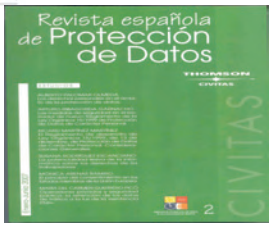
- On line reviews:
  - www.datospersonales.org
  - www.dataprotectionreview.eu
- Spanish Data Protection Review
- Monographs on data protection
- Annual Report

Third PrivacyOS Conference (26th – 27 of October, 2009)

Third PrivacyOS Conference (26th – 27 of October, 2009)

PRIVACY OS

Raising awareness of data protection



Third PrivacyOS Conference (26th – 27 of October, 2009)

PRIVACY OS

Raising awareness of data protection

Third PrivacyOS Conference (26th – 27 of October, 2009)

PRIVACY OS

Raising awareness of data protection

- Awards
  - European Award for the Best Public Practices in Data Protection. Fifth Edition (2008)
  - Award for the Best Scientific Paper on Data Protection
- Working Groups of Spanish DPAs

Third PrivacyOS Conference (26th – 27 of October, 2009)

PRIVACY OS

Raising awareness of data protection

Participation in European Projects:

- E-Prodat (Project leader)
- Europrise
- London Initiative
- DataProft

Third PrivacyOS Conference (26th – 27 of October, 2009)

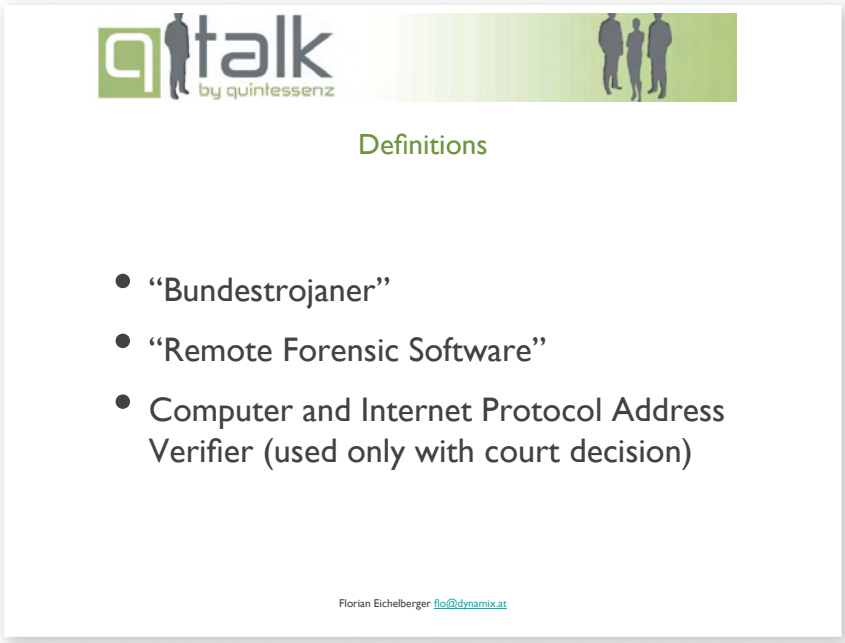
PRIVACY OS

Raising awareness of data protection

Recommendations and guidelines:

- Security measures for non computerized files of Social Services and Health Services
- Using of the census by City Councils
- Surveillance
- Publication of personal data in internet
- Using of personal data in e-government services

Third PrivacyOS Conference (26th – 27 of October, 2009)



In the parallel session, titled "The Spy at Home: Remote Forensic Software", Florian Eichelberger of Austrian privacy activist organization quintessenz e.V. informed about the possibilities and problems of so-called remote forensic software (RFS) in law enforcement. US-based law enforcement agencies are already allowed to use technologies such key loggers, Trojan horses or web traffic interception. The speaker dealt with the current (legal) situation in Austria in detail.

by Florian Eichelberger, quintessenz e.V.

Keylogger

- Keylogger Hardware
- Keylogger Software

Florian Eichelberger flo@dynamix.at

Trojans

- Netbus
- Optix Pro
- ERA IT Skype Trojan

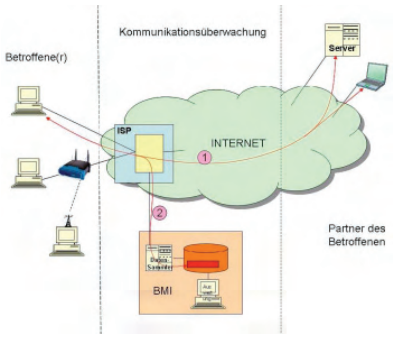
Florian Eichelberger flo@dynamix.at

How will they try to eavesdrop on people

- Keylogger (Hard / Software)
- Trojan (z.b. “Skype Trojan”)
- Remote Admin Software
- Surveillance at the ISP
- (Use of electromagnetic emission)

Florian Eichelberger flo@dynamix.at

Surveillance at the ISP



Florian Eichelberger flo@dynamix.at

Deployment

- Either remote oder local
- USB Sticks, Emails, CD’s
- Exploits / OS / Applikationen
- Man in the Middle

Florian Eichelberger flo@dynamix.at

Status Quo

There is no legal ground:

- Current regulation regarding searches (§§ 117 Z 2, 119 bis 122 StPO), do not allow for covert or "hidden" searches.

Source
http://www.justiz.gv.at/_cms_upload/_docs/AG_OnlineDurchsuchung_Endbericht.pdf

Florian Eichelberger flo@dynamix.at

Fundamental Problems (Technics)

- Forensic Problem with accountability
- Who created the data ?
- Are we spying on the right person ?
- Because of changing of the system, is this still valid evidence ?
- Traceability ?

Florian Eichelberger flo@dynamix.at

Fundamental Problem (Law)

- Secrecy / Privacy
- Surveillance of "protected" persons like priests, medical doctors, lawyers.
- Presumption of innocence
- Changes on the PC -> Weakening of evidence

Florian Eichelberger flo@dynamix.at

Terrorism

- Why not useful ?
- "Nobody is a terrorist until he committed an act of terror."
- Examples

Florian Eichelberger flo@dynamix.at

Illegal Pornography

- Without any evidence or suspicion, only widespread trojans will work at all.
- Established law enforcement methods are sufficient

Florian Eichelberger flo@dynamix.at

Nazi / Hooligan

- Why not
- Established law enforcement methods are sufficient
- Coordination from foreign countries / Mobile Phones / personally

Florian Eichelberger flo@dynamix.at

Fundamental Problem (Social)

- Abuse through the government
- In Berlin an agent of the secret service seems to have abused it
- http://www.berlinonline.de/berliner-zeitung/archiv/.bin/dump.fcgi/2007/0831/politik/0062/index.html
- Pot. Abuse by criminals.
- Bursting of a dam / broadening the use in a step-by-step tactics

Florian Eichelberger flo@dynamix.at

Detection and Protection

- Brain 2.0
- General Rules for safe working on a PC
- Full Disk Encryption
- Generic Detection Software
- Maybe more then 1 computer where only one is placed in an obvious location.

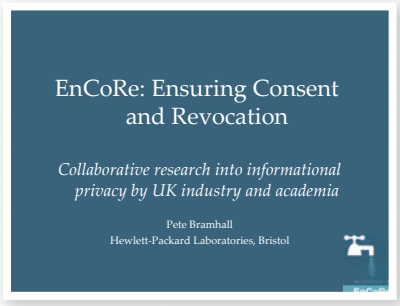
Florian Eichelberger flo@dynamix.at

Questions ?

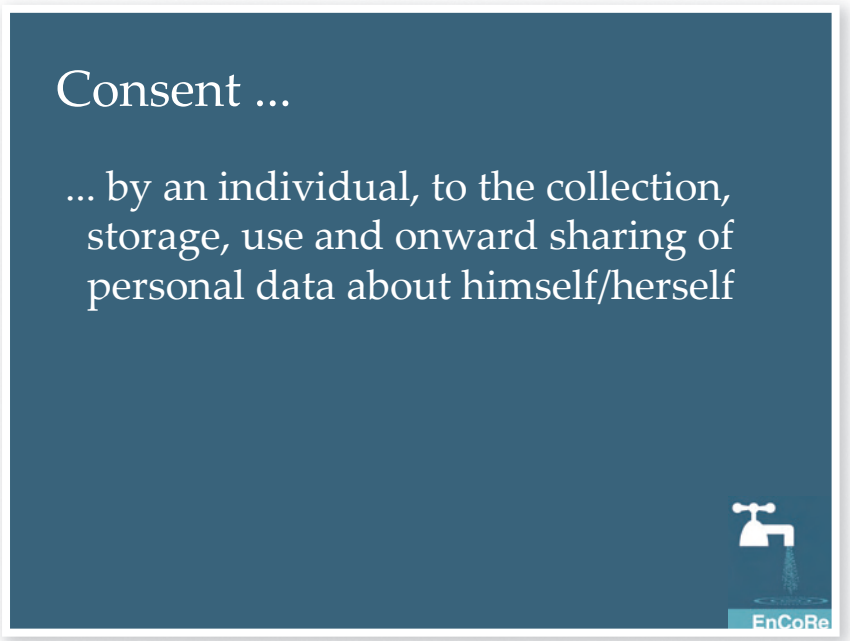
Florian Eichelberger flo@dynamix.at

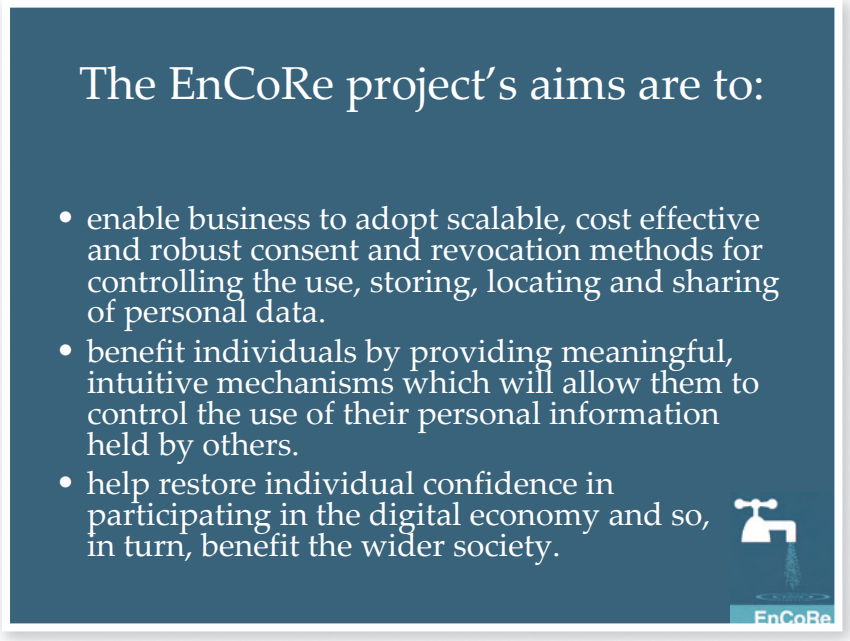
4. Ensuring Consent and Revocation: UK´s EnCoRe Project

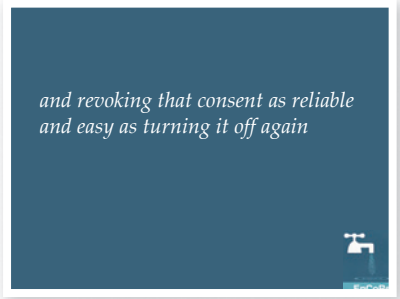
by Pete Bramhall, HP Labs



On behalf of Hewlett-Packard Laboratories UK, Pete Bramhall presented on the EnCoRe research project. This three year project aims to create mechanisms that enable data processors to obtain customers consent to data collection, storage,

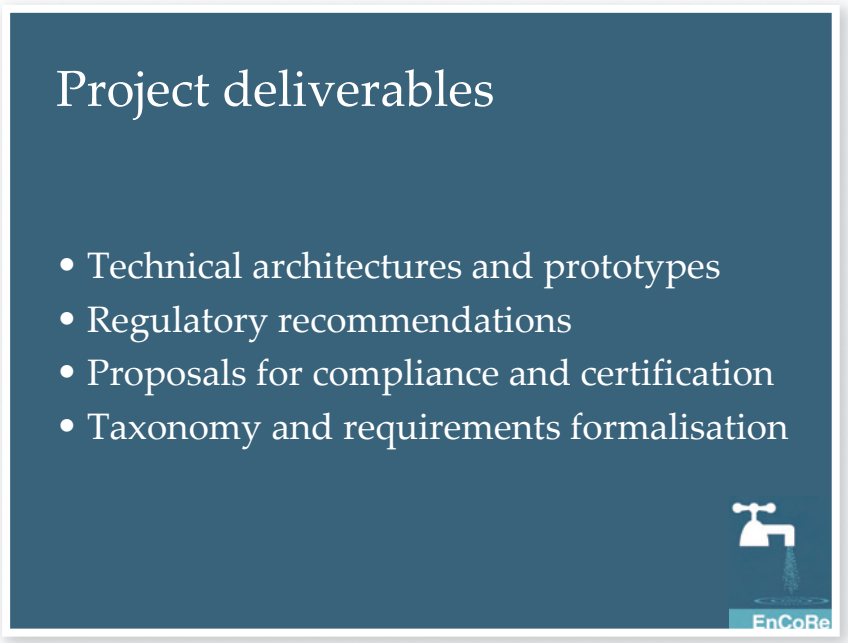






use and sharing in a convenient, reliable and revocable way. To illustrate this goal, the speaker used the picture of turning on and of a tap for allowing or revoking consent.

Among the project outcomes there will be technical architectures and prototypes, regulatory recommendations, compliance and certification proposals as well as taxonomy and requirements formalisation efforts. Bramhall explained the regulatory, business, end-user and technological challenges and informed about the current project status.



Research methodology

- Three case studies, each on a different scenario:
  1. Enhanced employee data sharing
  2. TBD – candidates are:
     1. Biobanks
     2. Assisted living
     3. ITSO – Public transport payment card system
     4. Smart metering
     5. Cloud computing
  3. TBD – candidates as above

EnCoRe

Challenges

Some challenges around consent by individuals, to the storage, use and sharing of their personal data:

- Regulatory challenges
- Business challenges
- End-user challenges
- Technological challenges

Regulatory challenges

- The explicit right to revoke consent to the processing of personal data by others is limited
- Lack of relevant case law and soft law limits this to being an implied right to withdraw consent

Enhanced employee data sharing

Scenario:

- Employer uses an external service ("WorkBook") to facilitate both internal work-related collaboration and external benefits management for employees
- Personal data is exchanged between employer and the WorkBook service provider
- Employees manage their WorkBook profiles and consents/preferences

EnCoRe

Business challenges

- "I know when I did my training one of the things I was told was that processing under consent is what the desperate resort to"
- Is business ready to buy-in to EnCoRe functionality?

End-user challenges

- "Natural consumer behaviour"
- "I never read the terms of agreement, not at all, it doesn't really interest me"
- "You needed an average reading age of like 27 to read the average privacy policy"

Enhanced employee data sharing

Use cases explored and supported by the technical architecture:

- Mary is hired at Company X, in UK
- Mary changes some of her personal data (profile)
- Mary starts using the company's "WorkBook" service
- Mary elects to allow a subset of her "WorkBook" data (her public profile) to be given to external organisations
- Mary uses the "WorkBook" service to book holidays
- Mary changes her preferences in the "WorkBook" Service
- Mary leaves the company

EnCoRe

Technological challenges

- How to ensure the consent/preference metadata sticks to the personal data it refers to?
- Integration with legacy systems

Project status (October 2009)

- Formalisation work on consent and revocation requirements in progress
- Taxonomy for consent and revocation in progress
- Five requirements-gathering workshops held
- Initial analysis of UK law re consent and revocation, with a focus on employee data
- Technical architecture V1 complete
- Compliance process design in progress

www.encore-project.info

http://www.twitter.com/encore_project

Background

- Based on research for the EU Project - Program on Fundamental Rights and Citizenship - "Information and Sensitization of Young EU Citizens on the Protection of Their Personal Data"

+

- Some comments on the recent Constitutional Court Decision on the data retention law

Elements of Methodology (1)

- **Starting Point Sources:** APTI's experience, EDRI-gram articles (www.edri.org/edrigram), news from other NGOs
- **Interviews (Bucharest, 06-08.2009):** Georgeta Basarabescu – President Romanian DPA, Alina Savoiu – Head of Legal department Romanian DPA (08.2009), other NGOs with activity on this field (ActiveWatch, Center for independant Journalism), forensic and cybercrime experts
- **Specific research on sources:** official documents, Parliamentary debates, Reports, public data, relevant organizations websites, press, etc.
- **General remark:** there is very little public information available on the public or private databases ; awareness among privacy concerns very low.
- **Other sources:** Survey on 60 young people (age 15-18) from 3 major cities – Bucharest, Craiova and Constanta on their usage of social networks and social networks danger**s.**

Elements of Methodology (2)

Selection of issues:

3 fact sheets: Biometric Passports, National DNA Database; Telecom Data Retention.
- A general overview of the social networks specifics in Romania: Some local social networks, but not the most used .

- Selected from the most publicly debated issues, comparative analysis goals, highlighting mutual influence between EU and national level.

- Other missing issues could not have been completed to to lack of public information, or impossible to get in a reasonable timeframe (e.g. Plans for biometric ID card, CCTVs in schools)

Supplementing the DPA reports from Slot 1, Bogdan Manolea (EDRi) reported on the state of privacy and data protection in Romania from a NGO perspective. After a short introduction into Romania's privacy politics, the speaker went into detail on three of the most present topics in Romanian DPA activities: Biometric passports (which are in a project pilot in one Romanian province and heavily disputed), national data retention legislation for telecommunication providers (which suffered from negative media coverage and is challenged by NGOs), and the national DNA database.

In conclusion, Manolea urges for the Romanian DPA to become more active in the process of awareness rising. In addition he opts for a stronger and more respected position of the DPA within the legal framework and political system of Romania.

by Bogcan Manolea, APTI-Romania / EDRi

General Context

DP Act 2001: transposition of DP Directive

DPA: Romanian DPA (ANSPDCP) – Autoritatea Nationala de Supraveghere a Prelucrarii Datelor cu Caracter Personal – set up in 2006, before that date - Ombudsman

Limited surveillance, due to incapacity of the Government to implement national projects.

Plenty of legislation – lack of information on how is applied, secondary legislation or its impact.

DP Act – still little implemented also by private sector

Mainstream media becoming interested on Privacy only on specific projects and then sending wrong information:

- Biometric passports (in)famous 666 number
- Data Retention directive (keeping the content of the communication)

Limitations in Practice (1)

- DP Act – a translation of the Data Protection Directive

- Its implementation basically started in 2006, following presure from the EU accession process

- DPA - small organisation (35 people in August 2009, covering the entire teritory, limited powers by law, no obligation to ask for its authorization or opinion before creating a database or law (but legislation in preparation), opinion not public

- Wide scope: DP Act, Privacy and E-Communications Regulations (e.g. spam, profiling,…), Data retention law

- DPA sees itself as a „register for controllers" rather than a privacy-orianted organization. Based its activities on inspections, rather than awareness.

-DPA – limited in staff and below average payment (generic for public sector in Romania) , but open for collaboration

- No NGO focused only on privacy (or with major parts on privacy issues), general Human Rights, FoE or Access to Information issues. Or Digital civil rights (APTI)

Limitations in Practice (2)

- No special awareness for youth sector

- As regards Internet privacy, basically no information in Romanian. However a lot of young people learn by themselves the basic protection methods if they are interested, but difficult to get to „complicated" issues (e.g. encryption)

- Major lack of awareness – EuroBarometer

• 79% of the Romanians have no idea that there is a law in the field of personal data.
• Romania is number one in EU countries with the percentage of the people (47%) not knowing that there are laws allowing you to have access to your personal data kept by others.

Main Findings

- Young adults not specifically targetted, but particularly concerned in some cases (data retention; Social Networks: biggest use age segment are 18-25 and 13-18)

- Social networks privacy could be a big boom: - most used network – HI5 based only in US, 2.25 m accounts from Romania (37% of the Romanian Internet users have a hi5 account). Most active segments are the users with ages between 18-25 (45.9%) of the users, then the users between 13-18 years old (26%) and 25-35 years (20.9%)

- New measures with no proper explanation or studies (Biometric passports for children over 6 years old)

- Not clear how to respect the DP act in several important circumstances (obtaining and keeping the DNA before the DNA Database act)

Biometric passport

- Application just in a Pilot Stage (one county – Ilfov) – deployment by the end of the year
- Nationals over 6 years old: a 5-years passport, with biometric; under 6 years: a 3-years passport, WITHOUT fingerprints
- Major disfunctionalities in first implementation (no notification, keeping 10 fingerprints, keeping all the application no access logs)
- Public protests related to religious beliefs (The Romanian Orthodox Church was forced to speak on the subject)

Data retention law

- Adopted as a consequence of the data retention directive – Law 298/2008
- Low public discussion within MCSI and the Parliament debate
- Public Outcry when the law entered into force (including in public protests and media)
  - Complaints on „keeping the content of communications”
  - Complaints from prosecutors on a procedure too complicated

Data retention law (2)

- Several NGOs decided to challenge the law
- To the Ombudsman (that may bring the case to the Romanian Constitutional Court (CCR))
- To make a „mock case" in order to raise a non-constitutionaly motion
- Civil Society Commisariat vs. Orange Romania
- Motion sent to CCR in March 2009
- CCR – formed by 9 persons ; traditionalists

Data retention law (3)

- Decision of the CCR on 7 October 2009, but no official press release
- Motion Admitted or Admitted in part ?
- Outside factors
  - Social unrests
  - Public debates
  - Communist experience (?)
- Decision to be published in the Official Monitor
- (Old) Govt reaction – changing the law....

Subscribe to EDRi-gram

Bi-weekly newsletter on European digital civil rights !
Free !!

www.edri.org/edrigram

Mulțumesc !
(you've just learn to say Thank You in Romanian)

Bogdan Manolea

bogdan at edri.org

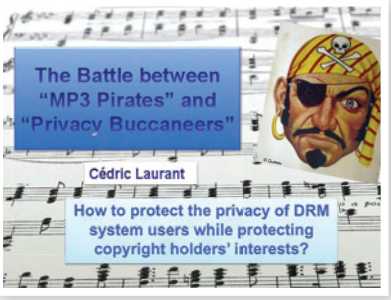
Conclusions

- DPA needs to be encouraged to be more public and to have pro-active actions + awereness actvities. More staff and resources are esential for a proper implementation of the DP act.

- Stronger legal objectives for the DPA, including obligation to get its opinion and publication of this opinion in the Official Monitor
- Public assesments on the implementation of law
- Basic awareness of children and youth-related privacy issues, especially in relation to Internet
- Waiting for the Constitutional court decision to assess its value (... and then to react)

Outline

- Introduction
- DRMS
  - When? Since when? What? How (do they work)? Who (are its stakeholders)? With whom (consumers) ? Why? (Advantages of DRMS) What next?
- Threats of DRMS for individuals' privacy (and solutions under discussion)
  - The law applicable to protect DRMS users' privacy
  - The right to privacy and data protection; the right to anonymity; how the law applies to DRMS
- Enforcement of data protection laws >< Enforcement of copyright laws
- Towards new solutions to protect DRMS users' privacy
- Suggestions for future work
- Conclusion



Introduction

- Core Issue C: Enabling privacy on the web
- What this presentation is not about:
  - Defending or attacking the downloading of MP3 files on P2P file-sharing networks;
  - Discussing copyright law (limitation of scope of "fair use") when using DRMS.
- What this presentation is about:
  - Compare the interests of data subjects (privacy) and the interests of copyright holders.

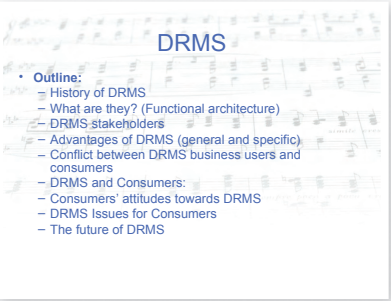
Independent privacy consultant Cédric Laurant investigated the question of how to balance Digital Rights Management (DRM) systems between user privacy and copyright protection in his presentation titled "The Battle between 'MP3 Pirates' and 'Privacy Buccaneers'".

Outlining the history of DRM systems, the speaker stated that they were invented tackle with paradigm changes that came along with the vanished reproduction cost of digital contents. DRM were thought to

DRMS: History

- The networked digital age has made it possible to do just about anything to digital content and at a very limited production cost.
- Great opportunities for new business models focused on creating and producing digital works.
- But threats to the livelihood of creators and artists?

➢ Need for a technology that would enable the secure creation, management, distribution and promotion of digital content on the Internet.



