Norsk Regnesentral
NORWEGIAN COMPUTING CENTER

www.nr.no

Privacy and Regulatory Requirements

Lecture 12 in INF3510 - Information Security
University of Oslo

Dr. Lothar Fritsch

Norsk Regnesentral
Norwegian Computing Center

Oslo, Norway

April 28, 2011

Dr. Lothar Fritsch

- Research Scientist in IT Security & Privacy in Norsk Regnesentral's ICT research department
- Diploma from University of Saarland
- PhD studies at Frankfurt's Goethe University's Information Systems department, PhD (Privacy specification for location services)
- Industry experience in IT security product management (e-Banking, e-Signatures, Payment)
- Participant in EU PET research, e.g. SEMPER, PRIME, FIDIS

Web: www.nr.no/ ~lothar

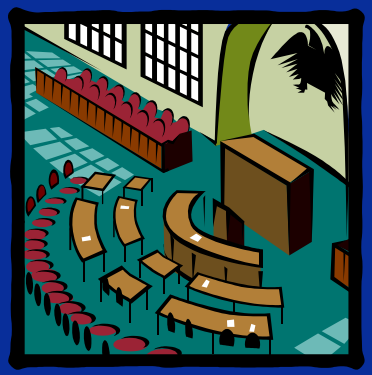
Lecture

- Regulation of IT
  - Examples: Finance, Electronic Signatures, Data protection
  - Data protection regulation
- Information Privacy & Privacy Enhancing Technologies (PETs)
  - What tools for anonymity & privacy are there?
  - Issues under deployment
- Case study: Location privacy in mobile apps

Regulation of IT security?

- Regulation is a term used for governmental control over societys' stakeholders' actions.
- Laws provide the grounds for regulation.
- Regulation follows political decisions, and usually relates to existing legal frameworks and societal demands.
- Regulation is often the result of either new risk for society, or persisting conflicts on the unregulated market, e.g. market failure.
- Self-regulation of stakeholders is another way of regulation.

Who regulates IT?



- The governments are the source of most regulation – even in the areas where government attention spawned effective self-regulation.
- Laws are suggested by government departments, parties, or parliaments.
- Law details are worked out by parts of the public administration.
- Post og Teletilsynet and Datatilsynet are specific supervisory authorities that regulate IT in Norway, among others.

Regulatory frameworks I: Basel II Financial Sector IT (2004)

- **Framework to regulate reliability of the financial sector**
- **Requirements for handling operational risk events:**
  1. Internal Fraud - misappropriation of assets, tax evasion, intentional mismarking of positions, bribery
  2. **External Fraud- theft of information, hacking damage, third-party theft and forgery**
  3. Employment Practices and Workplace Safety - discrimination, workers compensation, employee health and safety
  4. Clients, Products, & Business Practice- market manipulation, antitrust, improper trade, product defects, fiduciary breaches, account churning
  5. Damage to Physical Assets - natural disasters, terrorism, vandalism
  6. Business Disruption & Systems Failures - utility disruptions, software failures, hardware failures
  7. Execution, Delivery, & Process Management - data entry errors, accounting errors, failed mandatory reporting, negligent loss of client assets

Regulatory frameworks II: Electronic Signatures in Europe

- Goal: To provide a harmonized framework for the provision and use of electronic signatures in Europe.