DRMS: Stakeholders

- Government Agencies
  - Interested in controlled viewing and sharing of highly secure and confidential documents, audio and video data.
- Private Corporations
  - Want to limit the sharing of their proprietary information.
  - Track access and any modifications made to proprietary information.
- Owners of commercial content
  - Owners of works of authorship, artists, and publishers: want to gain revenue through sale and promotions.
  - But are concerned about protecting their copyrighted works from unauthorized use.

DRMS: Stakeholders

- Intermediaries (service providers, content distributors,…)
  - Want to minimize costs of providing services.
  - Are concerned about protecting themselves from lawsuits over illegal distribution.
- Producers of end user equipment (PCs, players, etc.)
  - Concerned about minimizing design and production costs.
  - Unwilling to pay for features that only some users need.
- End users
  - Interested in immediate access to desired content.

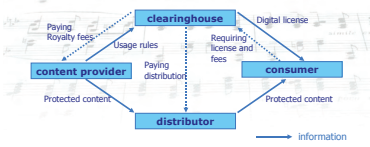
be the foundation for new business models for the producing industry, but turned out to pose various threats to creators and artists as well as to the users.

He described which stakeholders involved in a typical DRMS, mentioning and differentiating clearinghouses, distributors, content providers, rights owners/creators, consumers/end users, producers of end user equipment (players etc.) and possibly government agencies and regulators.

As for the advantages of DRMS, which allow for users licence validation by rights owners, Laurant summarized: downstream use (delivering controlled access top-down), the possibility for temporal modification of rights, outsourcing possibilities with responsibilities and license

DRMS: What are they?

Overview of a typical DRMS model



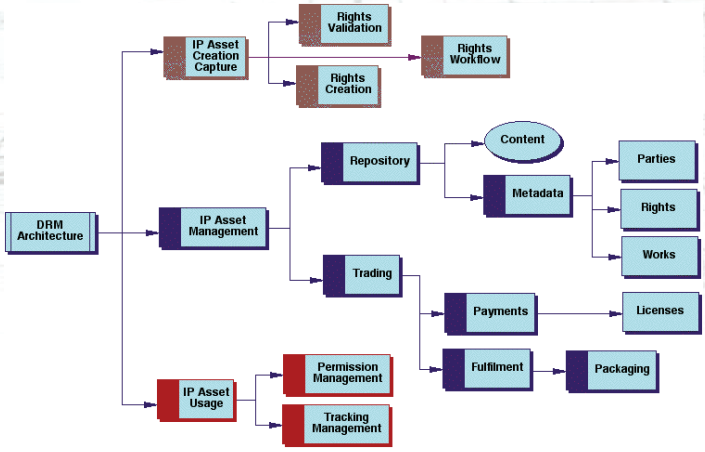
Graphic from: Qiong Liu, Reihaneh Safavi-Naini and Nicholas Paul Sheppard, "Digital Right Management for Content Distribution" (2007)

DRMS: What are they?

- Set of technologies that enable owners of digital works to specify and control:
  - the access they want to give consumers and
  - the conditions under which it is given.
- It includes:
  - **Persistent Protection:** technology for protecting files via encryption and allowing access to them only after the entity desiring access has had its identity authenticated and its rights to that specific type of access verified
  - **Business rights:** Capability of associating business rights with a content by contract, e.g. author's rights to an article or musician's rights to a song
  - **Access tracking**: Capability of tracking access to and operations on content
  - **Rights licensing**: Capability of defining specific rights to content and making them available by contract

DRMS: What are they?

Functional Architecture



Graphic from: Tipsy Talwar, "Digital Rights Management" (2004).

DRMS: What are they?

Functional Architecture

- **IP Asset Creation and Capture Module**
  - Rights Validation to ensure content being created includes the rights to do so.
  - Rights Creation to allow rights to be assigned to new content.
  - Rights Workflow to allow for content to be processed through series of workflow steps.
- **IP Asset Management Module**
  - Repository functions to enable the access/retrieval of content in potentially distributed databases and the access/retrieval of metadata.
  - Trading functions to enable assignment of licenses to parties who have traded agreements for rights over content, including payments from licensees to rights holders (e.g., royalty payments).
- **IP Asset Usage Module**
  - Permissions Management to enable usage environment to honor the rights associated with the content (only print document or view document once, without copying rights).
  - Tracking Management to enable monitoring of usage of content where such tracking is part of the agreed to license conditions, e.g., user has license to play video 10 times.

(Extract from: Tipsy Talwar, "Digital Rights Management" (2004).)

Consumers' attitudes towards DRMS

- **In**formed **Di**alogue about Consumer **A**cceptability of Digital **R**ights Management Solutions in **E**urope ("INDICARE")'s work
  - Open dialogue of stakeholders

(See Dr. Carsten Orwat, "Analysis of Consumer Issues and Paths for Concrete Approaches" (2005))

DRMS: Advantages
Control Access During Workflow

- Critical function of DRMS: **controlling allowed uses** of digital works of authorship **during workflow**.
- DRM technology extends and enhances the traditional role-based access by predetermining and controlling the exact use(s) of content.
  - *Example*: A draft manufacturing guideline circulated among an international standards committee to which are participating various companies. Using DRM technology, this can become a closed, circulation. The draft guidelines are in a tamper-proof format, with print-only user-rights, limited to a pre-determined timeframe, after which the draft is withdrawn and replaced by the final set of guidelines. The owner of the content, here the standards committee, can withdraw, alter, or grant permissions related to the content at any time.

DRMS: Advantages
Downstream Use

- Companies are able to **deliver controlled access downstream** so that their works of authorship can be licensed, deployed and repurposed by business partners **in accordance with terms of agreements**.
  - *Example*: Music publishers license DRM-enabled content to online transactional or subscription services. The DRM-enabled content allows both distributors and consumers to choose from multiple fee/free business models. For example, the content could be included in both the free-play list for one-time use on multiple devices, or it could be licensed on a fee-for play use by media companies, publishers corporate, government or institutional users. Further, with DRM-enabled content, owners may chose to permit licensees the ability to re-distribute or enter into republication agreements.

Consumers' attitudes towards DRMS

"Common Sense:

- Consumer acceptability is key for business success
- Consumer confidence and trust in services is pivotal
- Several deficits in consumer acceptability can be observed"

DRMS: Advantages
Modification of rights over time

- Systems must be able to accommodate changes by updating parameters of rights and usage as needed to accommodate new distribution models.
- Lack of ability to change access rights to content can be a serious business liability, cost a lot of money and be a disincentive to customers.

➢ DRMS can facilitate collaboration by persistently protecting critical copyright beyond business process of corporate organizations.

DRMS: Advantages
Regulatory and Business Standards

- Legislative and regulatory standards include security and privacy requirements

➢ DRMS solutions are able to offer assurance that processing operations on documents including personal data comply with the most current regulatory regimes on privacy and security.

DRMS Issues for Consumers

- Access and usage
- Transparency
- (Interoperability)
- (Privacy)

DRMS: Advantages
Outsourcing with responsibility

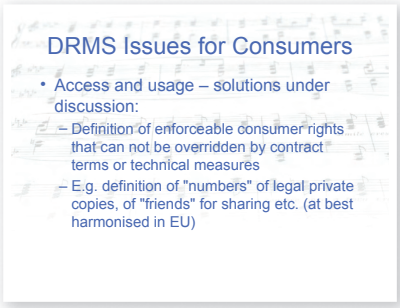
- Offshore processing and data-conversion service bureaus have long been a staple of trade, technical, professional and database publishers.
- Software and entertainment products are routinely outsourced. Growing trend to rely on outsourced personnel for the roles companies traditionally reserved for employees.
- Many people working on digital content products and processes do not necessarily have the same loyalty to the company.

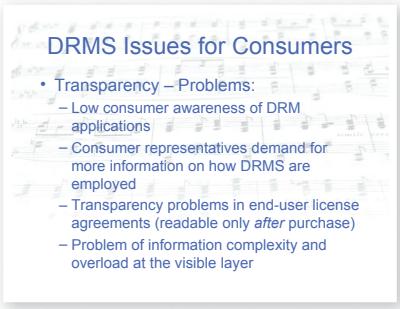
➢ DRMS can assure appropriate levels of accountability.

DRMS: Advantages
Protection throughout Content Lifecycles

- DRMS are able to protect against unauthorized use of software, music, film, images, videos, etc.
- They save on company time and resources that would be required upstream to detect and defer theft.

➢ DRMS-enabled protection can continue throughout the distribution of the content, auditing of its use, and accounting for its fees and licenses.





protection throughout the complete product lifecycle.

On the other hand DRM yields several threats for the individual's privacy, for example: massive dissemination of digital traces, the loss of anonymity through payment information disclosure, the risk of detailed personally identifiable user profiling by the service provider (e.g. music stores), the possibility of behavioural targeting through data mining. Last, but not least, the aggregation of non-sensitive data items could result in a data

The law applicable to protect DRMS users' privacy

- **Right to privacy and data protection**
  - Claim for privacy: the claim of individuals, groups and institutions to determine for themselves, when, how and to what extent information about them is communicated to others (Alan Westin)
  - 3 dimensions of privacy:

    1) **Personal privacy:**

    Protecting a person against undue interference and information that violates an individual's moral sense

    2) **Territorial privacy:**

    Protecting a physical area surrounding an individual that may not be violated without the acquiescence of the person

    3) **Informational privacy:**

    Deals with the gathering, compilation and selective dissemination of information

How data protection law applies to protect the privacy of DRMS users

- The law and how it is applied to DRM applications:
  - Data must be processed **fairly and lawfully**.
    - **Fairly**: not collected through surreptitious practices (cfr Flash "super-cookies").
    - **Lawfully**: EU regulations are breached when personal data is collected from EU-based data subjects without their unambiguous consent.
  - They must be collected for **explicit and legitimate purposes** and used accordingly.
    - **Explicit**, not with misleading language: "to enhance your consumer experience".
    - **Legitimate purposes**: not to sell your preferences for hard rock music to tatoo parlours.
  - Data must be **relevant and not excessive in relation to the purpose** for which they are processed.
    - **Relevant and not excessive**: not to use your music preferences to mine listeners' behavioural patterns to then sell it to third parties.

How data protection law applies to protect the privacy of DRMS users

- The law and how it is applied to DRM applications:
  - Data must be **accurate** and where necessary, **kept up to date**.
  - Transparency requirement: data controllers are required to provide reasonable measures **for data subjects to rectify, erase or block incorrect data about them**.
    - How can data subjects **correct inferential information** held about them and used to make decisions about them?
  - Data that identifies individuals must **not be kept longer than necessary**.
  - Special categories of personal data ("**sensitive personal information**")
    - Sensitive personal information: Are music choices per se sensitive? Is what could be inferred from them sensitive? Where to draw the line?

The law applicable to protect privacy of DRMS users

- The law:
  - Data must be processed **fairly and lawfully**.
  - They must be collected for **explicit and legitimate purposes** and used accordingly.
  - Data must be **relevant and not excessive in relation to the purpose** for which they are processed.
  - Data must be **accurate** and where necessary, **kept up to date**.
  - Transparency requirement: data controllers are required to provide reasonable measures **for data subjects to rectify, erase or block incorrect data about them**.
  - Data that identifies individuals must **not be kept longer than necessary**.
  - Special categories of personal data ("**sensitive personal information**")

Enforcement of data protection laws >< Enforcement of copyright laws

- Enforcing copyright laws aims at stopping the infringement of copyright (unauthorized uploading of files on P2P file-sharing networks, unauthorized copy outside the scope of "fair use", etc.).
  - → Copyright holders must know the infringer's identity and whereabouts necessary to bring lawsuits (identity and address information, "I&A information").
- Enforcing data protection laws aims at preventing unauthorized processing individuals' personal data and their further dissemination.
  - → Data subjects must know that their I&A information will be lawfully protected.
- Conflict of interests between copyright holders and data subjects about the data subjects' personal data.
- Enforcing both laws while solving the conflict of interests would logically lead one to entrust the I&A information of data subjects with third parties and strengthen the enforcement of data protection laws against copyright holders.
- Who could be those "third parties"?

Towards new solutions to protect DRMS users' privacy

- But if **identity** is not to be disclosed, how could **authentication** occur?
- Because **authentication DOES NOT IMPLY identification**.
- Difference between "identification" and "authentication".
- More areas of life will require authentication without identification.

The law applicable to protect DRMS users' privacy

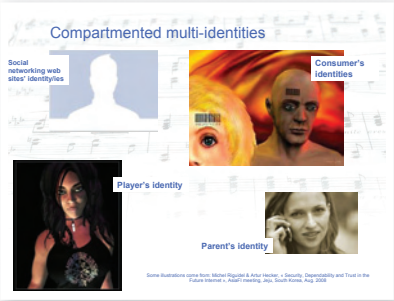
- **Right to anonymity**
  - Negative aspects:
    - May lead to abuses
    - Encourages lack of accountability
    - Avoids legal process
    - "I don't have anything to hide"
  - Positive aspects:
    - Promotes free speech
    - Protects individual freedom
    - Encourages diversity (in behaviours, opinions, communities)
    - Prevents conformism

Towards new solutions to protect DRMS users' privacy

- Identity management tools with third parties acting as an intermediary between copyright holders and data subjects.
  - De-identified personal data would be held by DRM data controller and personal data (especially the "identity and address" information) would be held by third parties.
  - Concerns:
    - Who decides the criteria to release the identity and address information?
    - Who can be those third parties? Judicial? Administrative?
    - Who would run them?

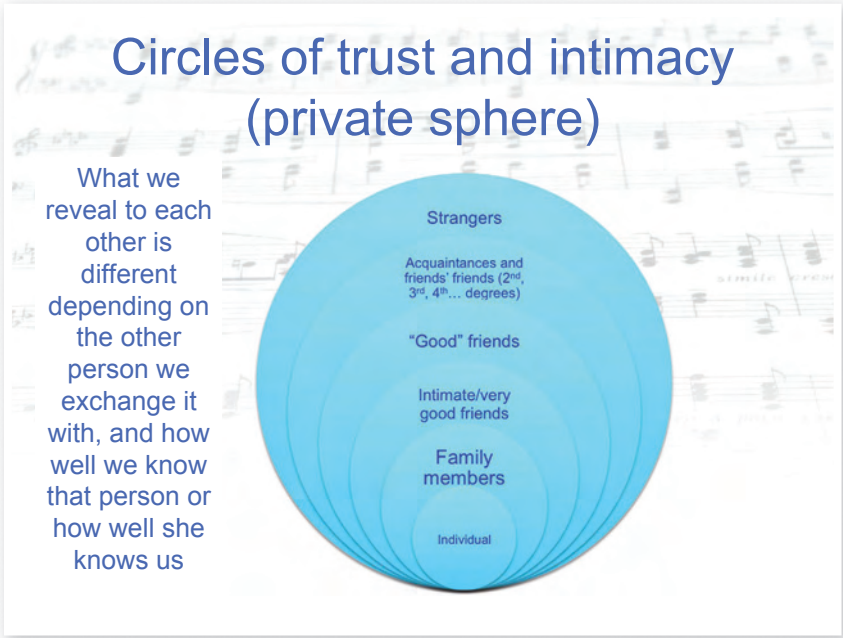
Towards new solutions to protect DRMS users' privacy

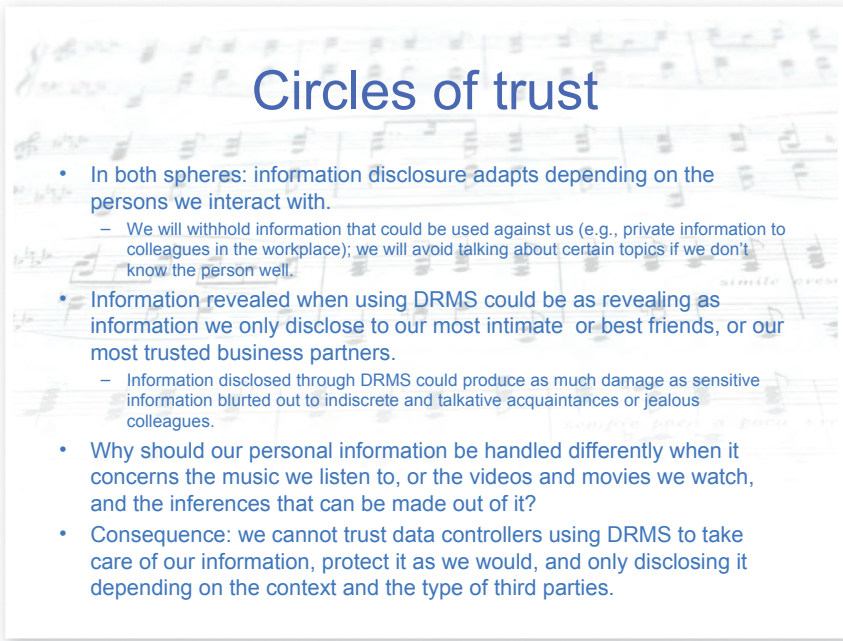
- Self-regulation? Business sectors' codes of conduct?
- New laws implementing the European Data Protection Directive?
- More global data protection rules and standards
- More globally harmonized technical solutions (to better handle transborder violations).



set which is to be regarded as sensitive information.

In conclusion, the speaker stressed the key paradox in the relation of DP laws to copyright laws: Accountability vs. Anonymity. Several possible solution approaches are proposed: First, a paradigm change for DRMS is necessary, so that they won't be based on identification but on authentication. Second, (compartmented) identity management concepts could help to resolve the paradox. Furthermore, effective self-regulation, possibly in form of an industry code of conduct and a more privacy-aware and proactive customer will improve the situation.





Towards new solutions to protect DRMS users' privacy

- Technical privacy controls (PET's): **to protect a user's identity/ies** via:
  - **Anonymity:** a user may use a product/service without disclosing his identity
  - **Pseudonymity:** a user may use a product/service by acting under a pseudonym
  - **Unobservability:** a user may use a resource or service without others being able to observe that the product/service is being used
  - **Unlinkability:** sender and recipient cannot be identified as communicating with each other

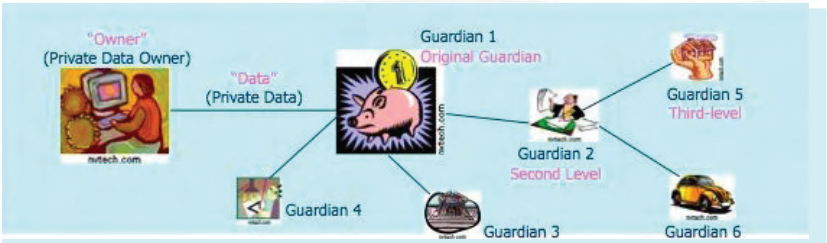
Towards new solutions to protect DRMS users' privacy
- Privacy-enhancing technologies?
  - Technical privacy controls: (Simone Fischer-Hübner)
    - to protect a user's identity/ies
    - to protect a usee's identity/ies
    - to protect the confidentiality & integrity of personal data

Towards new solutions to protect DRMS users' privacy

- **Technical privacy controls (PET's): to protect a usee's identity/ies via de-identification of data subjects**
  - **Perfect** de-identification:
    - Data is rendered anonymous in such a way that the data subject is no longer identifiable
  - **Practical** de-identification:
    - The modification of personal data so that the information concerning personal or material circumstances can no longer or only with a disproportionate amount of time, expense and labor be attributed to an identified or identifiable individual
  - **Controls** for de-identification include:
    - Privacy-preserving methods for data mining software

Towards new solutions to protect DRMS users' privacy
- **Technical privacy controls (PET's): to protect the confidentiality and integrity** of personal data via, e.g.:
  - Company privacy policies' security measures (encryption, etc.)
  - Specific tools (P3P: Platform for Privacy Preferences)

Towards new solutions to protect DRMS users' privacy



- "Guardian:"
  Entity entrusted by private data owners with collecting, processing, storing or transferring their data
  - owner can be an institution or a system
  - owner can be a guardian for his own private data
- Guardians allowed or required to share/disseminate private data
  - With owner's explicit consent
  - Without the consent as required by law
    - For research, by a court order, etc.

Towards new solutions to protect DRMS users' privacy
- Challenges of that approach:
  - Ensure that the data subject's metadata are never decoupled from his data
    - Metadata include owner's privacy preferences
  - "Privacy-Preserving Data Dissemination" Mechanisms:
    - Design of self-descriptive bundles
      - "bundle" = private data + metadata
    - Building of a mechanism for apoptosis of bundles
      - "apoptosis" = clean self-destruction
    - Development of a context-sensitive evaporation of bundles

Towards new solutions to protect DRMS users' privacy
INDICARE's solutions under discussion
- "Precise definition of legal information collection and management regarding DRMS-based services"
- "Granting anonymous access (e.g. by Trusted Third Parties)"
- "Privacy rights management (PRM), definition of ownership of personal data and access rights"
- "Self-commitment/self-regulation by DRMS vendors"
- "Pre-purchase information for consumers about company activities"

Another solution: a more privacy-aware and proactive consumer

- **How to avoid being profiled by DRM systems?**
  - "RTFM": read the privacy policies and don't do business with the companies with privacy policies that don't satisfy you.
  - Limit disclosure of your personal data; create several profiles and identities; use anonymous ways to pay online.
  - Do not buy digital works of authorship if you are not satisfied with them, with the choice of content; get it somewhere else: share mp3 with your friends; get mp3 from them (not through P2P).
  - Data limitation and user control: identity-management systems under the control of users with multiple and partial identities.
  - Privacy by design in DRM systems.

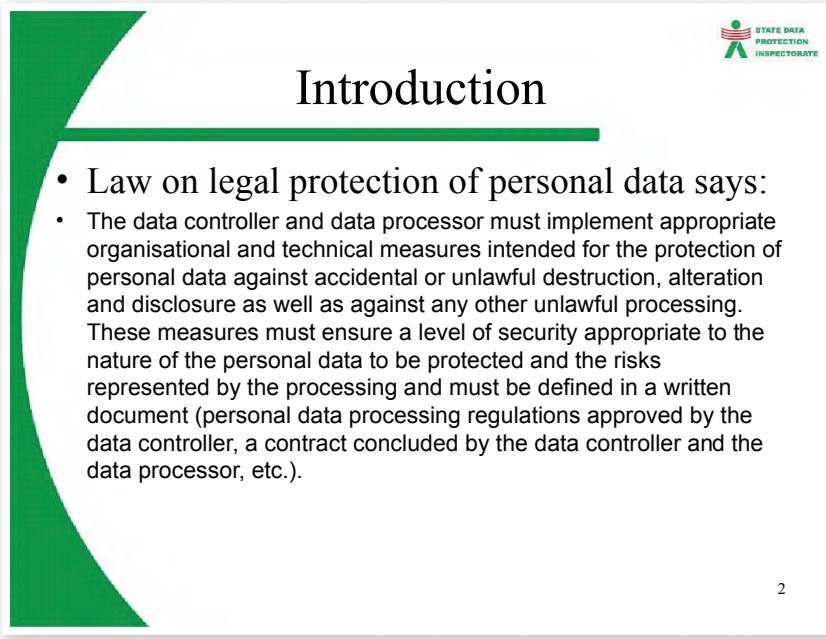
Suggestions for future work

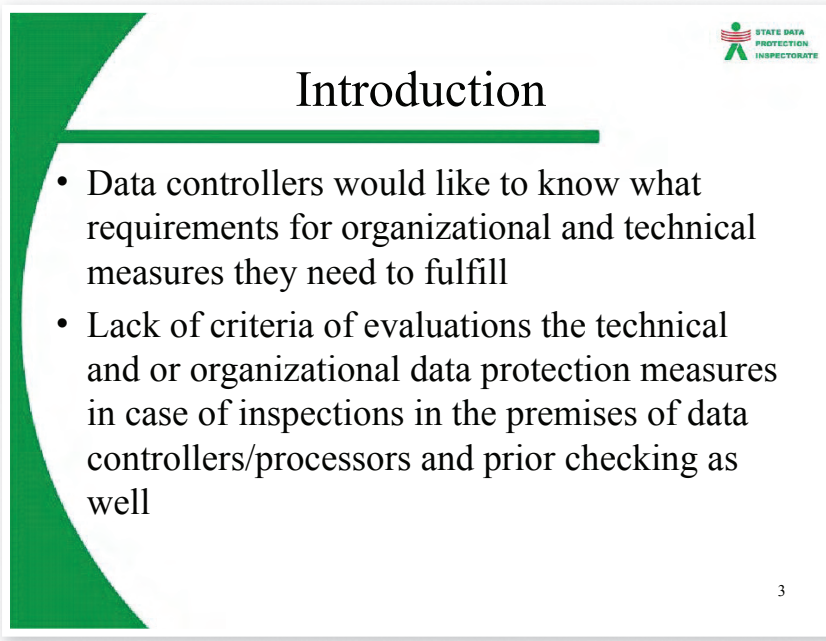
- Design a computing system that implements the "third-party" procedure explained.
- Make the system design compliant with privacy and data protection laws ("privacy by design")
- Build the system itself, then fine-tune the operational details in order for them to comply with data protection laws.

Conclusion

- More general threats to privacy: panopticism and normalized identity
- Challenges for the DRMS industry:
  - solve its inconveniences
  - harmonize diversity of platforms
  - find ways to effectively protect DRMS users' privacy
  - work with independent third parties for them to hold the DRMS users' identity and address information.

Cédric Laurant
cedric@laurant.org

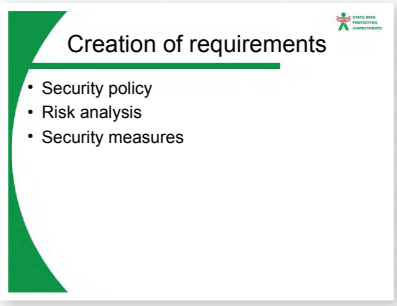




Mrs. Ausra Guciene from the Lithuanian Data Protection Authority reported on the implementation of the 2009 amendments of the Lithuanian law on legal protection of personal data. The law requires the data controller and data processor to implement organizational and technical measures to ensure a level of security appropriate to the nature of the personal data to be protected and the risks represented by the processing.

According to the 2009 amendment of the law, the State DPA is responsible for laying down the general requirements on the organisational and technical data protection measures. Based on this requirements catalogue data processors and controllers can start to self-validate their protection means. The catalogue is also the basis on which privacy protection inspections and audits are conducted by the DPA.

On the controller's or processor's side, the process will consist of three stages: First, the data controller develops and writes a security policy. Second step is a risk analysis to be performed by



the data controller, which form the base for the decisions taken in step three, where the data controller chooses which security measures shall be employed and writes documentation.

For more detailed information also see: https://www.privacyos.eu/wiki/index.php/Vienna_Slot_3B

Creation of requirements

- General security requirements created by Ministry of the Interior for government information
- Security standards:
  LST ISO/IEC 17799:2006
  LST ISO/IEC 27001:2006
- Good practice
- benchmarking

Creation of requirements

Target:
- Data controllers, public and private sectors
- Data processors, public and private sectors

Main issue:
- The data controller and data processor must implement appropriate organizational and technical measures ensuring a level of security appropriate to the nature of the personal data to be protected and the risks represented by the processing. Measures must be defined in a written document (personal data processing regulations approved by the data controller, a contract concluded by the data controller and the data processor, etc).

Creation of requirements

- 3 personal data security levels
- Criteria for security levels:
  - Sensitive/not sensitive personal data
  - Public/not public personal data
  - Accessibility through data transmission network
- Risk analysis for data the processing of which is related to high risk

8

Conditions

- If data could be assigned to few security levels than should be selected the higher of required
- Lower security level organizational and technical requirements are applicable to higher security level
- Additional security measures are recommended for very sensitive personal data with high risk

12

Security levels

- First level:
  - Public data
  - Data are processed in isolated internal data network without access through external data transmission networks

9

Security levels

- Second level:
  - Data are accessible through external data transmission networks
  - Automatic processing of sensitive personal data in a database/databases to which no access is provided through external data transmission networks

10

General requirements

First security level:

- approved written document/documents must be in place
- ensuring the management and control of access to the data
- ensuring safety of premises where personal data are stored
- ensuring protection of computer equipment against malware

13

Security levels

- Third level:
  - Automatic processing of sensitive personal data in a database/databases to which access is provided through external data transmission networks
- Data processing by other than automatic means

11

General requirements

- 9.1.1. the data controller;
- 9.1.2. the data processors (if any) and the functions performed by them;
- 9.1.3. the legal acts and standards governing the processing of personal data;
- 9.1.4. the defined legitimate purpose/purposes of processing of personal data;
- 9.1.5. the final list of personal data being processed for each defined purpose;
- 9.1.6. specific actions and/or procedures enabling the meeting of other requirements set for the data processing (i. e. how and when adjustments, corrections and updating of personal data will be carried out, how will the changed personal data be managed etc.);
- 9.1.7. time-limit/limits for the storage of personal data in an active and/or passive database and actions to be taken upon expiration of the time-limit;
- 9.1.8. procedure for the implementation of the rights of a data subject;
- 9.1.9. recipients of personal data and the procedure for the provision of personal data;
- 9.1.10. allocation of functions to persons authorised to process personal data;
- 9.1.11. procedure for the granting, revocation and modification of access rights and authorisations to process personal data;
- 9.1.12. the procedure for the briefing of persons authorised to process personal data and the training arrangements;
- 9.1.13. the procedure for the assessment of risks related to the personal data processing;
- 9.1.14. management of security violations and response actions;
- 9.1.15. the procedure for the crash recovery of data in case of data loss;
- 9.1.16. periodic review of the document/documents referred to in Sub-Clause 9.1 (updating as necessary) and control over the compliance with the provisions set forth therein;
- 9.1.17. the procedure for the making and storage of back-up copies of the data;
- 9.1.18. provisions governing other organisational technical data security measures are put in place;

14

General requirements

Second security level:

- access to personal data should be recorded and monitored
- the maximum allowable number of failed attempts to log in has been set;
- a query regarding personal data must state the purpose of the data search
- ensuring the use of safe protocols and/or passwords for access personal data via external data transmission networks

15

General requirements

Second security level:

- ensuring control of external data carriers
- ensuring that no IT testing is performed with real personal data except where real data must be used
- personal data in laptops

16

General requirements

Third security level:

- the electronic log of user log-ins to the database/databases must be reviewed at least once in a month, with review reports submitted to the data controller
- personal data in back-up copies and repositories are encrypted
- personal data transmitted via external data transmission networks are encrypted

17

General requirements

Additional measures:

- assessment of the data processing risk is made at least once a year
- an audit of the organisational and technical security measures is carried out at least once in two years
- tests of the disaster recovery of personal data are conducted
- personal data stored in active databases are encoded

18

Usage of requirements

- Inspections
- Registration in the data controllers register
- Prior checking.

19

Usage of requirements

- According to requirements there is established form for data controllers and processors for filling in case of registration in data controllers register and for prior checking
- Filled out form should be presented to Inspectorate as part of application for registration in state register of personal data controllers
- Registration of data controller or processor is performed if all requirements are fulfilled or data controller/processor promises in agreed terms to fulfill these requirements.

20

Fragment of form

3. Data access control		
3.1	Access to computer, computer network, data bases (*underline the necessary)* granted (suspended) according to procedure laid down in a written document	☐
3.2	Access to data granted only to person for whom data are necessary in discharge of his functions	☐
3.3	The user logging to computer, computer network, data bases (*underline the necessary*) is identified uniquely	☐
3.4	*The logging to computer, computer network, data bases (underline the necessary) is secured by password, other security measures (underline the necessary)* *Other measures (to be specified):* _____ _____	☐

Issues and concerns

- Data classification to security levels could be more developed
- Mandatory risk assessment should be done? Then for that purpose guidance or recommendations need to be created…
- Requirements for technical security measures have to be appended continually relating to new technologies and damages for person

22

Thank you for your attention

Aušra Gučienė, State Data Protection Inspectorate, Lithuania 23

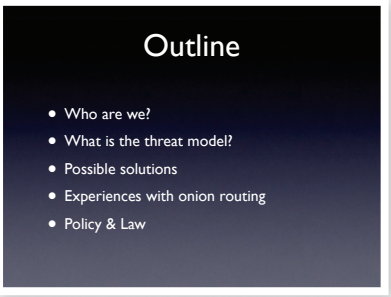
by Andreas Lehner, CCC Germany/EDRi

European Digital Rights

- Umbrella organisation for European national entities concerned with defending civil rights in the information society
- 29 members of which 11 are present at PrivacyOS today
- http://www.edri.org/

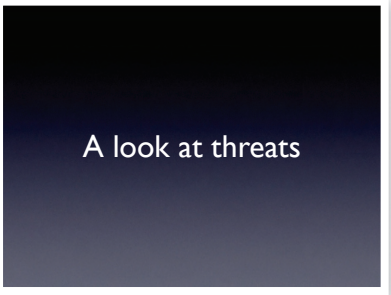
Chaos Computer Club

- One of Europe's largest and oldest hacker organisations.
- Strong technical background
- Focus towards implications of technology and the information age on society
- "Always yield to the hands-on imperative!"



Analogue vs digital telecommunications

- Eavesdropping (on content) simple
- Switch operators could track back calling party, albeit costly and complicated
- In the digital realm vastly simpler to store and analyse
- Raised desires by law enforcement & intelligence alike

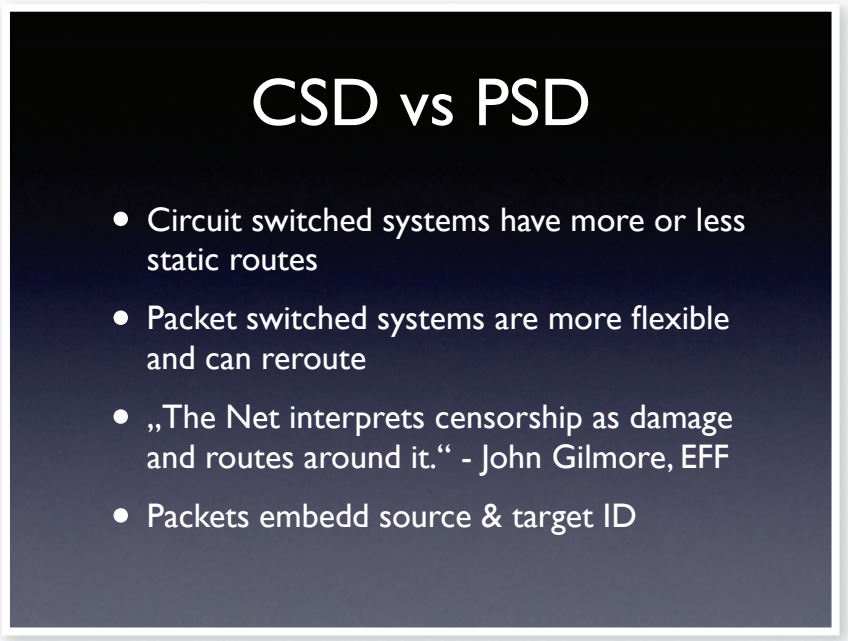


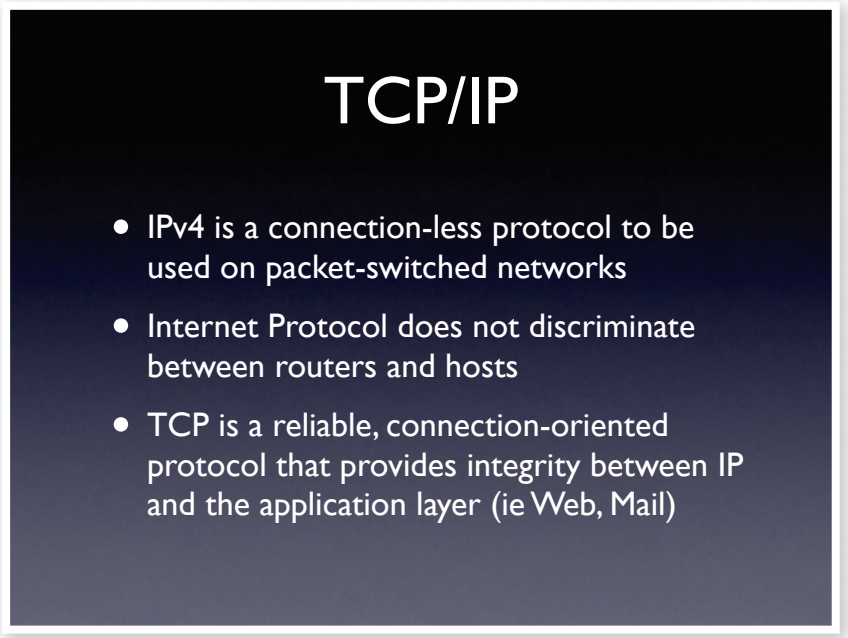
How to enable users to browse the web anonymously and without fear of prosecution was the topic of Andreas Lehner's presentation. The German activist for CCC (Chaos Computer Club Germany) and EDRi (European Digital Rights) is one of the project founders and technology experts on this matter.

His presentation included an introduction to anonymous surfing and overlay networks as well as experiences from operating TOR nodes. His introduction an overview of the threats in traditional (tele-)communication models, a differentiation between circuit and packet switched data, fundamentals of the abstraction layers (TCP/IP, HTTP, …) and, where the TOR network sets on, proxy-based communication.

The TOR network's core principle is that all HTTP communication is mediated by anonymous proxies. The proxies which are not the first or last node in the chain are fully unaware, what is requested from where by whom. As the proxies are operated by private persons and NGOs across the whole globe, the so called "jurisdiction hopping" comes into effect. The network ensures that there are nodes from different legal systems within the chain. This adds another dimension of difficulty to de-anonymization.

Currently there are two main issues on which the project team is working. The TOR-encrypted traffic is easily identifiable and the proxy lists could be blocked by law enforcement agencies or network providers, thus hampering the network's functionality in certain regions.





Proxies

- The easiest way to hide IP connection information is through a relay (eg NAT gateway, proxy)
- But this is a single point of failure and concentrates communication there, revealing information to the operator
- Susceptible to manipulation

Mixes and Proxies

- Split the power: Take two intermediaries
- Java Anon Proxy at TU Dresden, Andreas Pfitzmann
- CCC operated one half of a cascade for a number of years

Overlay networks

- Split the power: Take three intermediaries
- Protects against traffic analysis
- Create path dynamically and automatically
- Choose multiple paths simultaneously
- Trash used paths and change them frequently

Possible solutions

In the lively discussion following the presentation, the audience raised questions on performance improvements and whether intelligence agencies/ law enforcement agencies could try to subvert the network by running own nodes or whether operators of TOR nodes are exposed to risks of persecution. Other participants encouraged DPAs to take an active role in spreading the technology, for example by operating own anonymization network nodes or by researching the local legislative frameworks across the EU regarding node operations and provide local TOR node operators with documentation and legal advice.

Policy & Law

Data Retention

- This might threaten the anonymity properties
- How many different logs are there?
- How are they protected? Against whom?
- Strong need for a social movement against this, otherwise technology might not help!

Experiences with running TOR nodes

What we've learned

- All inquiries from law enforcement came from Germany
- Operators in other countries say the same
- When informed about TOR, prosecuters often stop; need to be educated further
- But: machines have been seized in Germany
- Publicity surely helps.

Questions?

Vulnerabilities

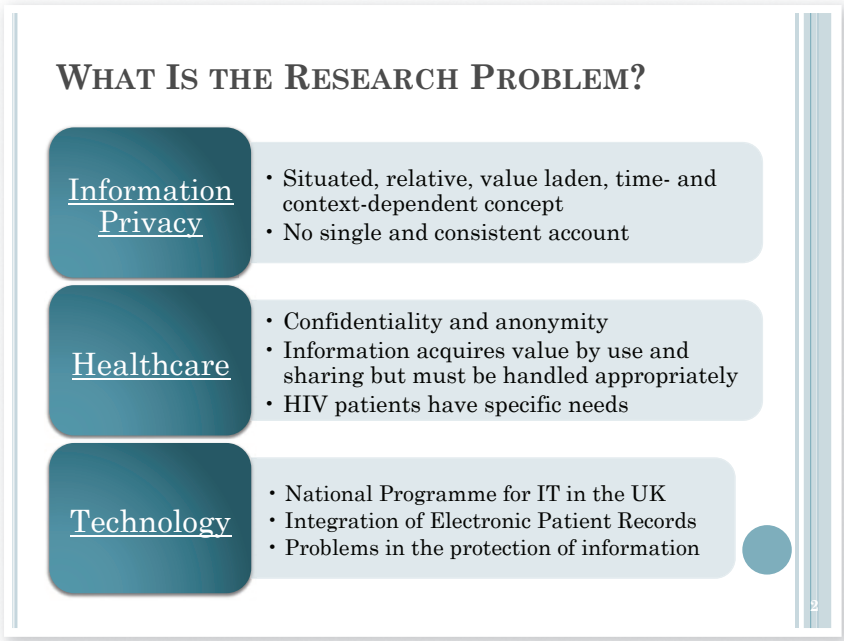
- A corrupt entry node knows that a user is talking, but not to whom
- A corrupt exit node knows that someone is being talked to, but not by whom
- Although exit nodes can eavesdrop on the traffic as it is, so application-level encryption is required

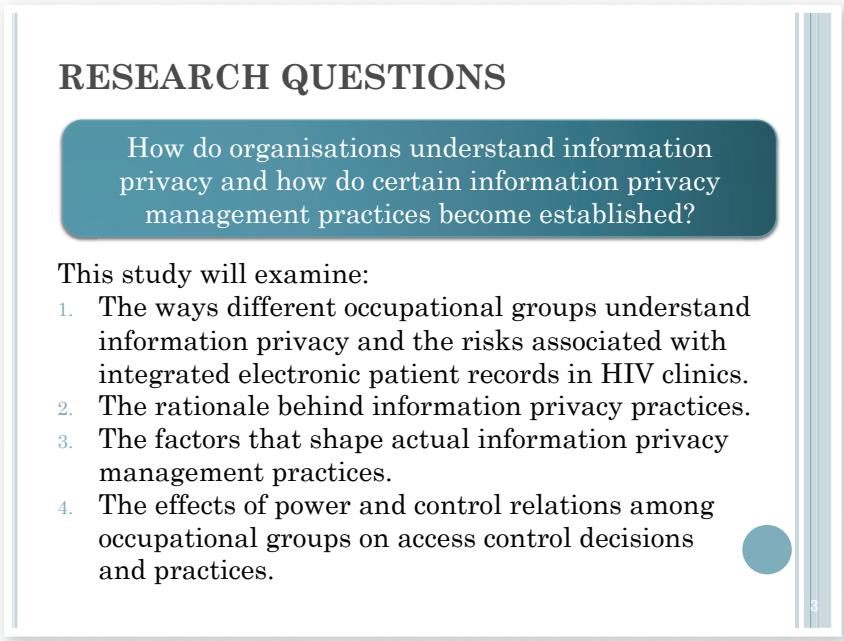
Anonymity properties

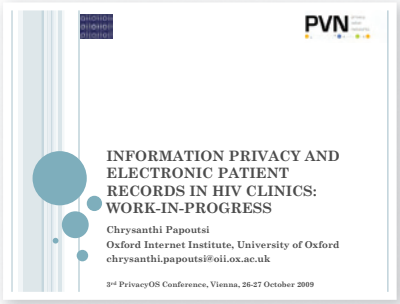
1. A local attacker cannot learn or influence your destination - useful for blocking resistance
2. No single router can link you to your destination - the attacker can not sign up relays to trace users
3. Your destination or an observer cannot learn your location - so you can't be found

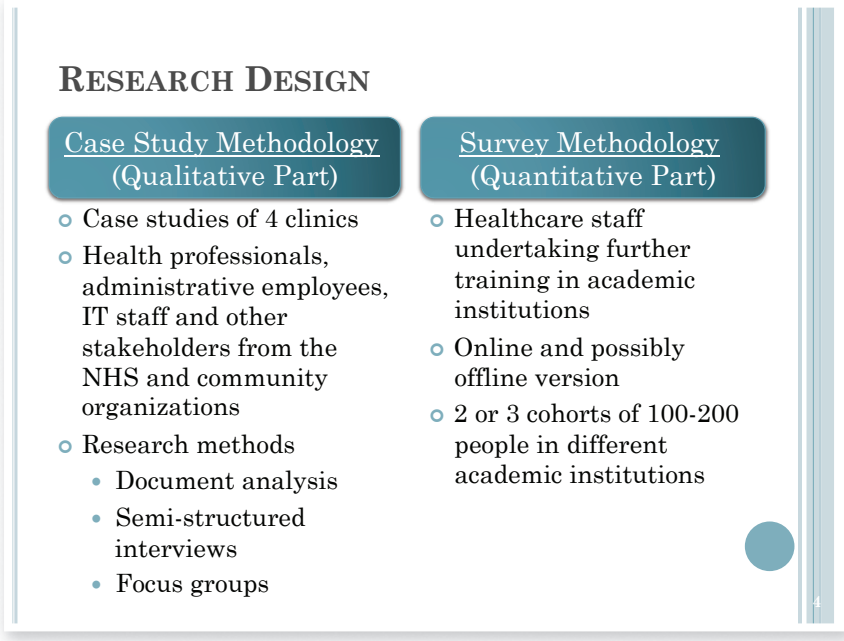
Current developments

- Bridge relays, as there is a directory of exit nodes, so they can be easily blocked
- Hiding the network footprint
- Trusting local hard- and software (eg in light of government RFS)
- UDP transport





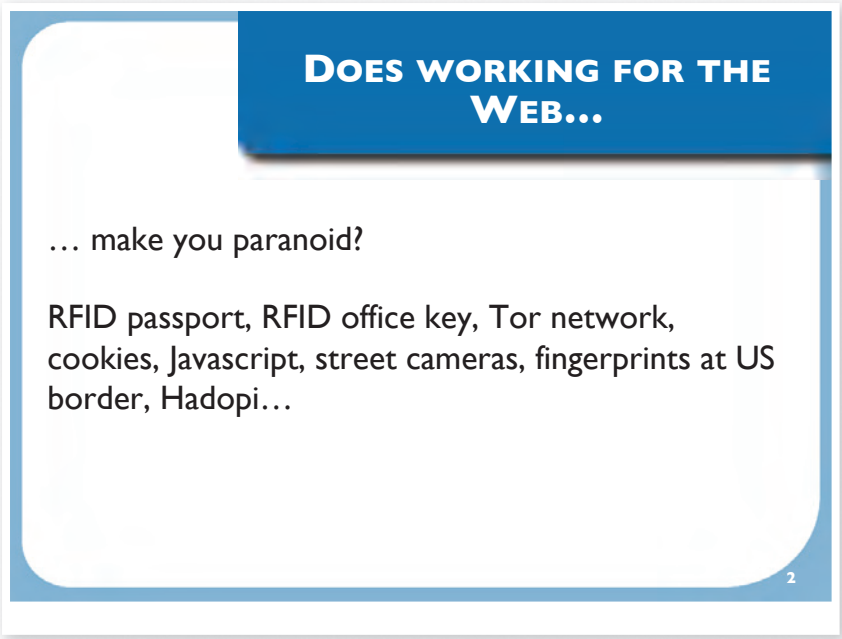


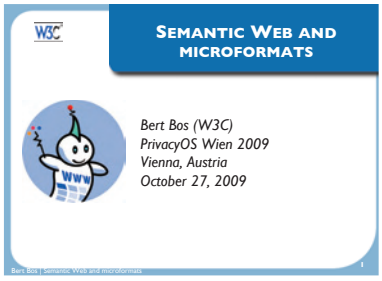


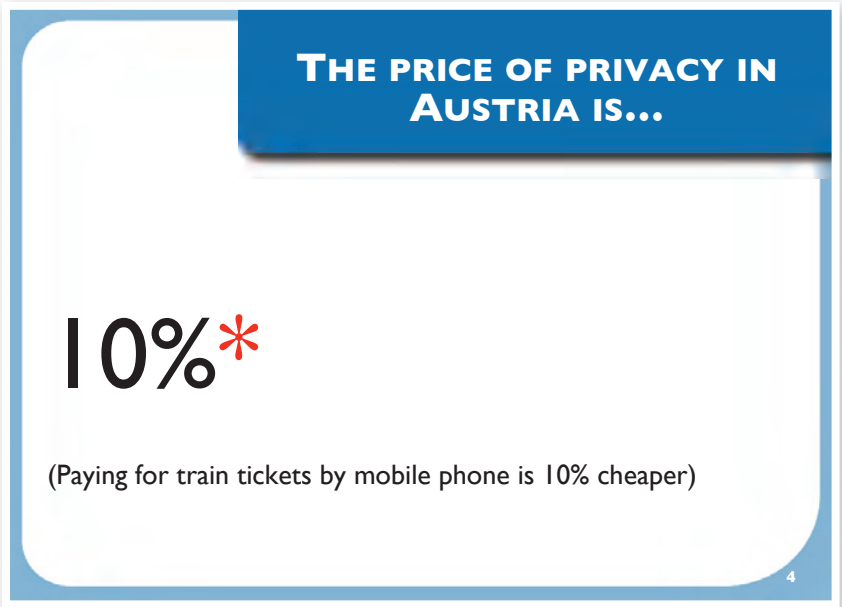
Chrysanthi Papoutsi, PhD student at the Oxford Internet Institute gave a presentation on her doctoral thesis dealing with privacy and electronic patient records in UK HIV clinics.