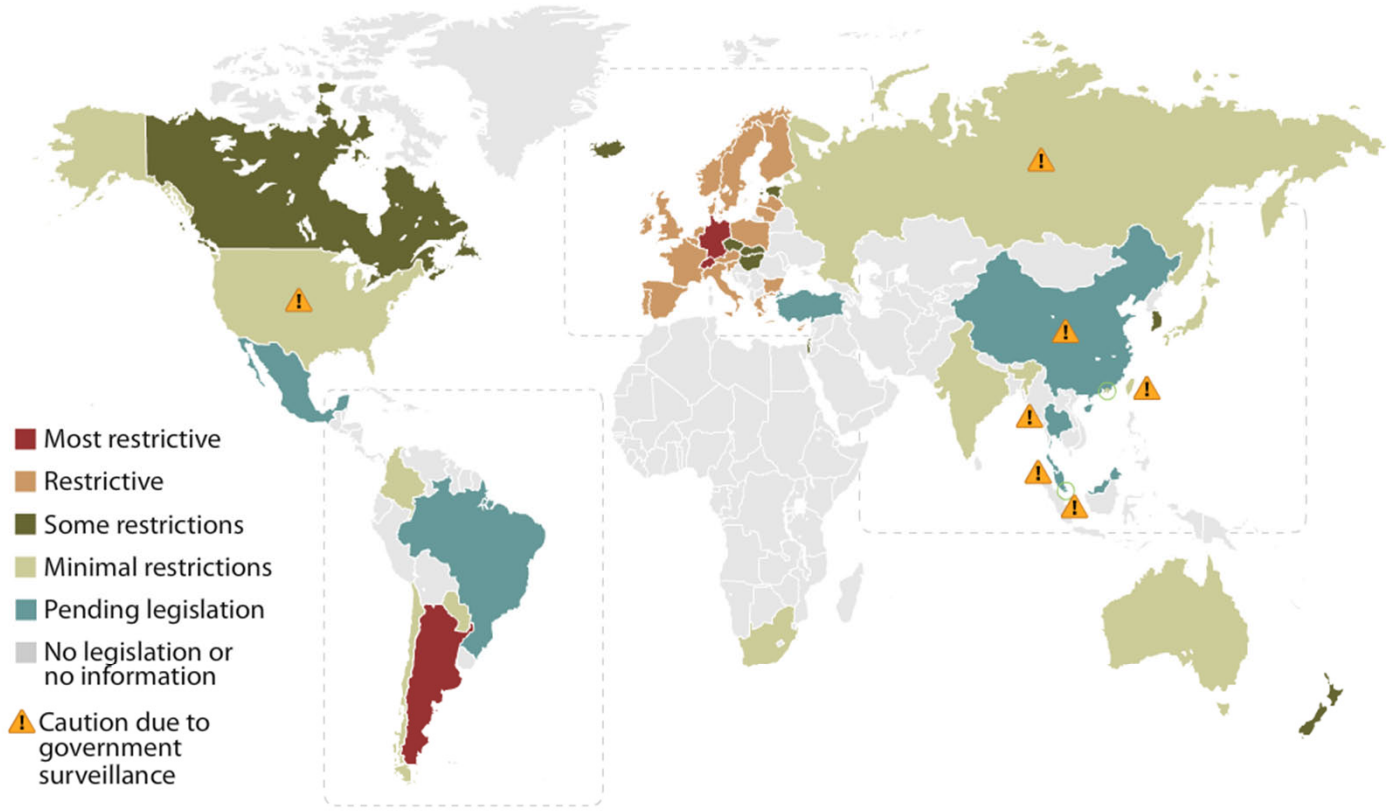
- Defines terms, applicability of e-signatures, responsibilities of certificate authorities (CAs), liability, and security requirements.
- Actual Common Criteria (ISO 15408) EAL4+ level security assurance required for «advanced signatures based on qualified certificates».
- CAs must hold 500.000€ assets for liability.

Commission of the European Union (1999) Community framework for electronic signatures: DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, Brussels.

Regulatory frameworks III: Data protection / privacy

- OECD guidelines define international basis for collection, use and transfer of personal data.
- Regional (e.g. EU-wide) formulation of common data protection rules for harmonized services.
- National implementation and supervision in national laws and law systems by the national governments.
- Datatilsynet is the supervisory authority in Norway. In Norway, privacy can easily be weakend through new laws (e.g. Skatteliste, road toll, whitewashing)
- Some countries require data breach publication.