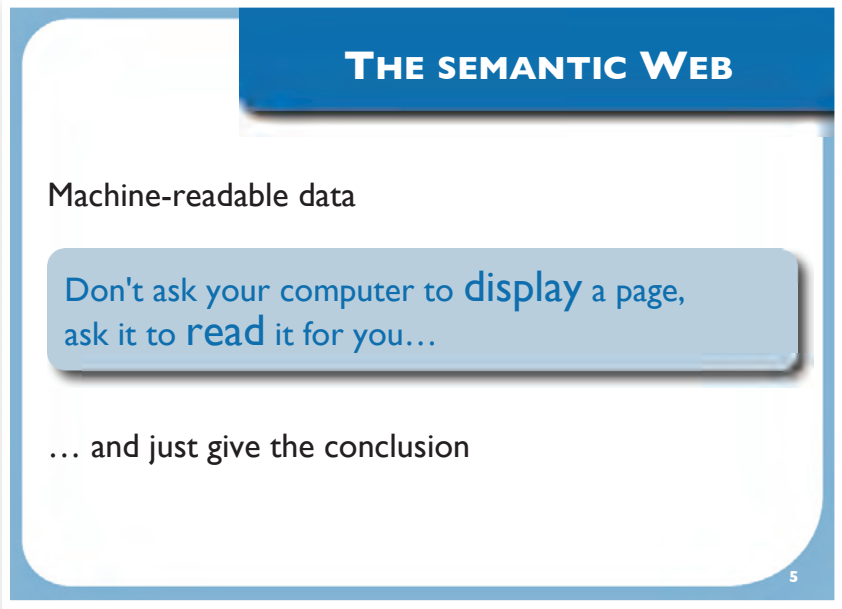
In the environment of HIV clinics, information gathering and sharing through integrated electronic patient records are critical for treatment and care. But adequate protection of this information is equally important to sustain the trust of HIV patients in the confidentiality of healthcare services. However, in the UK there is evidence of privacy problems in health information systems. There is a conflict between the ways organisations reportedly understand and value information privacy and the actual practices that seem to create privacy risks.

The speaker discussed emerging questions, the study of which can contribute to a nuanced understanding of the ways organisations understand and practice information privacy and mentioned research methodologies that can provide satisfactory answers.









For the World Wide Web Consortium (W3C), Bert Bos reported on Micro formats. After illustrating the W3C approach to the Semantic Web, the speaker went into detail on micro formats.

By adding unobtrusive semantic mark-ups to existing HTML within web sites, small pieces of information can be declared as such in a machine-understandable way. This machine-readable semantic markup enables computers to "understand" information and act accordingly or process the data automatically.

For example: Knowing that a certain piece of web site content contains address data, the computer could offer the user to use this data to do add it to his/her address book with just a single click or use it to automati-

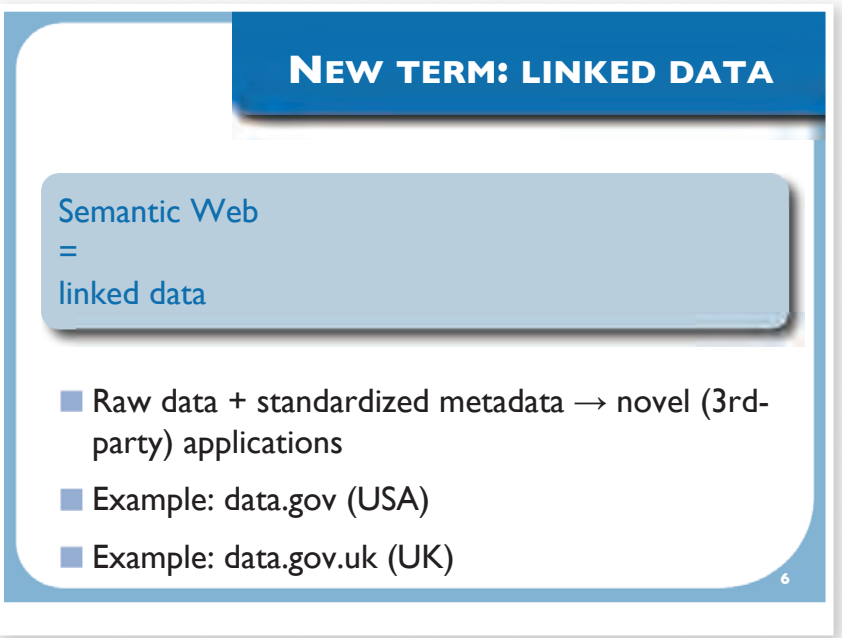
by Bert Bos, W3C

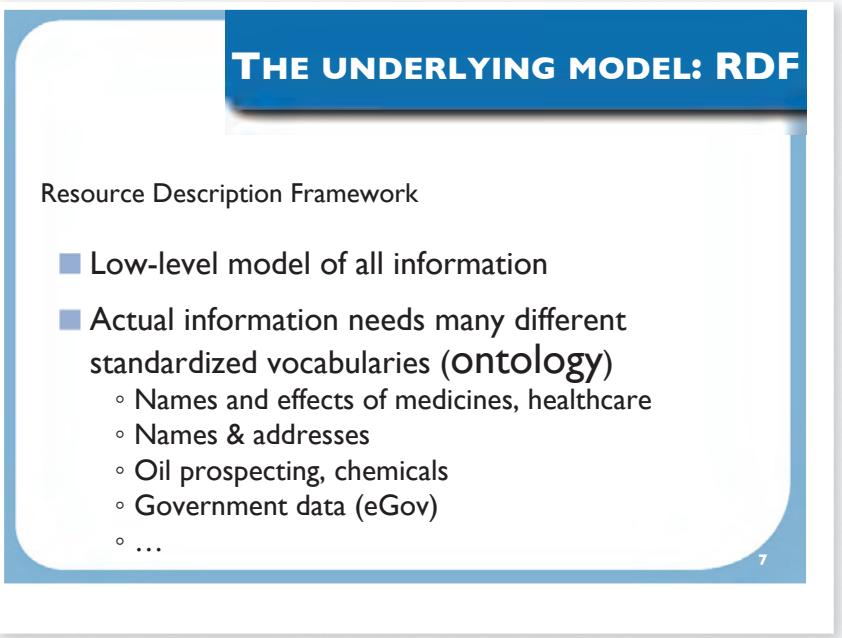
cally display directions on how to get there.

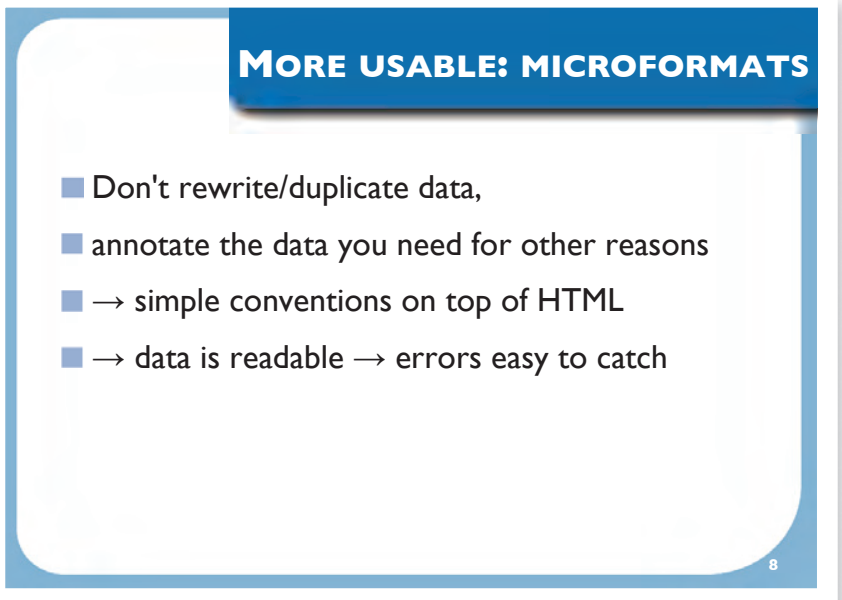
There are lots of uses for micro formats, e.g. formats for dates and events, media licences or geo information. As for the goals of Semantic Web technologies, the speaker quoted: "Don't ask your computer to display a page, ask it to read it for you and just give the conclusion".

Bos pointed out that micro formats also yield interesting uses for privacy-enhancing technologies (PETs). As an example, the "rel-licence" micro format could include machine-readable links to machine-readable privacy policies and have the client software act accordingly. For machine-readable policy languages, however, a lot of work has to be done.

For a full text of the talk see: http://www.w3.org/Talks/2009/1026-Various-Privacy-Vienna/all.htm







hCard example

```
<address>
 <img src="..." alt="">
 <a href="...">Bert Bos</a>,
 CSS contact
</address>*

<address class=vcard>
 <img class=photo src="..." alt="">
 <a class="fn url" href="...">Bert Bos</a>,
 <span class=role>CSS contact</span>
</address>
```

9

Alternative HTML-based approaches

- GRDDL* – Link to (XSLT) transformation HTML→RDF
- RDFa* – Alternative syntax for RDF as extension to XHTML (probably not HTML)

Microformats simplest & least powerful → my recommendation

10

Some popular microformats

hCard – contact data
hCalendar – calendars or individual events
XFN – personal relations (to other bloggers…)
rel-license – link to copyright info
hAtom – news feed
geo – latitude/longitude

11

GEO EXAMPLES

```
<p class=geo>The Riesenrad at
 <span class=latitude>48.216618</span>,
 <span class=longitude>16.395995</span>
...

<p class=vcard>...
 <span class=fn>Marian Kettel</span>...
 <span class=geo>...</span>...
```

13

XFN EXAMPLE

```
<a href="http://jeff.example.org"
 rel="friend met">...
```

contact acquaintance friend met co-worker colleague co-resident neighbor child parent sibling spouse kin muse crush date sweetheart me

12

TOWARDS LINKED DATA

Data using standard vocabularies → data using RDF ontologies → ability to compare data globally

But

- What about inconsistencies?
- What about permissions, licenses?

14

JUST STARTING: POLICY LANGUAGES

As there is no technical means to stop data collection…

- … need policies
- machine-readable policies
- rel-license
  - CC, ccREL
- downloadable fonts, geopriv, etc.

15

THE END

This talk: http://www.w3.org/Talks/2009/1026-Various-Privacy-Vienna/all*

16

Health registers – Czech republic

15 registers were established with the aim of registering and tracking patients with selected illnesses with serious social impacts, assessing of diagnostic and treatment methods, analysing evolvements, causes and affects of illnesses and statistical health research.

These include: National register of inpatients (NRHOSP), National register of women in childbed (NRROD), National register of newborns (NRNAR), National register of congenital defects (NRVV), National register of abortions (NRPOT), National register of physicians, dentists and pharmaceutists (RLZF), National register of users of substitutive drugs (NRUSL), National register of oncological diseases (NOR) , National register of vascular surgery (NRCCH), National cardio surgery register (NKCHR) , National Register of Joint Replacements (NRKN) , National Register of Cardiovascular Interventions (NRKI) , National register of occupational deseases (NRNP), National Register of Persons Refusing Donation of Tissues and Organs Posthumously, National register of IVF

Health registers

Processor of a data: Institute of Health Information and Statistics (ÚZIS ČR)

Data include: Birth number, nationality, health insurance number, data on health state of the patient and treatment and its results etc.

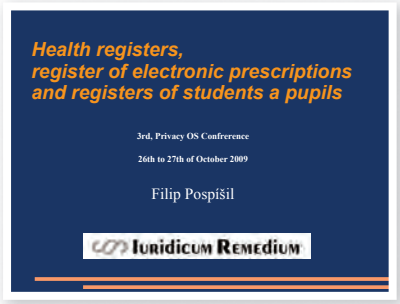
Retention period: data anonymised in 5 - 40 years
Access: processor, controller and relevant medical personell of the medical institution giving treatment to the patient relevant to the register. Relevant medical personell is a person appointed by the director or statutare representative of the medical institution and approved by the controller of the register.

Health registers

Legal basis: none specific legislation,
Ordinance of Ministry of health no. 552/2004 on transfer of the personal and other data into National health information system for the purpose of National health registers, Mandatory instructions of National Health Information Systems

Right to know and to access the data
Subjects can ask controller (Ministry of health) to clarify on extend of their personal data processed. Specific information on content of a data they can obtain only from medical facility that submitted the data to the register. Information on these rights are not publicly available to the data subjects.

Free consent of the patient with the procession of the data
Absent



The parallel session on privacy and health was opened by Filip Pospíšil from Czech watchdog NGO Iuridicum Remecum, who critically presented several projects for centralized governmental databases in Czech Republic. The NGO is focusing on legal aid against social exclusion, human rights and technology and Human Rights and Public Administration and as such also concerned with data protection and privacy issues.

A central national health database, for example, stores birth dates, nationality, insurance details, health state, treatments and therapies of patients as well as their results. The data processing is done by medical facilities only, but it is obligatory and there's no option for citizens to express or revoke their consent. Even the DPA criticizes the database for its thin legal basis (no law, just a ministerial decree) in respect to the sensitivity of the stored data and for intransparent data retention policies (storage durations between 5 and 40 years).

by Filip Pospisil, EDRi

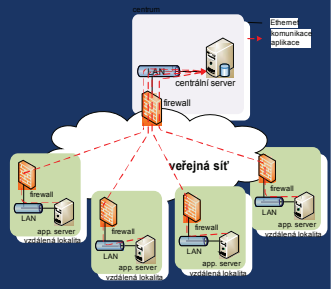
Health registers

Czech DPA Annual report 2008, p.91:
„Czech DPA considers problematics of new legal norms related to health registers to be socialy underestimated. Ministry of Health have not accepted request of the DPA to clarify whole concept of the registers.

DPA asked for clarification on data retention period in individual registers and explanation why is not (ulike in other EU countries) taken in account consent of the subject of the data. DPA have recommended that in the respect to the extremely sensitive data processed in the registers were those subject of the more detail legislation by the law and not just ministerial decree or Attachement of a legal norm.“ translation F.P.

...Nothing has changed so far

Central repository of electronic prescriptions



Established by the end of 2008
1) collection and processing of electronically prescribed medicinal products, but is being used also for
2) control of distribution and use of the medicinal products, “OTC medicinal products subject to sales restriction» - which contain some active substances which can be missused narcotic at illegal drug market and for
3) processing of information on prescription of pharmaceuticals to individuals.
By July 2009 data on medication of the 200 000 patients were submitted to the database daily.

Central repository of electronic prescriptions

In 2009 State Institute for Drug Control (SÚKL) started to request pharmacies to check in the repository whether specific patient have recieved medical products subjected to sales restrictions before, pharmacies were also requested to submit to the central repository data on distributed pharmaceuticals to individual patients.
This is being done without proper legal base just on the basis of Direction LEK 13 issued by the State Institute for Drug Control. Patients were not asked for their consent with procession of their seinsitive nor properly informed on the extend of the processing of their data.
Complains by the Czech association of pharmaceutists resulted in August 2009 decision of the Czech DPA that data are collected unlawfully by SUKL. Deletion of unlawfully collected data announced in mid October 2009.

Database of Union Information from Students´ Registers(SIMS)

Data from registers of students of individual faculties, universities are four times a year submitted to the Database of Union Information from Students´Register.
Registers started to be created from 1998 when a new law on universities was approved.
Institute of Computer Science of Maysaryk University mantains the register for Ministry of Education until today.
801 103 subjects data collected in May 2009 include: birthcode, name, surname, domicile region, state, previous education, uni/faculty, programme, study start, programme type, study length, newly admitted, dormitory, study end (date, form),study Histories, state code/citizenship, edu location, study form, study break, form of financing, parallel studies, total study length, etc.

Database of Union Information from Students´ Registers (SIMS)

Unclear system of administration of users rights, possible extention of the rights to share files on other subjects (state administration, private companies).

Subjects are not asked to give consent with the procession of their data nor they are informed of the way their data are further processed, shared and how they can modify them.

Centralised database of Informationfrom School Registers – primary, secondary and high schools (RgS)

Data from registers of pupils and students of individual schools are twice a year submitted in the electronical form to the central database of the Ministry of education.
Suspected leakages of a data from registers to a commercial subjects led DPA to start investigation.
Subjects are not asked to give their consent with the procession of their data. Detail information on the way data are processed is not publicly available.
Risks evolving from unclear system of administration of users rights, possible extention of the rights to share files on other subjects (state administration, private companies)

Conclusions

1) Rapid growth of the personal data collected in cetralised databases of the state institutions.

2) Missing clarification of the concepts of the registers.

3) Procession of the data often outsourced.

4) Ommitted principle of free consent of the data subjects with data procession.

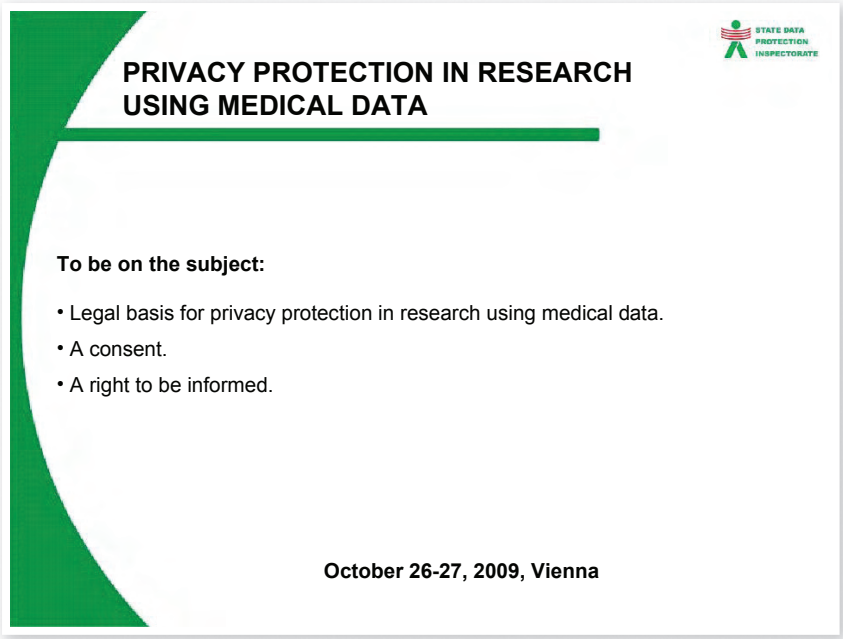
5) Often lacking legislative basis.

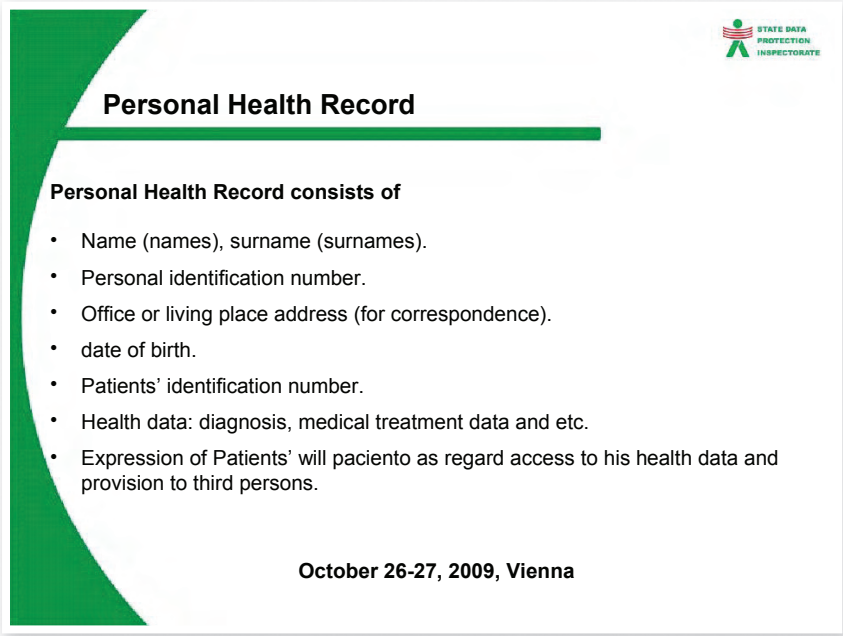
6) Reaction of the Data protection authority – post factum

7) Data protection principles ignored during assessment

Thank you for attention!

Filip Pospíšil
www.iure.org
www.slidilove.cz
iure@iure.org



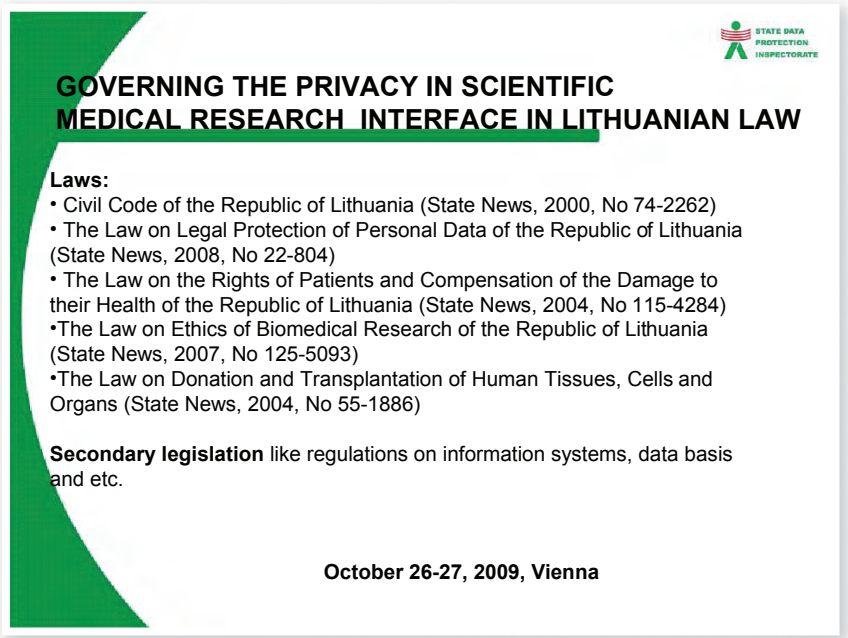


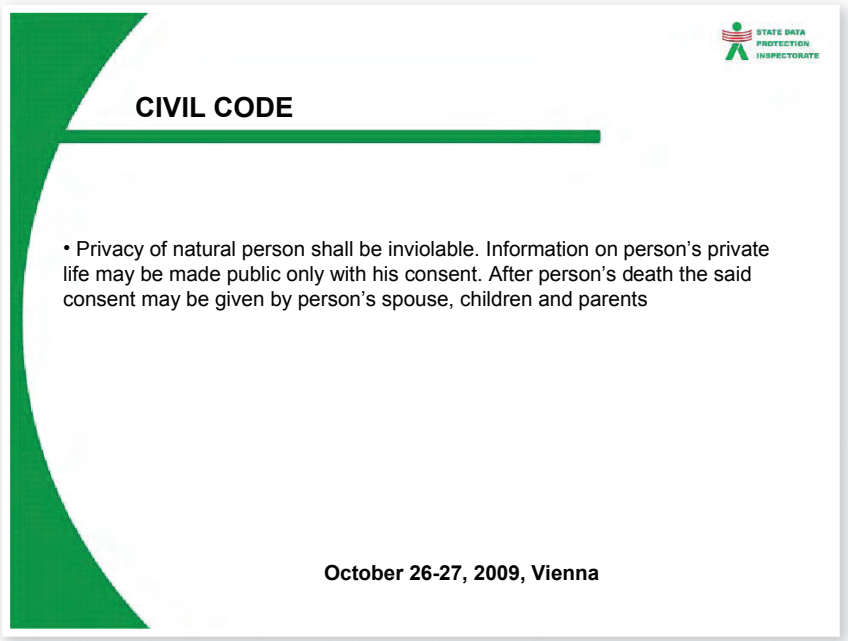
Similar critique to the one in the presentation given by Filip Pospisil was also valid for a central database on pharmaceutical prescriptions. Just recently complaints by Czech drug-maker association to the DPA resulted in deletion of the data. Until July of 2009, each day 200,000 submissions were made to the database unlawfully, as the Czech DPA stated in October 2009. Further risks and problems were demonstrated using the example of national databases of students and pupils.

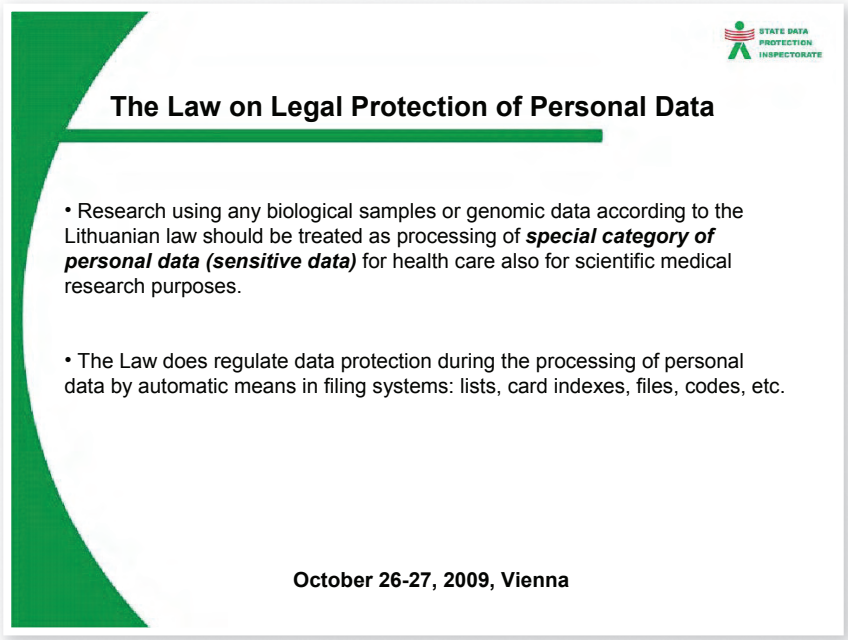
In conclusion, observing NGOs state that more and more personal data is collected by state institutions in centralized databases. At the same time they have to criticize a lack of clear (legal) concepts for these registers. In many cases, the data processing is sourced out and the principle of free consent of the data subjects is weakened. Some registers lack a legislative framework. Data protection principles are said to have been ignored during assessment and implementation of these databases. Its weak position limited the DPA to "post factum" reactions.

The Deputy Director of the Lithuanian DPA, Rita Vaitkevičienė, supplemented the Czech presentation with a view on legal issues regarding "Privacy Protection in Research Using Medical Data" in Lithuania.

There is a sound legal base for processing patient data und conducting research based on sensitive data with patient's consent. But as for biological samples or genomic data, there seem to be gaps and definitional inconsistencies within the Lithuanian legislation. The speaker proposes to treat these biological samples or genomic data should as a special category of personal data (sensitive data).







The Law on Legal Protection of Personal Data

• ***biological samples*** and ***genetic data*** – are they personal data? Are they identifiable or anonymous data?

• There is not provided definitions "identifiable" or "anonymous" data in the Law

• The Law says that personal data which have been used for scientific research purposes must be altered immediately in the manner which makes it impossible to identify the data subject

• ***"anonymous"*** data and ***"reference***" fall outside the scope of data protection law.

October 26-27, 2009, Vienna

The Law on Legal Protection of Personal Data

• Any of "**biological samples**", except anonymous forms, shall constitute personal data used for scientific medical research purposes, so all information about **human tissue samples** and all material like **biological samples** or **genetic data** should be processed according to the regulation of the Law.

• The Law does not provide any clauses regarding the data of deceased people. It is stated that the Law shall establish the rights of natural person as data subjects but it does not provide that natural person is only a living individual.

October 26-27, 2009, Vienna

The Law on Legal Protection of Personal Data

• The Law provides definition of special categories of personal data where there is stated that these data "shall mean data revealing […] his health".

• The collection, storage and use of tissue samples themselves may be subject to separate sets of rules especially if personal information is processed using information systems.

• Data controller has an obligation to alter immediately, in the manner which makes it impossible to identify the data subject, the personal data which have been used for scientific research purposes.

October 26-27, 2009, Vienna

The Law on Legal Protection of Personal Data

• The definition of “personal data” provided by he Law shows that it should be a single data subject to whom specific personal data relates.

• There is no indication that “***group data***” would ever be considered to be personal data.

October 26-27, 2009, Vienna

The Law on Legal Protection of Personal Data

A consent

• If the data controller is going to process sensitive data (health related data as biological materials of human origin taken from living or deceased person are sensitive data) a consent of the data subject should be expressed clearly, in a written or equivalent form or any other form giving an unambiguous evidence of the data subject’s free will.

• In the laws are settled specific fields were health related data might be disclosed and any consent of the data subject is not needed.

• The Law on Legal Protection of Personal Data applies to all ages. The rights of minors and legally incapable people must exercise the representatives.

October 26-27, 2009, Vienna

The Law on Legal Protection of Personal Data

A consent

• Personal data on a person’s health may be processed by automatic means, also for scientific medical research purposes the data may be processed only having notified the State Data Protection Inspectorate. In this case the State Data Protection Inspectorate must carry out prior checking.

• Research results shall be made public together with the personal data on condition that the data subject has given his consent to have his personal data made public.

October 26-27, 2009, Vienna

The Law on Ethics of Biomedical Research

Informed consent means an express written agreement given with full consciousness of the consequences by the research subject to participate in the research.

October 26-27, 2009, Vienna

The Law on Legal Protection of Personal Data

The right to be informed

Every data subject has the right:
• to know (be informed) about the processing of his personal data;
• to have an access to his personal data and to be informed of how they are processed;
• to object against the processing of his personal data.

October 26-27, 2009, Vienna

The Law on Legal Protection of Personal Data

The right to be informed

A data subject might expect only information about personal data attributes processed by data controller; for example his/her diagnosis made within the context of a biological samples and genetic data, or some other individual information originated through the course of the research. This would only be the case whilst the data held related to an identifiable individual and it would not apply to results of research, statistical data, anonymous data and etc.

October 26-27, 2009, Vienna

The Law on the Rights of Patients and Compensation of the Damage to Their Health

• Information about the state of health of the donor and recipient as well as all the other personal information including the data about the identity of such persons shall be confidential and shall be provided only in accordance with the procedure laid down in the Law.

October 26-27, 2009, Vienna

The Law on Ethics of Biomedical Research

• Information obtained in the course of a biomedical research about the subject's state of health, diagnosis, prognosis, medical treatment and other health-related personal information shall be confidential and may be provided only in accordance with the procedure laid down by the Law.

• The information obtained in the course of biomedical research about the subject's state of health, diagnosis, prognosis, medical treatment and other health-related personal information shall not be regarded as confidential and may be made public without the subject's consent if the subject's identity remains undisclosed after such information is made public.

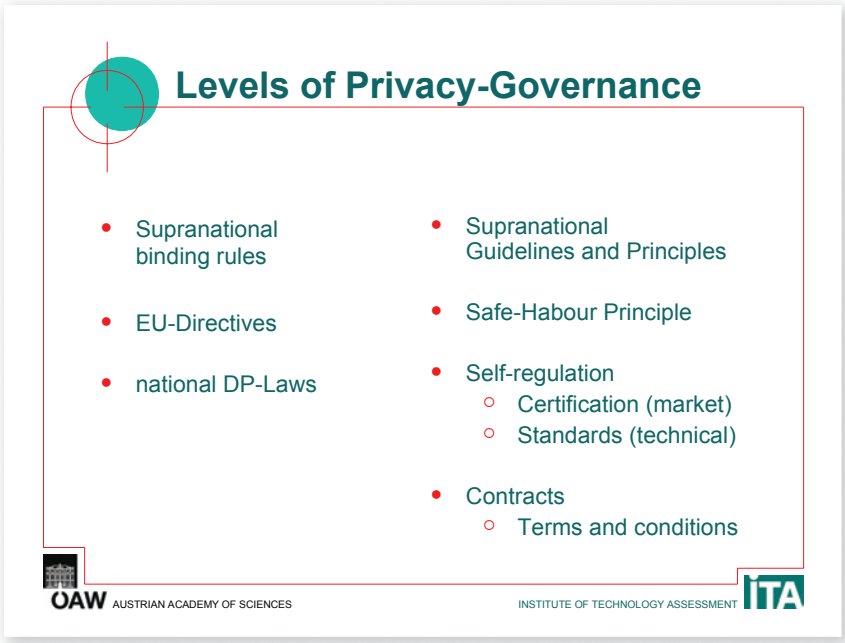
October 26-27, 2009, Vienna

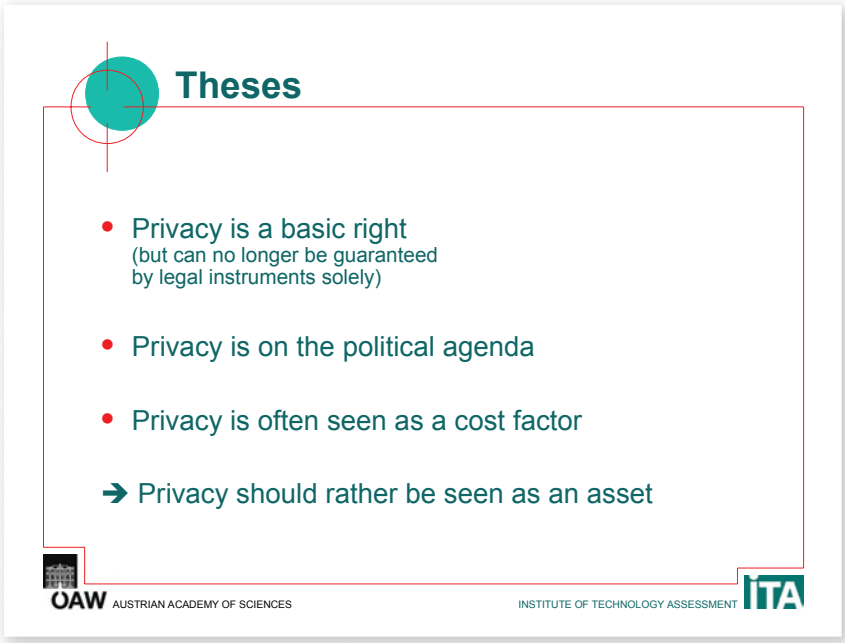
Thank you

Contact information

State Data Protection Inspectorate
of the Republic of Lithuania
A. Juozapavičiaus str. 6 / Slucko str. 2
09310 Vilnius, Lithuania
E-mail: r.vaitkeviciene@ada.lt
web: www.ada.lt

by Walter Preissl, ÖAW, Kirsten Bock, ULD, Andreas Krisch, mksult.at





Walter Preissl from the Austrian Academy of Sciences (ÖAW) reported on the current state of privacy protection in Austria and elaborated the implementation chances of privacy seals.

Kirsten Bock from ULD (Independent Center for Privacy Protection Schleswig-Holstein) gave an overview on the procedure of EuroPriSe and awarded the first Austrian EuroPriSe Seal to Kiwi Security for their product "Privacy Protector". This proxy software enhances the privacy features of CCTV and video surveillance. Faces can be scrambled and certain regions of the camera perspective can be exempted from surveillance to the live viewer (e.g. security personnel).

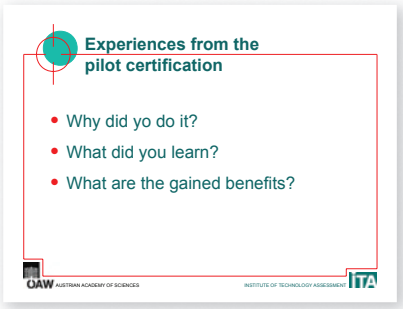
Andreas Krisch from mksult.at, who served as technical evaluator of the "Privacy Protector" on behalf of EuroPriSe, briefly reported on the technical aspects of the product and its evaluation.

The Austrian Situation

- No legal framework for privacy-certification
- Low awareness
- Expected low market

- EuroPriSe
  - 6 experts
    (2 legal, 3 technical & 1 legal & technical)
  - 1 pilot evaluation ➔ 1 Seal

ÖAW AUSTRIAN ACADEMY OF SCIENCES INSTITUTE OF TECHNOLOGY ASSESSMENT ITA



Objectives of the seal

- Promote privacy
- Build consumer trust in IT products and services
- More transparency in ICT
- Test comparative advantage of privacy friendly products and services → ROSI
- Simplifying certification for interested enterprises by issuing an European seal

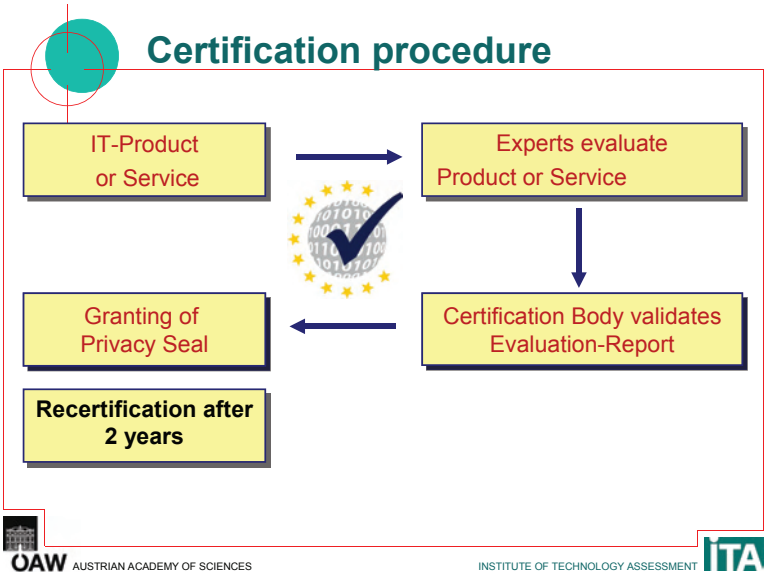
ÖAW AUSTRIAN ACADEMY OF SCIENCES INSTITUTE OF TECHNOLOGY ASSESSMENT ITA

Scope

The European Privacy Seal certifies that an IT product or IT-based service facilitates the use of that product or service in a way compliant with European regulations on privacy and data protection, taking into account the legislation in the pilot countries.
Pilot countries: Austria, Germany, UK, Slovakia, Spain, Sweden

ÖAW AUSTRIAN ACADEMY OF SCIENCES INSTITUTE OF TECHNOLOGY ASSESSMENT ITA

Certification procedure



Results and challenges

- 19 Pilot projects in 10 countries
- > 70 Experts
  9 Seals granted
  (+1 re-certification; 10 in progress)

- European criteria
- Resources for CA
- Support by DPAs
- Expectations of CA and enterprises
- Chicken and Egg-Problem

https://www.european-privacy-seal.eu/

Conclusions

- (New) instruments available
- Competitive advantage to be gained
- Special responsibility of politics and public procurement
- High potential in „sensitive“ areas
  - Security
  - e-Government
  - e-Health
  - ...

Two final theses

- Regulation is indispensable
  - and must be possible (resources)
- Additional instruments and incentives necessary
  - Privacy by Design, PRISE-Matrix, PIA etc.
  - Public procurement and funding schemes are crucial
  - Still low awareness
  - Self-regulation – the Seal – will make its way

European Privacy Seal

Privacy at its best!

Kirsten Bock
PrivacyOS, Vienna
27. October 2009

ULD

Future of Privacy

Positive incentives necessary

- Privacy Enhancing Technologies
- Good privacy practices

Ways forward

- International standards
- Regulated Self Regulation: Privacy Seals
  - Voluntary
  - Public recognition of privacy best practice in an easily identifiable way

ULD 2

EuroPriSe

- Introduced as a project in June 07 – February 09
- EC funding: 1.3 M. eTEN
- Partners a.o.: APDCM, CNIL, Ernst & Young, TÜViT, ITA
- Deployment since March 2009 by ULD
- More than 80 admitted experts from 10 countries
- More than 20 running projects
- Supported by EDPS
- Praised by French Senate Report (06/09)
- New Logo since 08/09

EuroPriSe European Privacy Seal → Euro PriSe European Privacy Seal

ULD 3

Motivation

- Trust
- Compliance
- Marketing Advantage

ULD 4

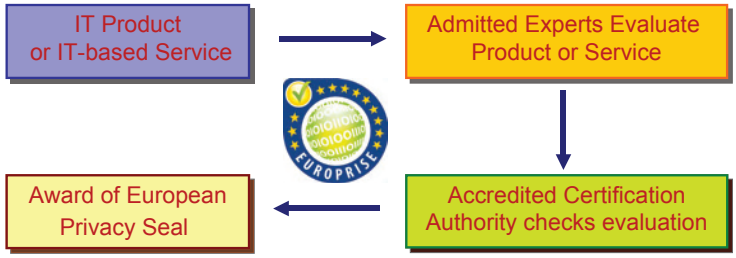
Trust

- Impartial Certification Body
- Transparency

ULD 5

Transparency

… in procedure



Validity: 2 Years

© EuroPriSe®

ULD 6

Transparency

… by public criteria

www.european-privacy-seal.eu

Compliance

… be compliant with data protection law!

The European Privacy Seal certifies that an IT product or IT-based service facilitates the use of that product or service in a way compliant with European regulations on privacy and data protection.

Marketing

9

Conclusion

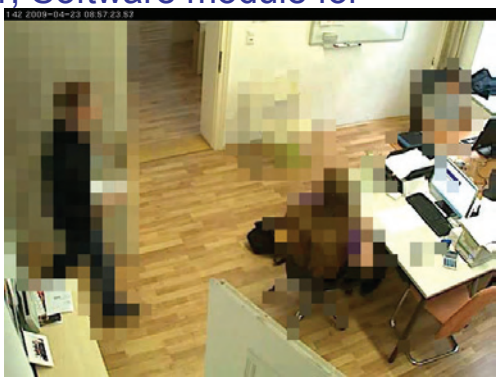
- Transparent procedures
  - Reports published at https://www.european-privacy-seal.eu/awarded-seals/
- Relevant criteria
  - European Data Protection Directives
  - Art. 29 WP Opinions, European Court Rulings
  - https://www.european-privacy-seal.eu/criteria
- Qualified Experts
  - Special training
  - EuroPriSe Commentary
- Independent Certification Body
  - DPA knowledge and approach

Four-Eye-Principle guarantees consistence & comparability

10

KiwiVision (08/09)

Privacy Protector, Software module for integration in a video management system Version 1.0



ULD 11

Criteria

- Set 1: Fundamentals
  - aspects of processing and
  - technical construction
- Set 2: Legitimacy of Data Processing
  - Legal basis for processing
  - Special r relating to various phases of processing
  - Compliance with general data protection principles
- Set 3: Technical-Organisational Measures
  - Passwords, firewalls, encryption, pseudonymisation, logs, etc.
- Set 4: Data Subjects' Rights
  - Information, withdrawal of consent, right of access etc.

ULD 12

Website Publication

KiwiVision Privacy Protector,Software module for integration in a videomanagement system Version 1.0

- **Certificate Cert. No.** DE-090017
- **Validity:** 11/08/2009 until 12/08/2011

- **Public report:** KiwiVision Privacy Protector Short Public Report (PDF)
- **Manufacturer/Provider:** KiwiSecurity Software GmbH

- **BEST:** The usage of the Privacy Protector supports the principle of proportionality and the usage of the least invasive technology with regard to video surveillance in an effective way by anonymisation of video data and data minimisation.
- **ATTENTION:** The legitimacy of the video surveillance system needs to be evaluated separately on a case by case basis by the operator of the video surveillance system. The circumstances of a certain video surveillance system need to be taken into account to ensure the success of the application. Therefore installation and configuration have to be carried out by especially trained personnel.

ULD 13

Website Publication

- **Summary**
  KiwiSecurity's Privacy Protector is a software module for integration in a video management system and provides very effective algorithms for anonymisation of video data.
- **Details**
  The purpose of the Privacy Protector is to anonymise video data (by obfuscating persons or objects in the video) from surveillance cameras and storage devices in real-time. It also provides the possibility to define fixed obfuscated or non-obfuscated regions. To ensure a smooth functioning of the Privacy Protector, the surveillance system needs to use static surveillance cameras without automatic zoom. In case of moving cameras it is to be noted, that the Privacy Protector will obfuscate the entire scene until the new background has been learned by the software.

ULD 14

Website Publication

Potential areas of operation are from highly frequented public spaces (airports, railway stations, etc.) to even working places. Depending on the area of operation and technical settings chosen for the surveillance system, access for monitoring personnel can be restricted to obfuscated video data. Access to the non-obfuscated video data can be reserved to specially authorised users (supervisors, etc.). In practice, the Privacy Protector will operate between the video signal of surveillance cameras and the picture displayed on the monitor or the storage device. Furthermore it can be used to obfuscate video data retrieved from a storage device. This results in displaying just obfuscated video data, with the monitored persons not identifiable.

ULD 15

Costs

- Depending on size of project
- Expert fees
- Certification fees
  - Based on effort or flat rate negotiable
  - Starting from 2.800 €

ULD 16

Thank you!

Contact:
Kirsten Bock
europrise@datenschutzzentrum.de
www.european-privacy-seal.eu

ULD 17

mksult.at

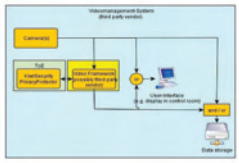
Mag. Andreas Krisch
akrisch@mksult.at

EuroPriSe
Technical Evaluation
Privacy Protector

PrivacyOS - 3rd Conference
Vienna, 27.10.2009

EuroPriSe: Privacy Protector

System Overview

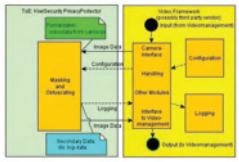


Evaluation Process

- define Target of Evaluation (ToE)
- select relevant EuroPriSe Criteria
- plan legal and technical evaluation
- perform evaluation
- integrate evaluation results
- deliver evaluation report

EuroPriSe: Privacy Protector

System Overview



Evaluation: Key aspects

- proper definition of ToE
  - what is and what is not part of ToE
  - potential changes within EuroPriSe validity period
  - primary and secondary data
- informative user manual
  - input for risk assessment
  - input for IT security
  - information on configuration and use

Evaluation: Key aspects

- technical evaluation
  - test scenarios for functional test
  - code review (undocumented functionality?)
  - proper logging
  - document the evaluated version
  - prepare for re-evaluation
    - CVS / SVN version numbers

mksult.at

Mag. Andreas Krisch
akrisch@mksult.at

Thank you for
your attention!

PrivacyOS - 3rd Conference
Vienna, 27.10.2009

Introduction

- Blocking is an incorrect term – perhaps we should start using the German word Zugangserschwerung!
- Forms of access limitation in place in Scandanavia, Italy and a few other countries
- ISPs like DNS blocking because it is cheap and useless, so it is the standard „compromise solution“
- UK uses „Cleanfeed“, a worse, better and equally useless technology

European Digital Rights

Addressing the problem?

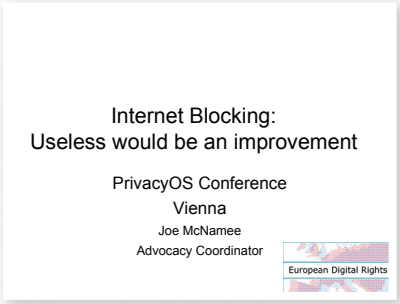
- Web blocking doesn't address
  - P2P
  - E-Mail
  - FTP
  - Shared webmail accounts
  - Private forums
  - Usenet
  - Instant Messaging
  - …

European Digital Rights

Addressing the problem? 2

- "Blocked" sites…:
  - Remain online…
  - With victims remain unidentified and unprotected…
  - With criminals unprosecuted
- "The sites in question are crime scenes almost always geographically located in major EU trading partner countries

European Digital Rights



In the parallel slot, Joe McNamee of NGO EDRi combined the very late-breaking issue of web blocking and privacy concerns. The speaker demonstrated the limitations of current web blocking efforts (e.g. its limited technological scope) and questioned the adequacy of web blocking, as only symptoms are fought. The web sites in question remain online, with possible victims remaining unidentified and unprotected and with the criminals remaining unprosecuted.

The speaker criticizes policy makers tough talk on blocking, as it seems to reduce pressure on them to take real international action. With the European Unions data retention laws in force, even accidental access tries to blocked resources by totally non-suspect personal data are logged and stored. McNamee warns that even if the technology is ineffective, the principle is becoming acceptable and opens doors for further, stronger surveillance systems. Further he questions the legality of web blocking as regards European human rights of privacy and freedom of expression.

by Joe McNamee, EDRi

What is it for?

- Is the idea to block deliberate access?
  - Blocking the web does not block the other methods of exchanging content
  - The most common web blocking systems are the easiest to circumvent
  - Blocking lists are increasingly ineffective due to permanently changing IP addresses / domain names
  - No statistical change in numbers of reports to hotlines in countries with blocking

What is it for? 2

- Is the idea to block accidental access?
  - Average of one user per thousand per year reports suspected illegal content in the most active Internet country in Europe (UK)
  - Denmark statistics show lots of comlaints of „blocked“ sites
  - The vast majority of those reports refer to legal content
  - Where is the evidence that accidental access is a major problem?