Interactive Data Protection Heat Map

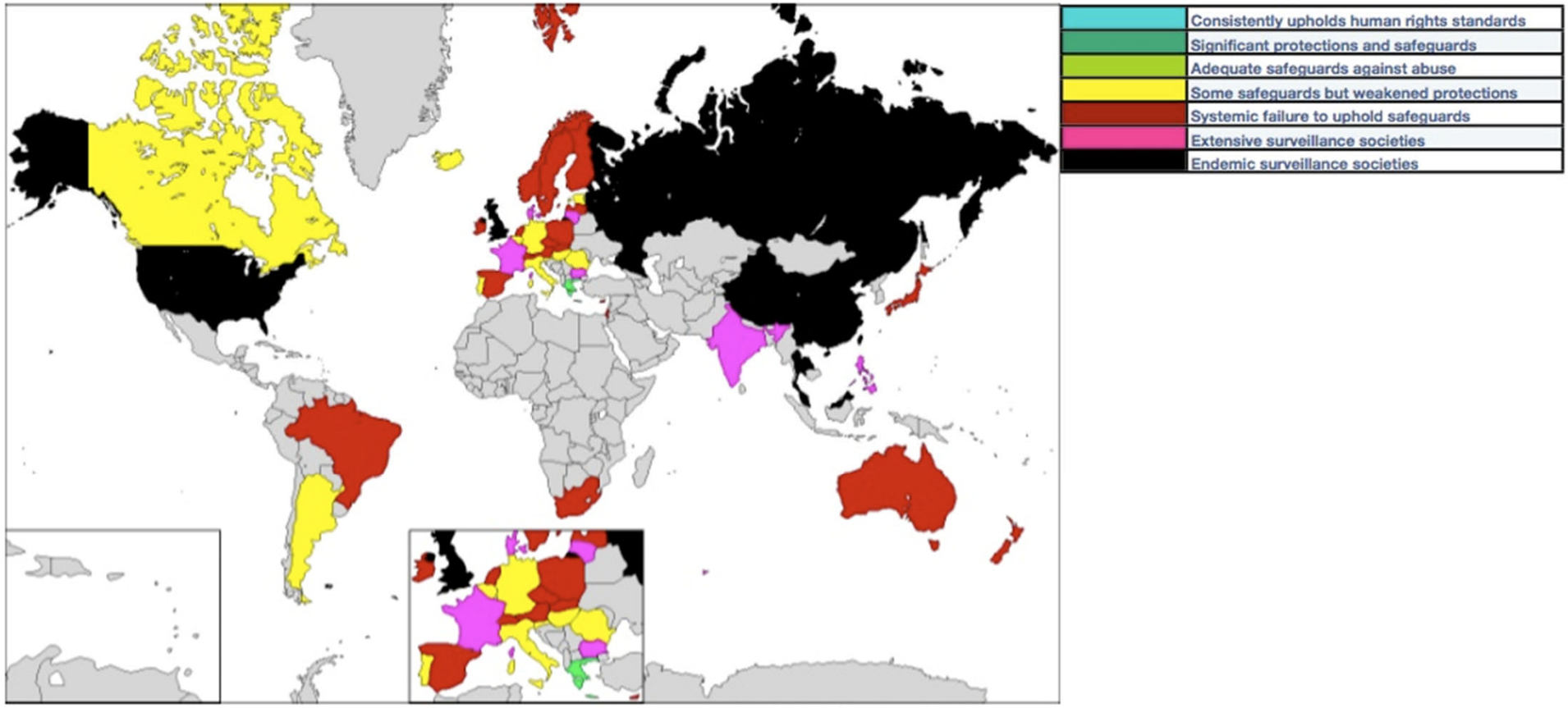


Source: US Department of Commerce and country specific legislation

Source: Forrester Research, Inc.

Note: This interactive map provides information on national data protection laws that have either been enacted or are currently under consideration around the world. It does not address sectoral laws, local laws, criminal/civil code provisions, or constitutional provisions that may address data protection. It is intended for information only and is not an authoritative statement or summary of the actual laws in these countries, and it may not reflect all recent changes and legislative updates.

Map of Surveillance Societies around the world



Map developed from http://english.freemap.jp

https://www.privacyinternational.org/article/leading-surveillance-societies-eu-and-world-2007

Data Protection Regulation

- What is privacy?
- Complications with data protection
- Application of legal frameworks

What is «privacy»?

- The «right to be left alone», American postulation by Warren & Brandeis in Harvard Law Review 193 (1890).
- European focus on government-citizen relationship grounded on freedom vs. totalitarism:
  - Data protection necessary to enable personal freedom and choice.
  - Informational self-determination basis for free decision, interaction and participation of citizens.
  - Often anchored in constitutions with reference to the fundamental human rights.

Complications with data protection

- Geographically: USA vs. Europe (e.g. Safe harbor).
- Legally: Jurisdictions different in different locations.
- Sectoral (USA): Industry self-regulation with occational sectoral regulation (e.g. health data).
- Future challenges: Interpretation of personal data through others in wrong contexts.