Collateral damage

- Talking tough on blocking reduces pressure to take real international action
- Blocking lists have and will become public, creating advertising for illegal sites
- Innocent sites have been and will be blocked
- “Thin end of the wedge” – blocking demanded for intellectual property, terrorism, anorexia, gambling, video games…
- Where next for Internet freedoms in a society where ISPs have control over what we see?

Privacy impact (Domino stage)

- Users redirected to ISP-hosted blocking page in several countries (great for adding bots and search engine to the „hit“ statistics!)
- Log files provide (so far unused) personal data on who access the pages
- Under data retention, totally non-suspect personal data is collected… so what's next for this data?
- Where will we be in five years, after blocking has started for gambling, terrorism, anorexia, violent games, etc?

Privacy impact (Ripple stage)

- Inverse relationship (apart from IPR) between proportionality and blocking
- Once the door is opened with child abuse,
  - Then the censorship can start
  - Then „for protection“ of citiyens the IP addresses can be stored and
  - Then the range of content can extend further and further.

Privacy impact (Nuclear stage)

- It does not work, but the principle is becoming acceptable
- Cleanfeed works better – with the added value of being the world´s most advanced web surveillance system
- The UK is already at the next stage, with „digital britain“ looking at DPI to track illegal content

A legal interference in communication?

- As regards the right of private life, the ECHR allows interference (art. 8)
  - "*in the interests of national security, public safety or the economic well-being of the country*
  - *for the prevention of disorder or crime*
  - *for the protection of health or morals*
  - *for the protection of the rights and freedoms of others*".

European Digital Rights

A legal interference in communication? 2

- As regards the right to freedom of expression, the ECHR allows interference (art. 10)
  - *"in the interests of national security, territorial integrity or public safety*
  - *for the prevention of disorder or crime*
  - *for the protection of health or morals*
  - *for the protection of the reputation or rights of others*
  - *for preventing the disclosure of information received in confidence*
  - *for maintaining the authority and impartiality of the judiciary".*

European Digital Rights

Conclusion

- Web blocking is worse than useless because
  - It doesn't work
  - It only addresses one of many communication methods
  - It does not have a clear purpose
  - It is probably illegal
  - It undermines efforts to persuade governments to take effective international measures
  - It promotes a culture where ISPs regulate what consumers see – undermining net neutrality
  - It causes the non-availability of legal content
  - It leaves illegal content online and victims unprotected
  - Blocking lists are a security threat as they have been and will inevitably continue to be leaked

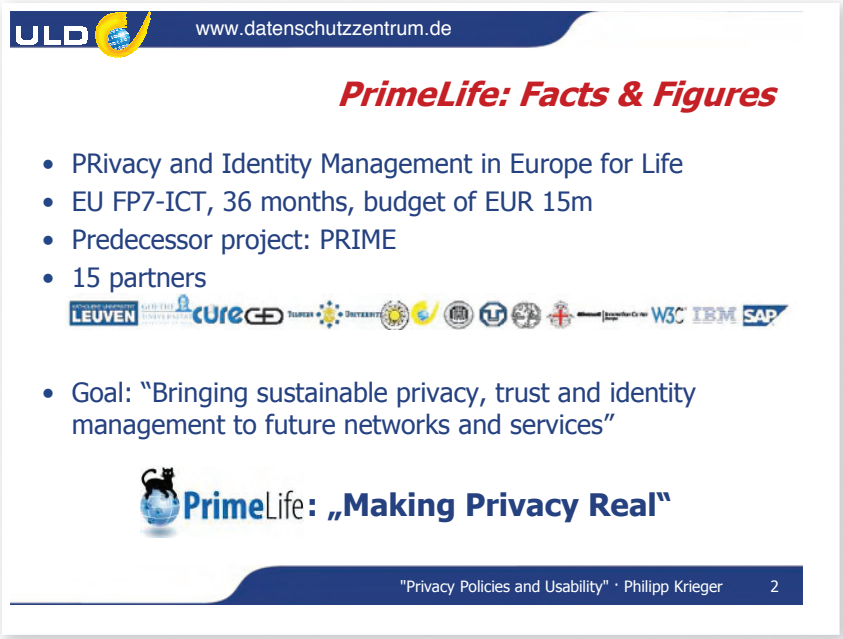
European Digital Rights

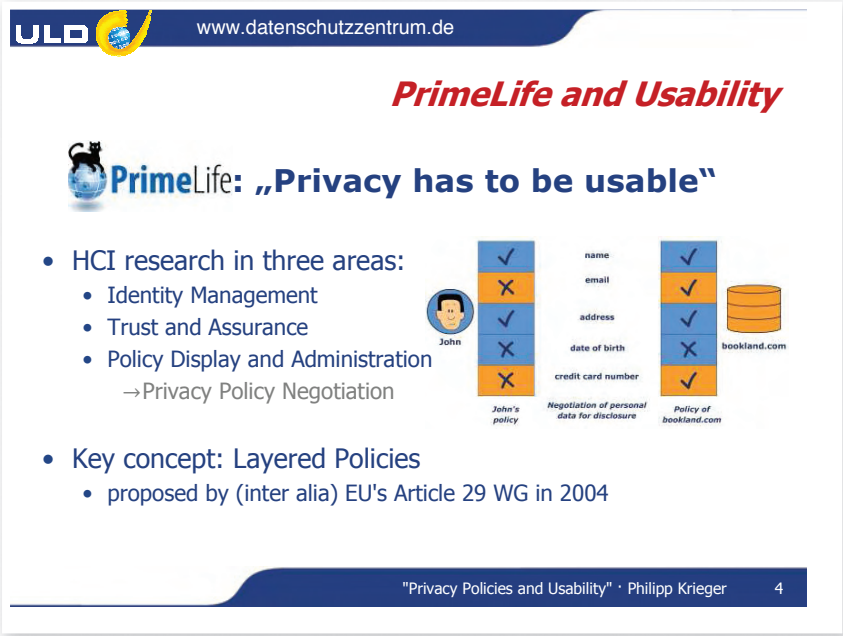
Joe McNamee
Advocacy Coordinator
European Digital Rights
www.edri.org
joe.mcnamee(at)edri.org

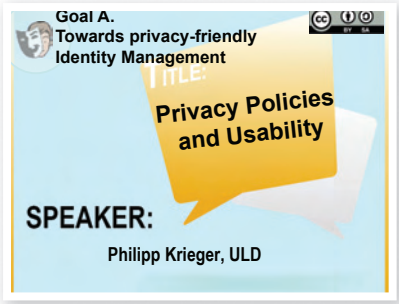
A legal interference on communication? 3

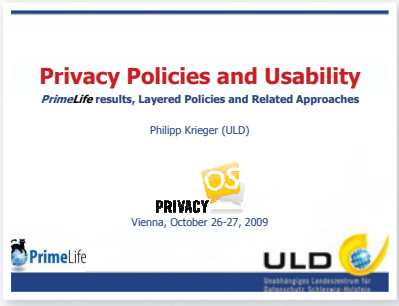
- *As regards the right to freedom of expression, the ICCPR allows interferences (art. 19)*
  - *"for respect of the rights or reputations of others"*
  - *"for the protection of national security or of public order (ordre public), or of public health or morals".*

European Digital Rights









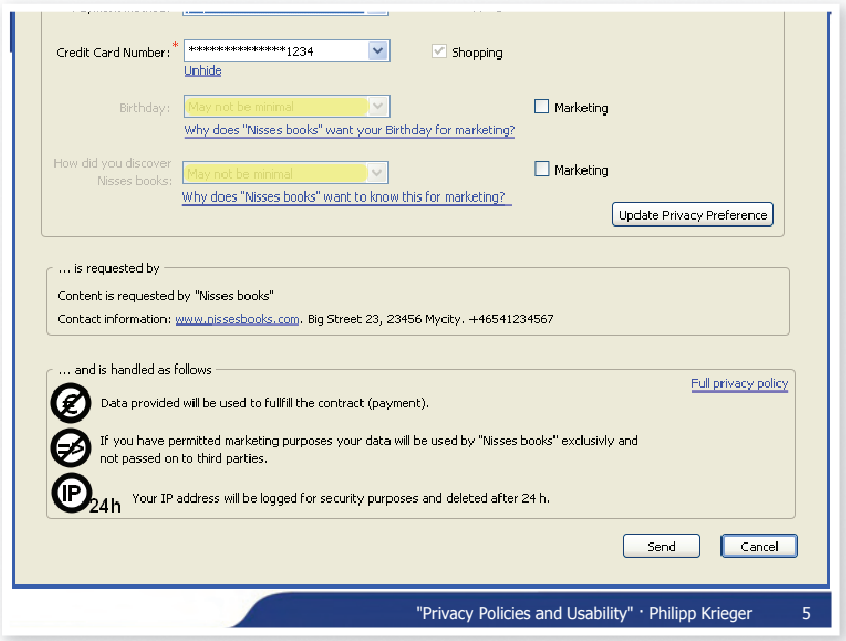
Philipp Krieger from ULD presented current research of EU-funded research project PrimeLife on the Usability of Privacy Policies in Web contexts. Demanding that "privacy has to be usable", the project is conducts Human-Computer Interaction (HCI) research in three areas: identity management, trust and assurance and policy display and administration.

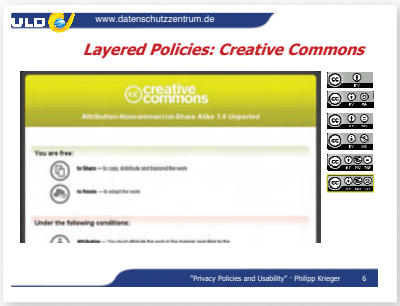
As privacy policies currently are often too long and complicated for users, a resurrection of a multi-layer approach is proposed. As other implementations, such as the Creative Commons licences show, show the possibilities of multi-layer policies. Their proposal is to add a new layer on top of the full privacy policy, a condensed privacy notice that contains an iconic summary of the privacy policy, thus creating attention and providing a quick overview.

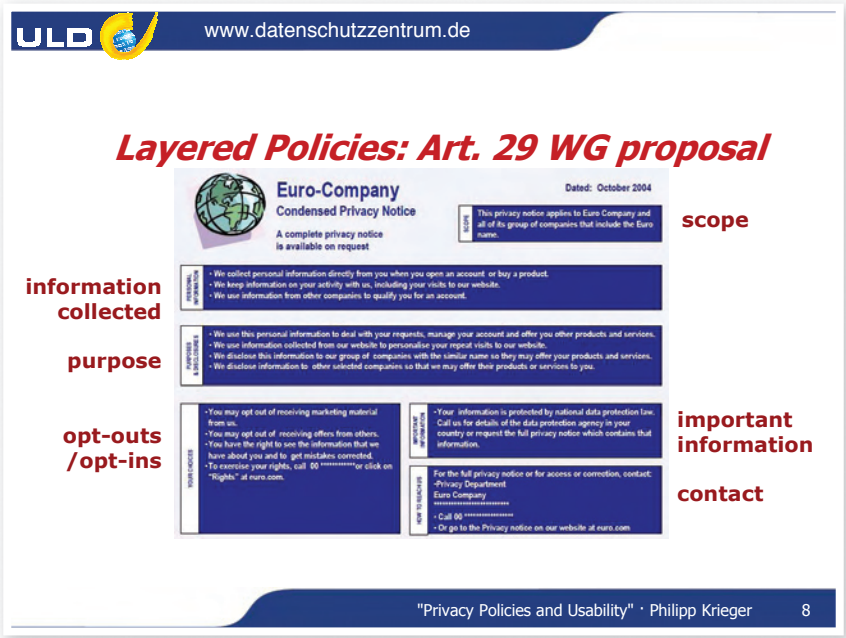
A prerequisite for icon-based privacy policies will be the standardized use of a standardized vocabulary of icons. When considering the "usability" of privacy, the speaker recommends

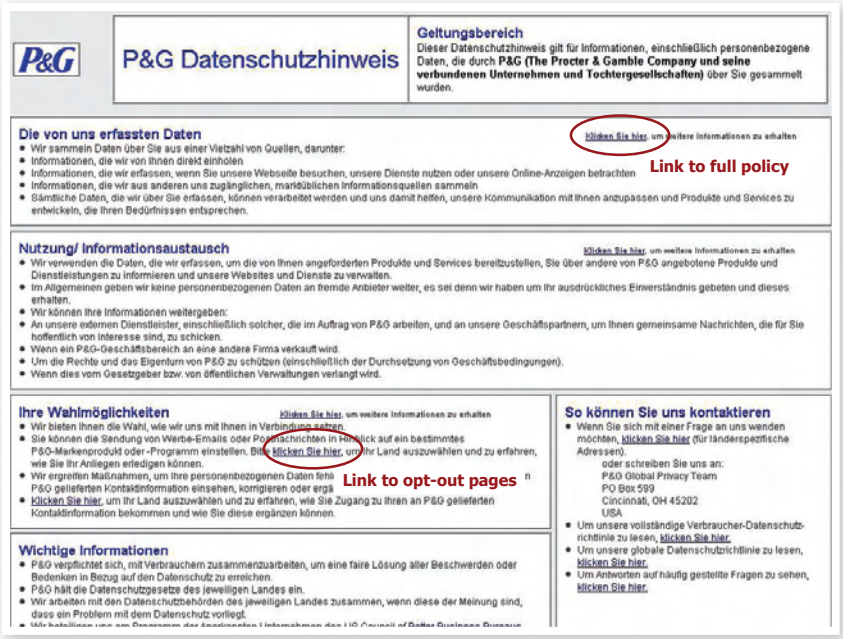
starting with privacy policies, because they resemble an "everyday scenario" to most web users and because they are crucial for Informed Consent.

After presenting several other approaches to privacy policy display, the speaker concludes several central challenges: As privacy is not the user's primary intent, his/her focus will be on the primary task. And the majority of user is unaware of privacy concerns in general. Furthermore, legal compliance poses challenges to the design of privacy-enhancing graphical user interfaces such as icons.

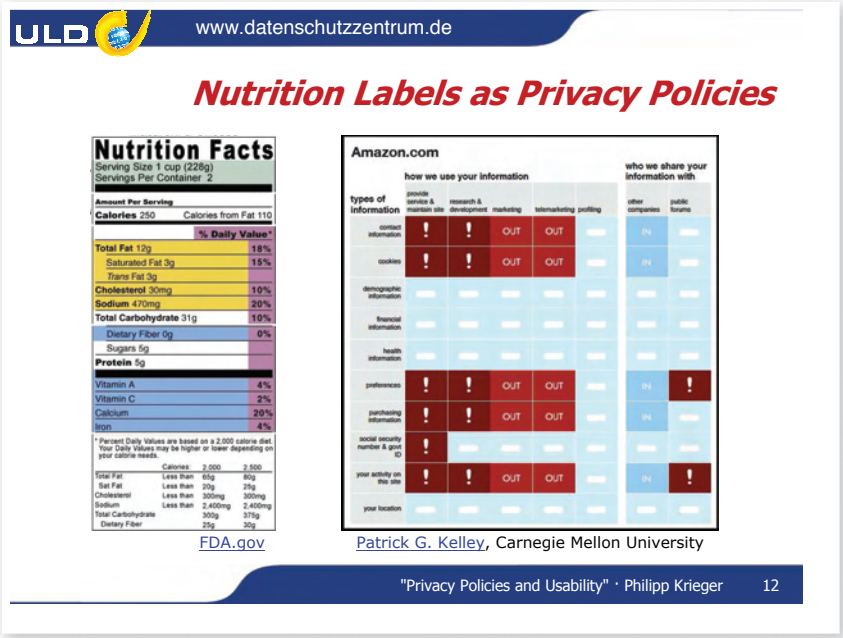


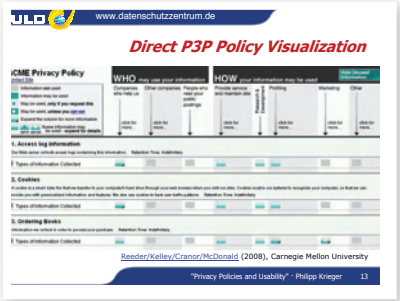


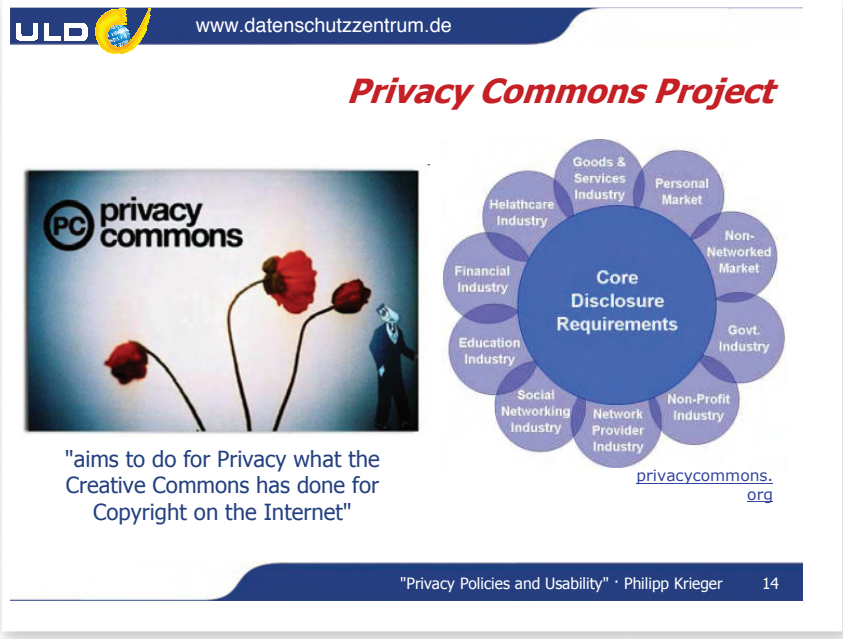



P&G Datenschutzhinweis
Geltungsbereich
Dieser Datenschutzhinweis gilt für Informationen, einschließlich personenbezogene Daten, die durch P&G (The Procter & Gamble Company und seine verbundenen Unternehmen und Tochtergesellschaften) über Sie gesammelt wurden.
Die von uns erfassten Daten
Klicken Sie hier, um weitere Informationen zu erhalten
Link to full policy
Nutzung/ Informationsaustausch
Ihre Wahlmöglichkeiten
Link to opt-out pages
So können Sie uns kontaktieren
Wichtige Informationen


Microsoft


ULD
www.datenschutzzentrum.de
Nutrition Labels as Privacy Policies
Nutrition Facts
Serving Size 1 cup (228g)
Servings Per Container 2
Amount Per Serving
Calories 250
Calories from Fat 110
% Daily Value*
Total Fat 12g 18%
Saturated Fat 3g 15%
Trans Fat 3g
Cholesterol 30mg 10%
Sodium 470mg 20%
Total Carbohydrate 31g 10%
Dietary Fiber 0g 0%
Sugars 5g
Protein 5g
Vitamin A 4%
Vitamin C 2%
Calcium 20%
Iron 4%
Amazon.com
how we use your information
who we share your information with
types of information
FDA.gov
Patrick G. Kelley, Carnegie Mellon University
"Privacy Policies and Usability" · Philipp Krieger 12


ULD
www.datenschutzzentrum.de
Direct P3P Policy Visualization
Reeder/Kelley/Cranor/McDonald (2008), Carnegie Mellon University
"Privacy Policies and Usability" · Philipp Krieger 13


ULD
www.datenschutzzentrum.de
Privacy Commons Project
privacy commons
"aims to do for Privacy what the Creative Commons has done for Copyright on the Internet"
Goods & Services Industry
Personal Market
Helathcare Industry
Non-Networked Market
Financial Industry
Core Disclosure Requirements
Govt. Industry
Education Industry
Social Networking Industry
Network Provider Industry
Non-Profit Industry
privacycommons.org
"Privacy Policies and Usability" · Philipp Krieger 14

ULD www.datenschutzzentrum.de

Privacy Policy Usability: Key Challenges

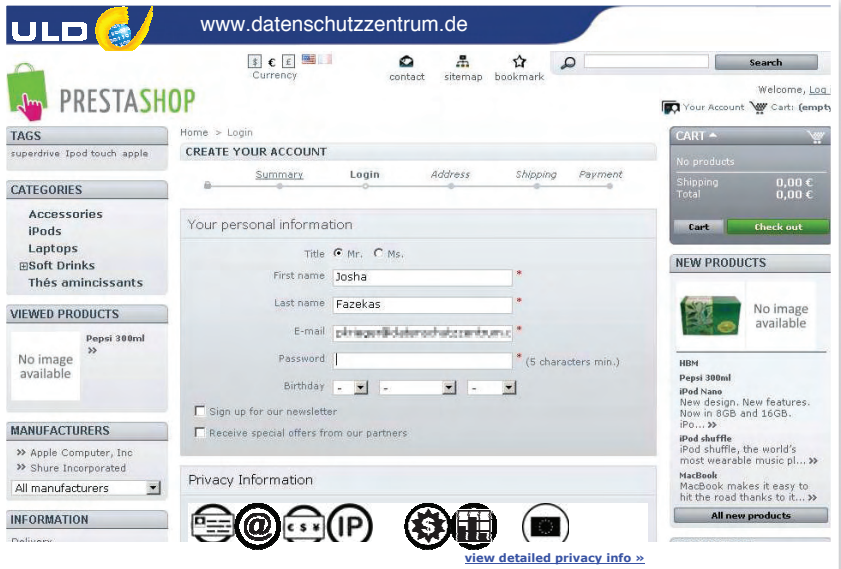
- **Why start with privacy policies?**
  - ✓ "everyday scenario" (they are already there)
  - ✓ crucial for *Informed Consent*
- **PrimeLife research identified central challenges**
  1. Privacy is not the user's primary intent!
  2. User's focus is on primary task!
  3. Majority of users is unaware of privacy concerns!
  4. GUI design requires legal compliance!

ULD www.datenschutzzentrum.de

Proposition: Icon-based Summary Layer

- Visualize core information with icons
  - data types, purposes, retention
- Icons linking to appropriate sections of privacy policy
- Advantages:
  - Closer integration into disclosure process
  - Attention catching
  - Scale effects: creating trust and rasining awareness
  - High recognition value, increased usability

ULD www.datenschutzzentrum.de

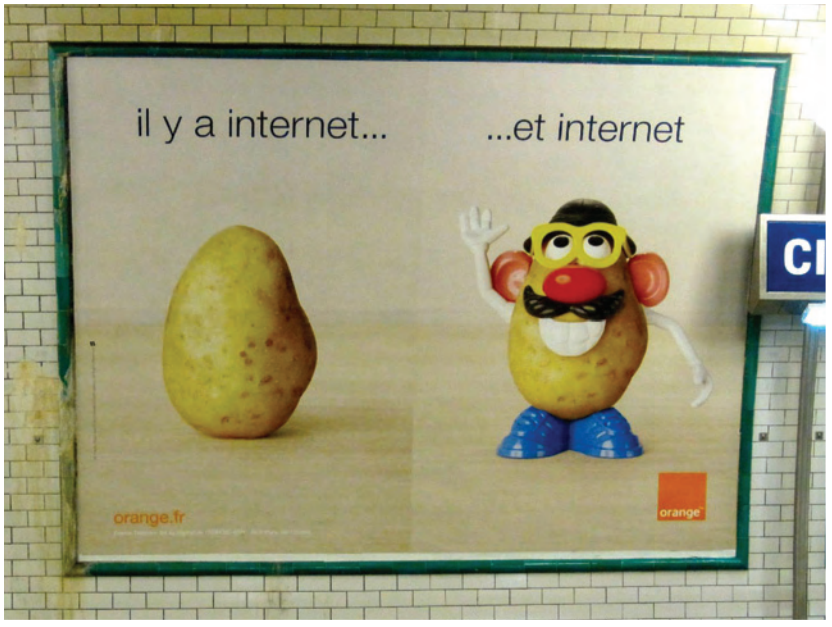


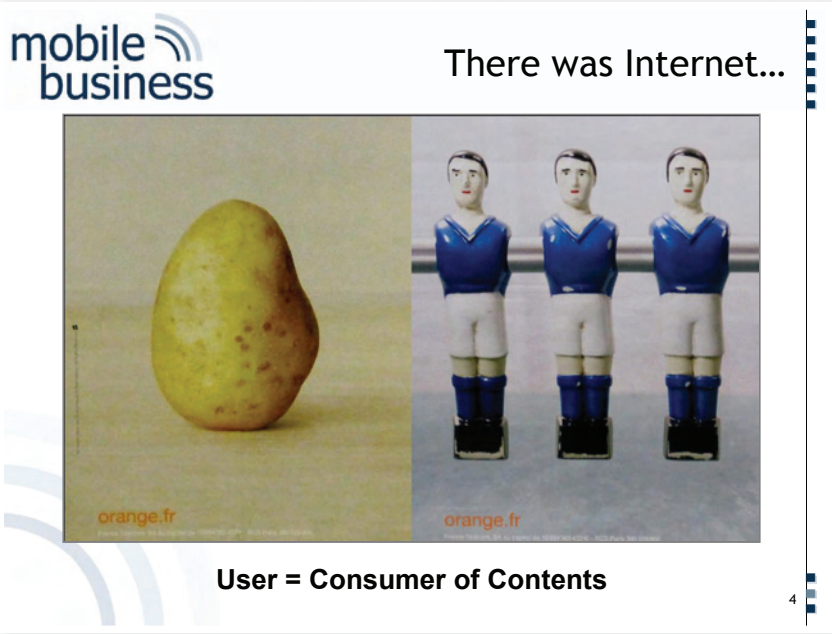
ULD www.datenschutzzentrum.de

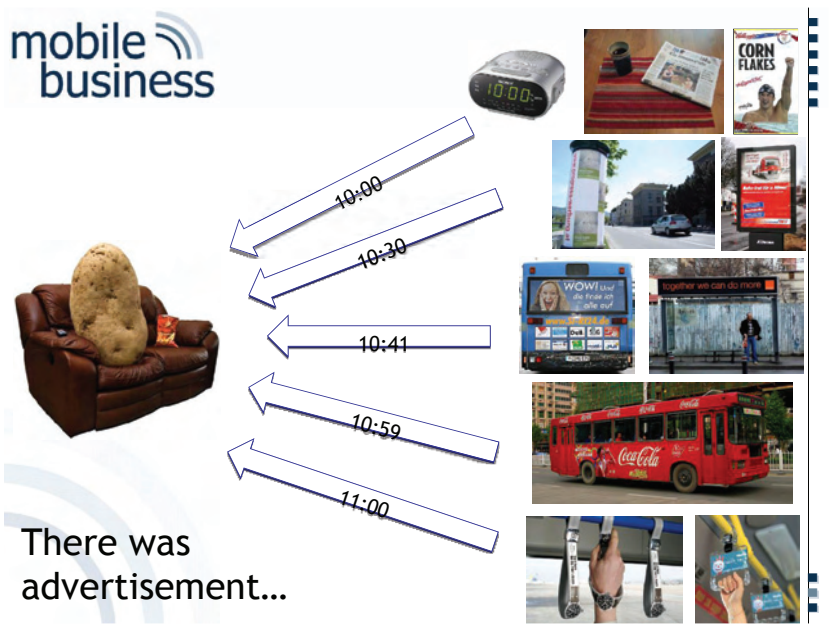
Thank you!

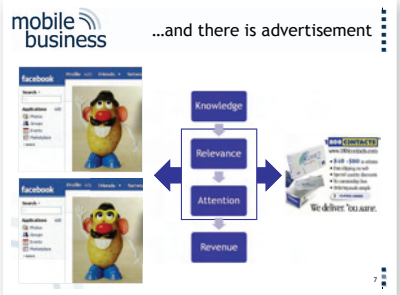
Any Questions?

contact:
phil@metaphil.de

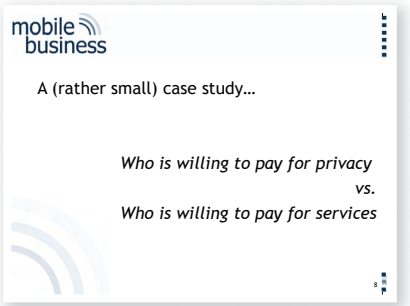






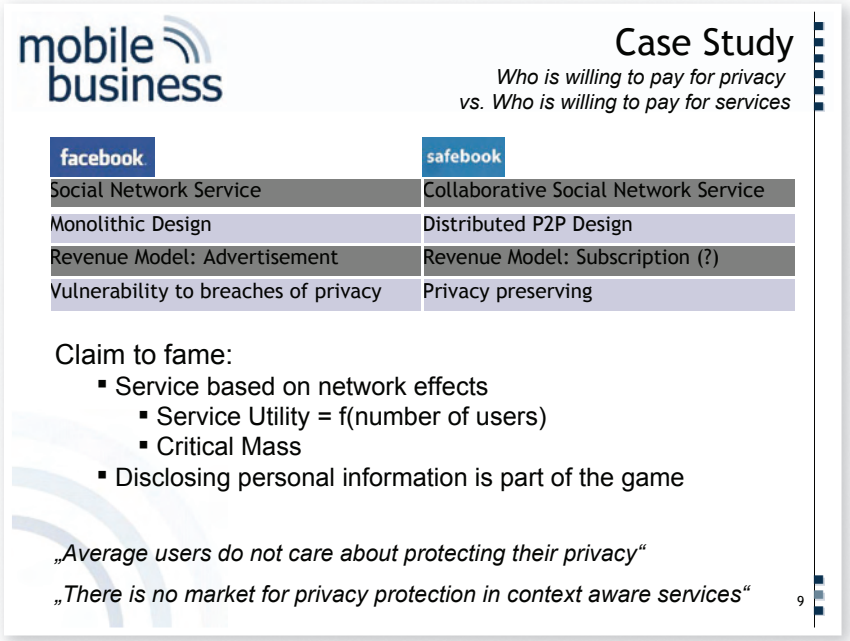


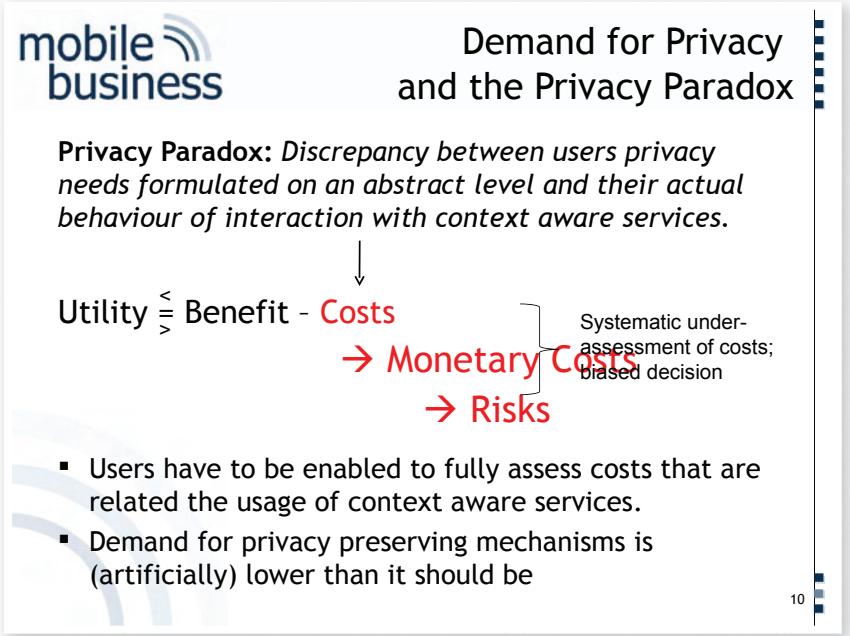
André Deuker, PhD student to the Goethe University Frankfurt/ Main is researching on the multilateral design of privacy awareness, taking into account the interests of all stakeholders.

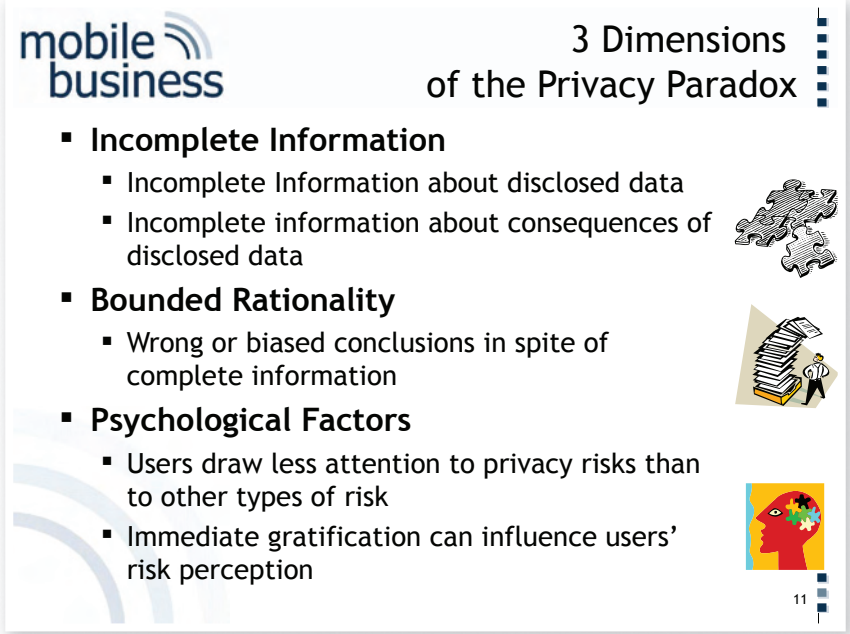


As Attention is to be regarded as a scarce resource, privacy concerns have to compete for attention with personalized advertising in common ad-based revenue models as found in the Web 2.0.

The speaker's findings are based on the assumption that raising demand for privacy is equal to raising awareness for privacy topics. Raising awareness can take place on a general level, e.g. by data protection authorities and the provision of brochures, lectures, and the education of teachers, parents, and children. But raising awareness can also take place in an application specific context just in the moment when users are interacting with an application. Providers could be motivated to implement awareness either by legal obligation or by economic incentives.







Raising Privacy Awareness to address the privacy paradox

Privacy Awareness:
Awareness of what data is disclosed and what consequences/risks this might bear.

A precondition for the employment of PETs:

- Identification of risks
- Assessment of risks

→ Users need to be motivated to address their own limits of risk perception.

13

Summary

- *Attention is a scarce resource*
- *User Information = Relevance = Attention = Revenue!*
- *Many business models require information about their users & can exist with limited privacy protection*
- *Artificially low demand for privacy due to the Privacy Paradox (PP)*

12

How to Raise Privacy Awareness?

On a general level:

- Tutorials, Talks, Campaigns

On an application level:

- Before using the service
- While using the service

→ **Informing & Warning**

Challenges for Privacy Awareness on an Application Specific Level

Technical: How can/should privacy awareness be integrated in context aware services?

Organisational: Can privacy awareness be integrated into business models?

- More parties involved than in the process of raising application independent privacy awareness.
- Interests of all involved parties have to be considered and harmonised
- Legal Obligation vs. Economic Incentive

cash flow, retention rate (switching costs), data

15

Incentives to establish application specific context awareness

Users will provide less, or incomplete information when they are concerned about their privacy.

Independent of this service, provided personal information can be misused, e.g. to create tracking profiles.

Raising privacy awareness within context aware services seems to contradict the service provider's interests.

16

Expanded Privacy Awareness

H1: To overcome the privacy paradox, raising privacy awareness on an application specific level should be closely connected with raising knowledge about methods and tools essential to satisfy needs with regard to the protection of privacy in a meaningful way.

- Awareness of problems + Awareness of possible solutions
- Users have to be provided with means to satisfy raised privacy needs, otherwise they will abstain from providing personal information

17

Resulting Incentives

H2: Raising privacy awareness in connection with providing privacy enhancing technologies on an application level can strengthen the relationship between user and provider of a services.

H3: The combined approach of raising privacy awareness and providing means to react will result in a higher disclosure of personal data and retention rate.

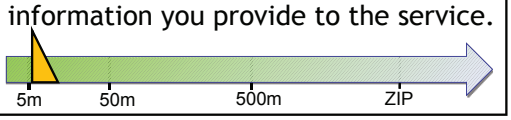
18

mobile business

Awareness of problems + Awareness of possible solutions

Independent of this service, provided personal information can be misused, e.g. to create tracking profiles.

Please adjust the precision of location information you provide to the service.



Users have to be provided with means to satisfy raised privacy needs, otherwise they will abstain from providing personal information.

mobile business

Potential Effects

- Changing attitudes towards competitive, less privacy sensitive, services.
- Higher Retention Rate
- Disclosure of additional information

mobile business

Summary

- *Attention is a scarce resource*
- *User Information = Relevance = Attention = Revenue!*
- *Many business models require information about their users & can exist with limited privacy protection*
- *Artificially low demand for privacy due to the Privacy Paradox (PP)*
- *Privacy Awareness in Business Model Architectures*
  - *Legal obligation vs. Economic incentives*
- *Conflict of Interest → Design of Privacy Awareness*
  - *Expanding the Concept of Privacy Awareness*

mobile business

Thank you for your attention!

andre.deuker@m-chair.net

The Militarization of Cyberspace, [Version 1.0]

There is a new asymmetric threat rising from the darker spheres of the internet. Large, global networks of hijacked computers run by criminals can suddenly transmute into mercenary armies and attack the infrastructure of a country.The role of botnet warlords and their zombie armies in current military strategies and the implications on privacy.

Erich Moechel Vienna PrivacyOS 2009 10 27

Evolution of the Botnets: 1999 - 2002

- After Melissa, ILOVEYOU etc. worms started transporting more and more trojans from 1999.
- CNN, Yahoo et al. downed by DDoS attack 2000
- Trojans and worms start dominating hitlists
- Phishing attacks on eBay, Paypal & Co 2001
- Sporadic DDoS-Attacks: Japan, Falun Gong et al. US accusing China on DoD network attacks
- 2002 “Identity Theft” on the rise in the US
- DDoS-Blackmail against gambling websites

Evolution of the Botnets: 2002 - 2005

- Black market: Botnet herders, spammers, phishers, fraudsters etc.
- Around 2003 first large phishing waves hit European banking systems
- More worms: Slammer, Mydoom, Netsky, Sober sporting new features
- Global zombie PC count 2005: one million. Phishing reaching a climax

Erich Moechel from Austrian NGO quintessenz e.V. describes a new asymmetric threat rising from bot networks consisting hundreds of thousands of remote-controlled personal computers on the World Wide Web. Those attacks, targeting private companies, governments as well as individuals by blackmailing or phishing and are very common and their impact continues to increase with several recent examples of botnet attacks under regime of cyber criminals.

The speaker describes how new threat constellations like botnets invalidate a strategic axiom which is valid since antiquity. The axiom indicates that infrastructure and topography always benefit the defending side. This is no longer the case with Denial of Service (DoS) cyber attacks, as they become more powerful, the better the victim’s infrastructure (e.g. internet connection) is. Massive cyber attacks are hard to detect early, harder to assess and near to impossible to counter. As phishing causes more and more incidents of identity theft, botnet cybercrime is closely related to privacy.

by Erich Moechel, quintessenz e.V.

Evolution of the Botnets 2005 -2007

- 60 percent of new malware trojan type
- Targeted attacks using zero day exploits at Tibetan and Falun Gong dissenters
- Fully fledged malware suites hit the market
- Rise of the super botnets: RBN, Srizbi, Rustock, Storm.
- Estonia cut off by a massive DDoS-Attack

Evolution of the Botnets 2007 -2009

- Browser plug-ins become a primary source of infections
- Rent-a-botnet for DDoS on medium targets for less then 5K USD
- Malware distribution shifting from e-mail to multiple channels. “Drive by“ infections.
- Differentiation in botnet types

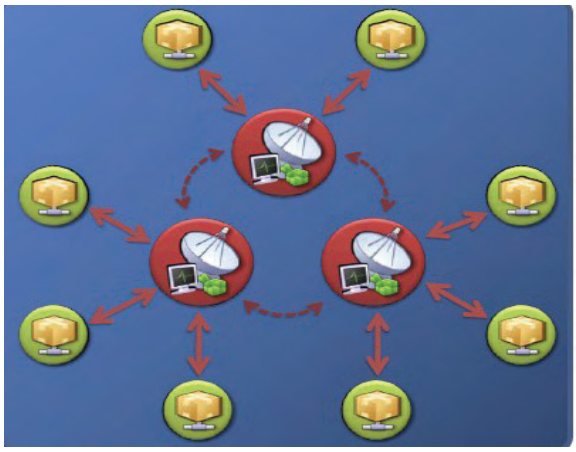
DDos attack at US targets

[image creator unknown]

„Independence Day“: The DDoS Attacks on South Korea, July 2009

- Three major waves around July 4 2009
- Banking sector hit, Online banking halted for days
- Sophisticated „fast flux“ programming
- Fire and forget: Fully automated, rotating command/control
- No supersize but „upper middleclass“ botnet. Estimated 50. – 150.000 PCs

Type of botnet most likely used in South Korea [graph courtesy damballa.com]



The lessons of „Independence Day“

- The better the defender's IT infrastructure the more firepower has an attacking DDoS force.
- This topples a strategic axiom valid since antiquity: Infrastructure and topography always counted on the defending side.
- Much more impact with improved timing of attacks and/or use of a supersize botnet
- Attack first mistaken as a „symbolic“ event, very late initial reaction by the Korean government

Recent numbers form the darker spheres of the internet

- 14 million newly infected PCs in Q2 2009, or 150K per day.
- Rustock and Cutwail botnets currently sporting up to two million zombie PCs each
- Spam capacity 1-3 billion e-mails per hour
- Price drop in botnet rentals below 1K USD for mid scale DDoS attacks.

The botnet dilemma from a military perspective

- Massive cyber attacks hard to detect early, harder to assess, impossible to counter
- Mindless mercenaries attack from around the globe and inside a beleaguered country
- No visible enemy to engage – no retaliation
- A dozen specialists, half a year and 200K USD cash are enough to constitute a zombie PC army big enough to take down the USA

Contact, coordinates

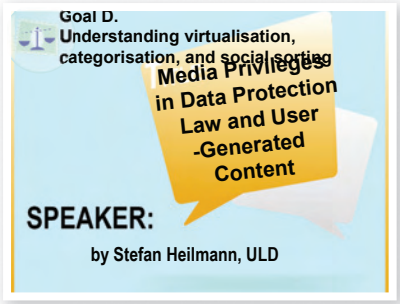
For more information and contact data:
http://moechel.com
email:
firstname@lastname.com

key id: **0x007DB429**
fingerprint
9F49 57E7 8824 26C8 78B5 F3B6 F416 7AFB 007D B429

(Classic) Media Law

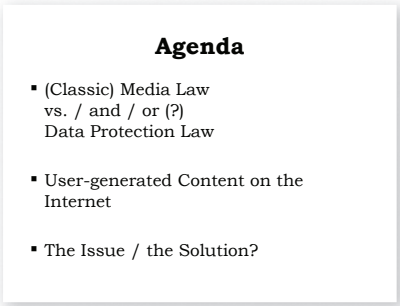
- Protects individuals against …
  - defamation
  - misrepresentation
  - breach of privacy
  - a couple of more types of infringements

  by (media) publications.



(Classic) Media Law

- General rules:
  - More or less freely balancing freedom of speech/press/other media and rights of individuals along more or less "traditional" lines/tests/criteria
  - Important test: *matter of public interest* cf. ECHR case *Von Hannover*

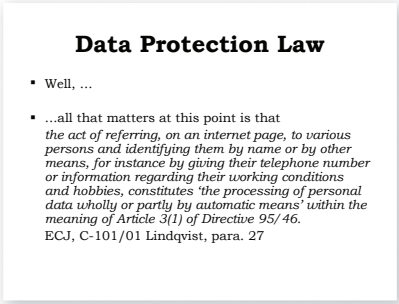


(Classic) Media Law

- Provides for a distinct set of remedies
  - injunctive relief
  - right to reply / for rectification
  - (punitive) damages
  - a couple more
- Enforcement
  - Individually by courts
  - Self-regulation of the press
  - Some co-regulatory efforts

The parallel slot was held by PhD student Stefan Heilmann from ULD. He presented a legal perspective on the relation between "Media Privileges in Data Protection Law and User-Generated Content".

By analyzing two cases, the speaker demonstrated conflicting constellations between DP legislation and (classlc) Media Law. The first case was heard at the European Court of Justice (the Lindqvist Case, C-101/01) and, in laymens terms, deals with an overlap of allowed publication of personal data and coincidental publication of sensitive data. The second case made it to the German Federal Court and discusses the liability of service providers for content generated by their users. The platform spickmich.de allowed pupils to evaluate their teachers.



Together with the audience the speaker discussed the theory that "everybody is a data" controller and the question where "journalistic purposes" (a term used in the reasons for the judgement) begin. To avoid the exaggeration of "everybody is a journalist", the speaker proposes to differentiate between (mass) media activity and individual exercise of freedom of speech.

Data Protection Law

- So, DPL is applicable. So what?
  - Strict rules for processing of special category data (Art. 8 DPD)
  - Information obligations (Art. 11 DPD)
  - Strict rules for transferring data to third countries (Chapter IV)*
  - The data controller is subject to supervision by data protection authorities
  - Etc.

** which is what is happening when you publish data online*

Data Protection Law and the Media: The Issue

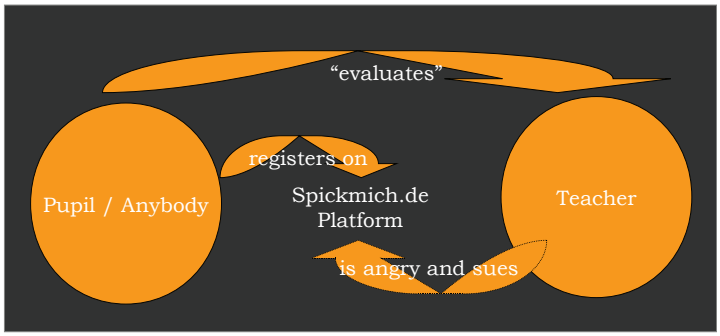
- So:
  Media publication "online"
  = data processing
- Yet:
  Strict data protection regime ~~may be~~
  is in conflict with freedom of speech / press / broadcasting

Data Protection Law and the Media: The Solution (until recently)

- Media "background activities":
  Data protection law media privilege*
- Publication of personal data: Media law ignores applicability of data protection law** and judges along "classic" balancing rules

**We'll come to that very soon* ***At least in Germany*

The Spickmich.de Case - a typical UGC constellation*



** And – to my knowledge – the first German online publication case to consider data protection law*

User-generated Content

Data Protection Law and User-generated Content

- Anybody can (and does) publish online

→ "Anybody is a data controller" *(Wong)*

- BUT: What about "in the course of a purely personal or household activity"? *ECJ in "Lindqvist": Not if you publish online! **

**This might be worth questioning / discussing!*

Media Privileges for User-Generated Content: The Solution (now)?

- Journalistic purposes exemption

Art. 9 Directive 95/46/EC

*Member States shall provide for **exemptions or derogations** from the provisions of this Chapter, Chapter IV and Chapter VI for the processing of personal data carried out **solely for journalistic purposes** or the purpose of artistic or literary expression only if they are **necessary to reconcile the right to privacy with the rules governing freedom of expression**.*

But: What exactly are journalistic purposes?

- Five points of view:
  - *Article 29 Group*
  - *Swedish Supreme Court*
  - *Advocate General*
  - *European Court of Justice*
  - *German Federal Court of Justice*

But: What exactly are journalistic purposes?

1. Article 29 Group (Rec. 1/97)

- *Derogations and exemptions under article 9 might not be necessary where the flexibility of various provisions of the directive or the derogations allowed under other specific provisions (which of course must also be interpreted narrowly)* ***already allow a satisfactory balance*** *between privacy and freedom of expression to be struck.*
- *Derogations and exemptions under article 9 can […] be granted […] to anybody processing data for journalistic purposes.*
- *Derogations and exemptions may cover only data processing for* ***journalistic (editorial) purposes including electronic publishing****.*

But: What exactly are journalistic purposes?

2. Swedish Supreme Court
(293-00 - Ramsbro)

- *[…]* ***inform, exercise criticism and initiate debate in societal issues of importance for the public.***
- *The fact that electronic or other media published texts contain insulting or deprecating data or judgements does not mean that this takes away its character of journalistic purpose. On the contrary such a fact is to be looked upon as a normal ingredient within the scope of a critical societal debate.*

But: What exactly are journalistic purposes?

3. Advocate General (C-73/07 - Satamedia)

- *65. The concept of journalistic purposes* ***refers to the activity of the mass media, particularly the press and audiovisual media****. The origin of the Data Protection Directive shows that journalistic purposes are* ***not confined to the activity of institutionalised media****. As the Commission initially proposed an exception for press organs and audiovisual media, the term 'journalistic purposes' resulted from several succeeding drafts which broadened the scope of the exception for media undertakings and extended it to* ***all persons engaging in journalistic activity.***

But: What exactly are journalistic purposes?

3. Advocate General (C-73/07 - Satamedia)

- *68. […] the dissemination of personal data pursues journalistic purposes if it **aims to impart information and ideas on matters of public interest.***
- *77. […] information and ideas relate to a matter of public interest **where they link up with a public debate which is actually taking place or where they concern questions which, according to domestic law and social values, are by nature public issues,** but not where details of an individual's private life are disseminated which have no connection with a public function of the person concerned, particularly where there is a legitimate expectation of respect for private life.*

But: What exactly are journalistic purposes?

3. Advocate General (C-73/07 - Satamedia)

- *However, it must be added that **State authorities, including the courts, cannot ascertain exactly where there are journalistic purposes.** It is hardly possible to determine in advance what information relates to matters of public interest and, in the final analysis, it is at least partly up to the media to create public interest in the first place by the communication of information.*

But: What exactly are journalistic purposes?

4. ECJ (C-73/07 - Satamedia)

- *62. […] Article 9 of the directive is to be interpreted as meaning that the activities referred to at points (a) to (d) of the first question, **relating to data from documents which are in the public domain under national legislation**, must be considered as activities involving the processing of personal data carried out 'solely for journalistic purposes', within the meaning of that provision, if the sole object of those activities is **the disclosure to the public of information, opinions or ideas**.*

But: What exactly are journalistic purposes?

5. German Federal Court of Justice (VI ZR 196/08 - Spickmich.de)

- *Media privilege (journalistic-editorial purposes) is only for those services* ***"deserving" special press treatment****.*
- ***Just collecting and transmitting users' contributions*** *(even if they are journalistic / editorial in nature) does not constitute journalistic purposes*
- *(HOWEVER: Freedom of expression* ***can be a legitimate interest for data processing*** *(Art. 7 lit. f DPD)*

Your solution?

- Public interest as the standard test for journalistic purposes?
- Disclosure to the public as always representing journalistic purposes?
- From "anybody is a data controller" to "anybody is a journalist"?
- Alternatives?

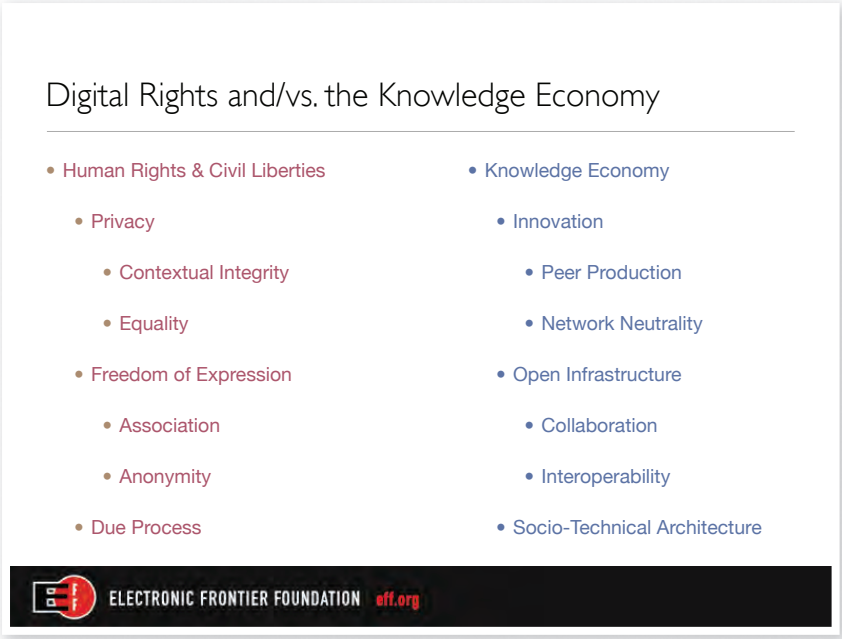
My suggestion so far:

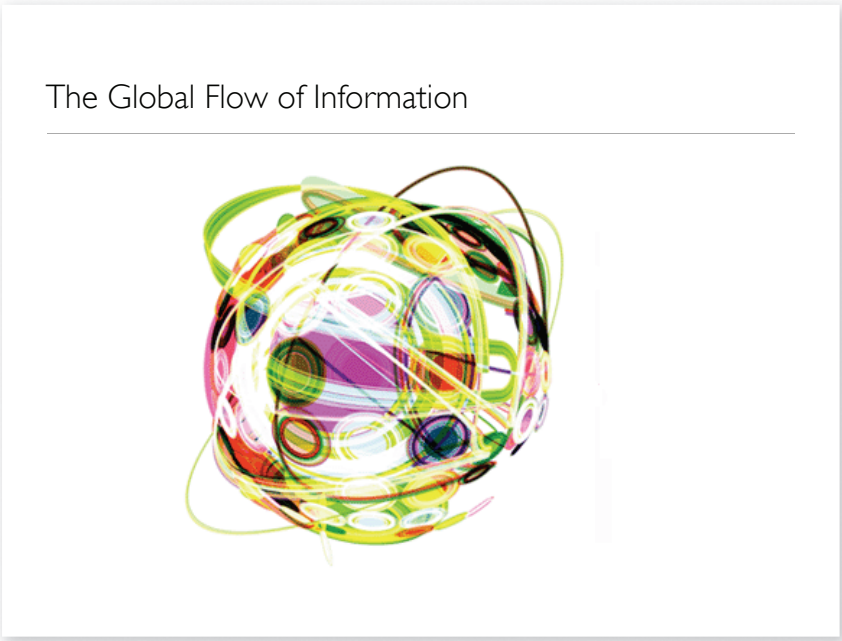
- Not everyone will be pursuing "*journalistic* purposes" when publishing online
- Differentiation between (mass) *media* activity and individual exercise of freedom of *speech*
- Some (non-exclusive) criteria for identifying journalistic activity:
  - Periodical publication
  - Objectivity as a basis of reporting
  - Universality in reported topics
  - "Publicity" (meaning a certain "audience")
  - Integration into editorial (or similar) structures
  - …

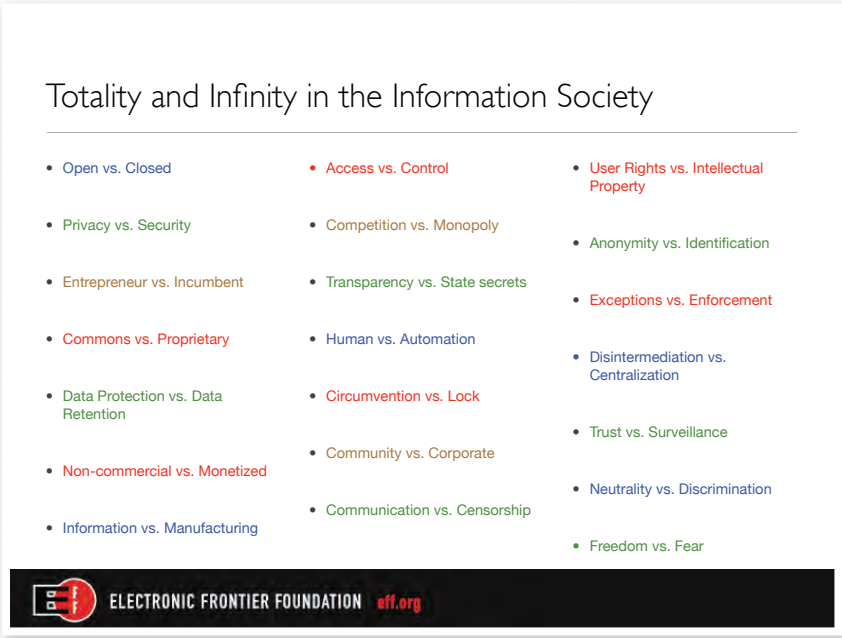
Thanks

Any more suggestions?
I'll appreciate them.

s.heilmann@hans-bredow-institut.de







The final slot presented a NGO activist strategy to implement privacy ethics in EU-funded research. Eddan Katz, International Affairs Director of the EFF (Electronic Frontier Foundation), demanded for complete restoration of due process in the knowledge economy and information society.

The EFF sees the due process paradigm endangered by the 9/11 shift towards a more and more surveilling society. By showing a promotional video from an EU-funded project called INDECT ("Intelligent Information System Supporting Observation, Searching and Detection for Security of Citizens in Urban Environment"). The organization opts for a dedicated privacy ethics review of EU-funded projects.

by Eddan Katz, EFF

Restoring the Paradigm of Due Process

- Presumption of Innocence
- Burden of Proof
- Probable Cause
- No prior restraint
- Particularized Suspicion
- Proportionality
- Right to Appeal
- Impartial Judge

The Surveillance Society

- Panopticon (Bentham)
  - Omni-present surveillance
  - Disciplinary Power of the Gaze (Foucault)
- Digitally Networked Environment
  - Borderless Communication
  - Information Intermediaries
  - No sidewalks in Cyberspace
- Balancing Tests (Lyon)
  - Coordination - how social relations reshaped
  - Risk - risk management decision-making
  - Privacy - socio-technical architecture
  - Power - information assymetries and social conditioning

Echelon and Data Mining

- UK-USA Security Agreement [WWII] (Australia, Canada, New Zealand, UK, and US)
  - Hierarchical Military Access to Intelligence Information
  - Menwith Hill: Transborder surveillance of domestic citizens
  - Industrial Espionage for Domestic Protectionism
  - Data Mining Framework Inversion of Due Process
- Report on the Existence of a Global System for the Interception of Private and Commercial Communications (ECHELON interception system). 2001/2098(INI). (11 July 2001).
  - Voted on September 5, 2001
- Violation of Data Protection Directive
- Fundamental Right to Privacy (Art. 8 ECHR)
- Cryptography as a Means of Self-Protection

The 9/11 Paradigm Shift

- Amplified Threat of Terrorist Violence
  - Distortion of Balancing Tests
    - War and Security vs. Freedoms and Rights
  - Technology and Responsibility
    - Autonomous Technics as out-of-Control
    - Network Effects
- Continental Europe Strategic Constraints
  - Diplomatic Intelligence Reciprocity
  - No Effective Search
  - Governance & Ethics

EU INDECT Project

- Intelligent information system supporting observation, searching and detection for security of citizens in urban environment
  - to develop a platform for: the registration and exchange of operational data, acquisition of multimedia content, intelligent processing of all information and automatic detection of threats and recognition of abnormal behaviour or violence
  - to develop the prototype of an integrated, network-centric system supporting the operational activities of police officers, providing techniques and tools for observation of various mobile objects
  - to develop a new type of search engine combining direct search of images and video based on watermarked contents, and the storage of metadata in the form of digital watermarks

INDECT Project Funding & Launch

- Framework Programme 7
- Research area: SEC-2007-1.2-01 Intelligent urban environment observation system
  - Start Date: 2009-01-01
  - Duration: 60 months
  - Project Cost: 14.86 million euro
- http://www.indect-project.eu/
- Beta Launch -> UEFA 2012 Championship (Poland/Ukraine)

Activist Intervention Proposal # 1: Going Viral on the YouTube Video

- Raising awareness by forwarding INDECT Project YouTube video to interested friends and colleagues and encouraging thoughtful and educating comments.
- http://www.youtube.com/watch?v=dl5g93m-SbA

INDECT Partners

- AGH University of Science and Technology (Poland) - Project Coordinator http://www.agh.edu.pl/en
- Gdansk University of Technology (Poland) http://www.pg.gda.pl
- InnoTec DATA G.m.b.H. & Co. KG (Germany) http://www.innotec-data.de
- Grenoble INP (France) http://www.grenoble-inp.fr
- MSWIA - General Headquarters of Police (Poland) http://www.policja.pl/
- Moviquity (Spain) http://www.moviquity.com/webingles/index.htm
- PSI Transcom GmbH (Germany) http://www.psi.de/
- Police Service of Northern Ireland (United Kingdom) http://www.psni.police.uk/
- Poznan University of Technology (Poland) http://www.put.poznan.pl
- Universidad Carlos III de Madrid (Spain) http://www.uc3m.es
- Technical University of Sofia (Bulgaria) http://www.tu-sofia.bg
- University of Wuppertal (Germany) http://www.uni-wuppertal.de
- University of York (Great Britain) http://www.york.ac.uk
- Technical University of Ostrava (Czech Republic) http://www.vsb.cz
- Technical University of Kosice (Slovakia) http://www.tuke.sk/tuke?set_language=en&cl=en
- X-Art Pro Division G.m.b.H. (Austria) http://www.x-art.at
- Fachhochschule Technikum Wien (Austria) http://www.technikum-wien.at

ELECTRONIC FRONTIER FOUNDATION eff.org

Activist Intervention Proposal #2: Make INDECT Project Deliverables Public

- University Research Center Contacts
  - Computer Science research throughout the European-wide community can make sure that the project outcomes can be commented upon and criticized by tech & policy analysts.
- York University Social Media Project
  - XML Data Corpus: Report on methodology for collection, cleaning and unified representation of large textual data from various sources: news reports, weblogs, chat
  - Highlighted on Wikileaks - Oct. 4, 2009. Made available publicly subsequently at http://indect-project.eu/files/

ELECTRONIC FRONTIER FOUNDATION eff.org

EU Security-Industrial Complex

- Ben Hayes, Statewatch. "NeoConOpticon"
  - http://www.tni.org/en/report/neoconopticon
- EU Security Research Program (7 yrs.) =1.4 bln Euros.
  - Funding of Applied Technology, Not Scientific Research
  - Industry Capture & Policy Laundering
  - Information Security industry growth
- Systematic Concentration of Entrenched Lobby

ELECTRONIC FRONTIER FOUNDATION eff.org

INDECT & Framework Program 7 Ethics Review

- University Research Centers & Project Partners each have an ethics review reporting to INDECT Ethics Review Representative:
  - Drew Harris, Assistant Chief Constable, Crime Operations Department, Police Department of Northern Ireland
- DG Research: Dir. L (Science, Economy, & Society), Unit 3 (Governance & Ethics)
  - Exclusion from funding: cloning, genetic manipulation.
  - Ethical Issues: Research on Human Beings; Privacy and Data Collection; Use of Animals; Research Involving Developing Countries; Dual Use

ELECTRONIC FRONTIER FOUNDATION eff.org

Activist Intervention Proposal #3: Introduce External Ethics Review and Opinion

- DG Research - Governance & Ethics Unit Continuous Reporting Review
- Provide Technology, Law, & Policy experts for outsourced review. SINAPSE
- European Data Protection Supervisor
  - Article 46 (e) - exert prior notification & monitoring developments

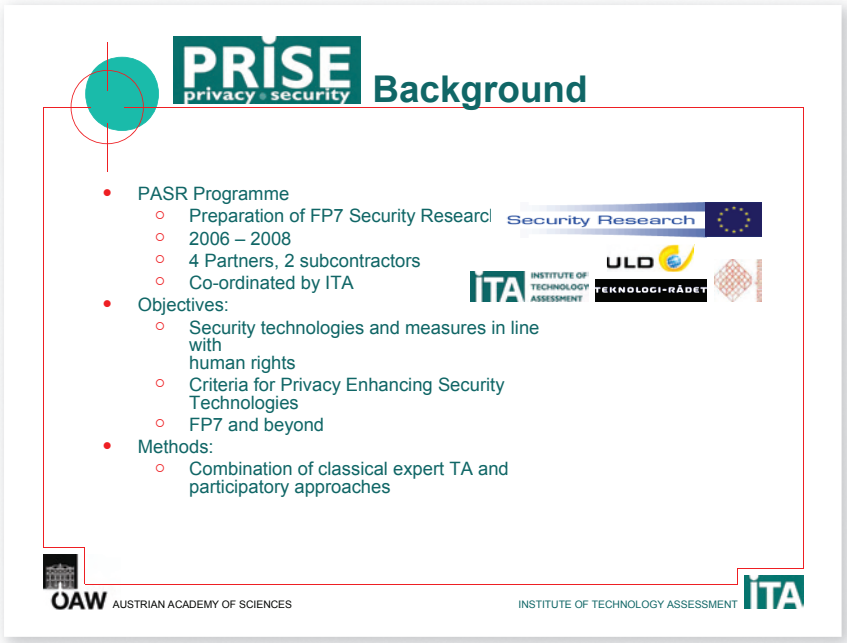
Re-identification & the Private/Commercial Transfer to Law Enforcement of Potentially Identifiable Information

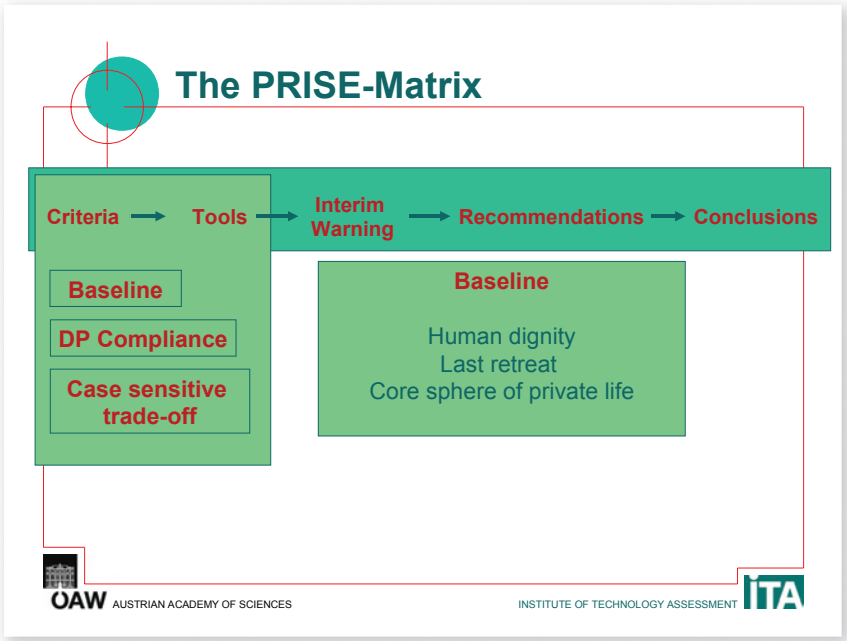
- Data can either be useful or perfectly anonymous but never both. (Paul Ohm)
- Compelled Transfer of Personal Data for National Security and Law Enforcement Reasons
- Behavioral Targeting Advertising supporting web growth
- Data Mining Providing Commercially Valuable Data

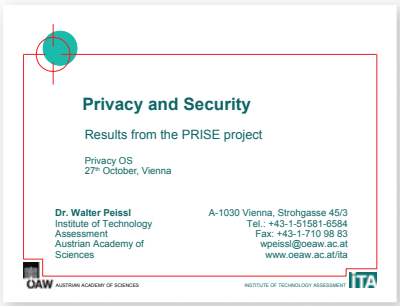
Activist Intervention Proposal #4: Institutionalize Privacy Ethics for Contextual Integrity

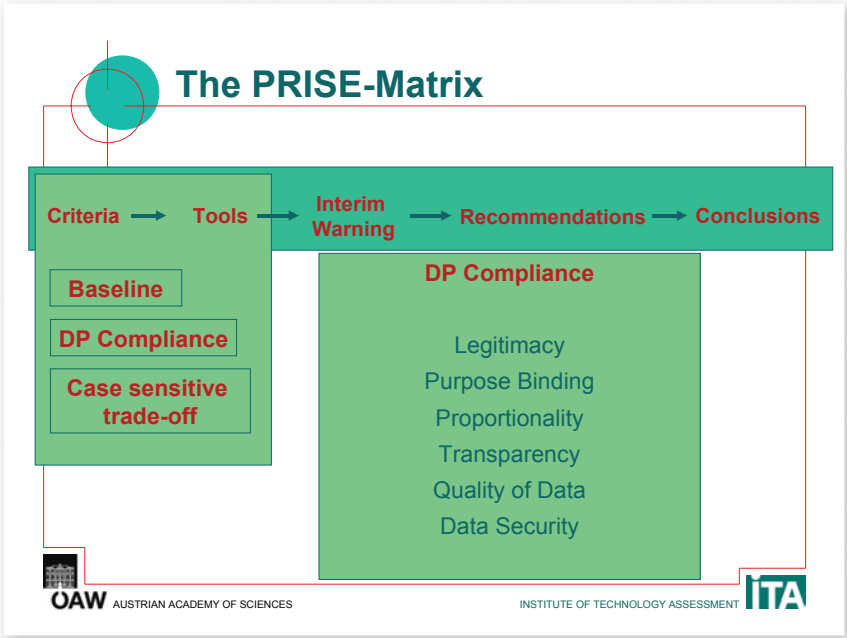
- Framework Program Review 7 Mid-Term Review (2010)
  - Insufficient focus on privacy ethics beyond Data Protection Directive
  - Institutionalize privacy ethics guidelines for EU-funded security research
  - Internal Support from Governance & Ethics Unit
- Data Protection Directive Consultation (Dec. 31, 2009)
  - Potentially Identifiable Information
  - Higher Standard of Privacy Ethics for Research
  - Preserving Contextual Integrity between Commercial & Law Enforcement

- Please Support EFF: http://www.eff.org/support
- eddan@eff.org







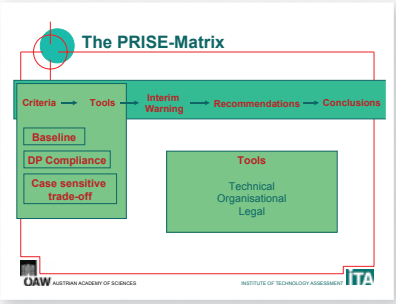


Encouraged by Eddan Katz' presentation, Walter Preissl spontaneously gave a short overview of the results of the PRISE-Project.

PRISE, an EC-funded research effort, has developed a methodology to include proactive privacy practises at early stages of research.

Possibly due to lack of time, the results were not incorporated for the 7th Framework Programme's calls. If this had happened, the current concerns regarding the INDECT-Project might have been avoidable.

by Walter Preissl, ITA



The PRISE-Matrix

Criteria → Tools → Interim Warning → Recommendations → Conclusions

- Baseline
- DP Compliance
- Case sensitive trade-off

Case sensitive trade-off

technology complies with privacy principles
known (estimated) security gain negligible

or

technology does not comply with privacy principles
known (estimated) security gain high

OAW AUSTRIAN ACADEMY OF SCIENCES — INSTITUTE OF TECHNOLOGY ASSESSMENT ITA

Outcome

- The PRISE Matrix
  - Procedure
- The PRISE Handbook
  - Guidance
- Checklists
  - Realisation
- Statement paper
  - Recommendations

http://prise.oeaw.ac.at

OAW AUSTRIAN ACADEMY OF SCIENCES — INSTITUTE OF TECHNOLOGY ASSESSMENT ITA

Recommendations

- Baseline of privacy
- No zero sum game
- No general access to databases
- Essential non-functional requirement
- Shared responsibility
- Regular reassessments as safeguard

OAW AUSTRIAN ACADEMY OF SCIENCES — INSTITUTE OF TECHNOLOGY ASSESSMENT ITA

Conclusion and Outlook

This 3rd PrivacyOS conference has shown the importance of having a platform for European experts for exchange of data protection issues and topics. The success of the conference furthermore lies on bringing together representatives of NGOs, industry, academia as well as regulators. This leads to important discussions from several points of view and widens the horizon in many ways. The variety of topics shows the different areas in which privacy is discussed and has to be discussed. The reports of the data protection authorities demonstrate that there is a need to exchange experiences in fields of eID, eGovernment and eHealth. Furthermore, EU funded projects use PrivacyOS as a platform to discuss open issues within the project and to gain information from experts that are not part of the project.

PrivacyOS managed to gain attraction for representatives from relevant NGOs, as well as enterprises, such as Microsoft. By way of the Open Space approach all these experts were encouraged to hold slots, thus covering a variety of topics from net activist projects to citizen rights. But the event also raised attention beyond the inner-european discourse, which is shown by the participation of an US expert. Quantitative, qualitative as well as informal feedback by the participants during the event shows overall satisfaction. The good to excellent ratings within the questionnaire regarding content and presentation also indicate approval of the concept and implementation of the project.

The 3rd conference in Vienna was held under the patronage of the Chairman of the ARGE DATEN – Privacy Austria, Dr. Hans G. Zeger. The ARGE DATEN is a non-profit marketing and non-governmental organisation in Austria and is examining the interaction between the usage of computer science, information law and society. The representation of the conference by respected patrons further supports the outreach of the project.

PrivacyOS is also seen as an information service on privacy issues in the EU. Participants want to be informed and want to use new approaches regarding important privacy issues in their products and activities. The idea of PrivacyOS to bring together activities, initiatives and projects active in privacy protection across Europe and to give an opportunity to articulate and exchange best practices, challenges and solutions following the Open Space approach stipulated increasing interest.

In concluding, the expected impact of the project, to create a long-term collaboration in the thematic network and to establish collective interfaces to other EU projects as well as national and international networks has well developed. Furthermore the PrivacyOS conference has expanded to being a motor for momentum among European Privacy experts.

PRIVACY OS

www.privacyos.eu