International: OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data – in OECD member countries

- Collection Limitation Principle
- Data Quality Principle
- Purpose Specification Principle
- Use Limitation Principle
- Security Safeguards Principle
- Openness Principle
- Individual Participation Principle
- Accountability Principle

http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html

EU directive on data protection

- Creates a harmonized space for handling personal information in EU and EFTA/EØS countries. Rules based on OECD.
  - Transparency, Legitimate purpose, Proportionality.
  - Supervisory authority and public register of processing operations.
  - Transfer of personal data to third countries.
- However, in most member states, a violation of privacy laws is not a capital crime of great interest to the government solicitor.

EU directive: Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data (2008)

Cross-border issues

- Today's internet services and mobile networks / apps are located in many countries.
- They can be moved easily, along with their data.
  - Resulting conflicts, e.g.: Passenger records, SWIFT transactions, access of Google or Yahoo records by local authorities
- Consequence: Safe harbor agreement EU-USA
- The regulation was made for central data centers, not for Cloud Computing and global mobile phone networks.

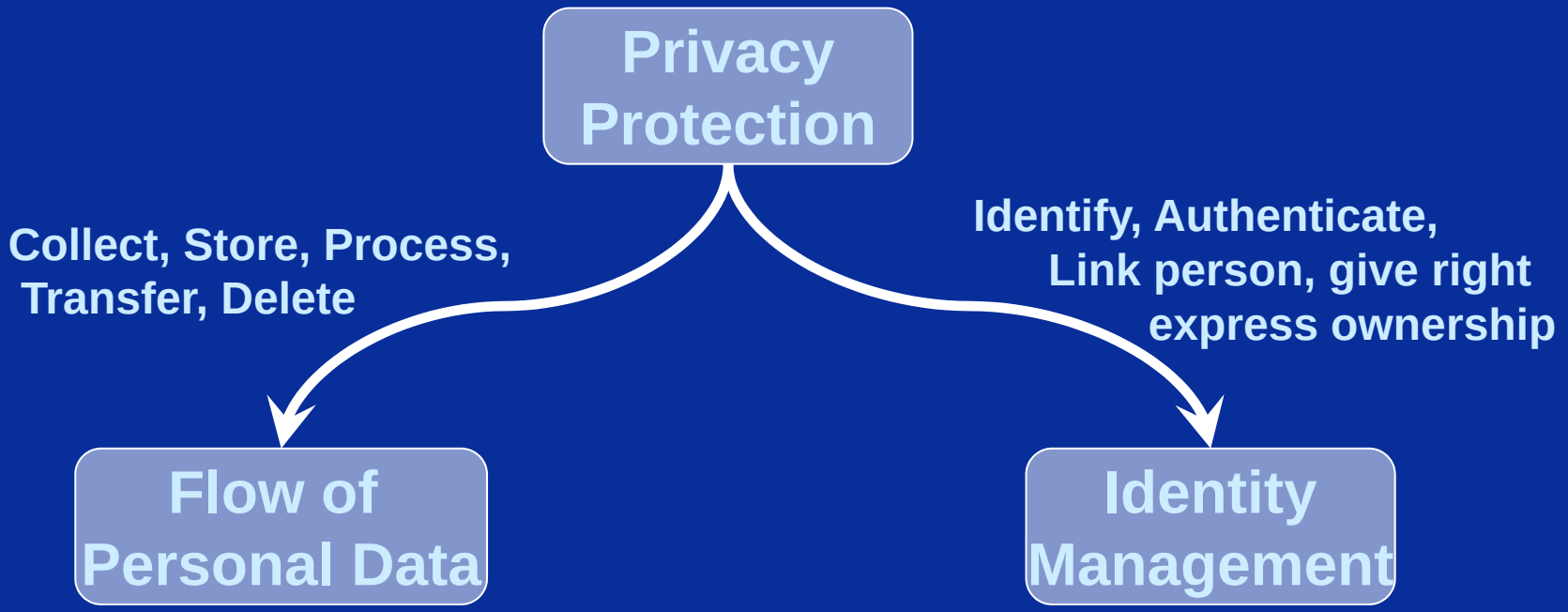
Tension with other laws

- Data retention for intelligence / criminal investigation.
- Anti-money-laundry frameworks require identification (BASEL II, Sarbane-Oxley).
- Specific tax laws, e.g. Norway's Skatteliste and Norway's scanning of credit card payments.
- Telecommunications regulation, e.g. concerning operations, or forensic needs (in Norway: «ekomloven» LOV 2003-07-04 nr 83: Lov om elektronisk kommunikasjon.)

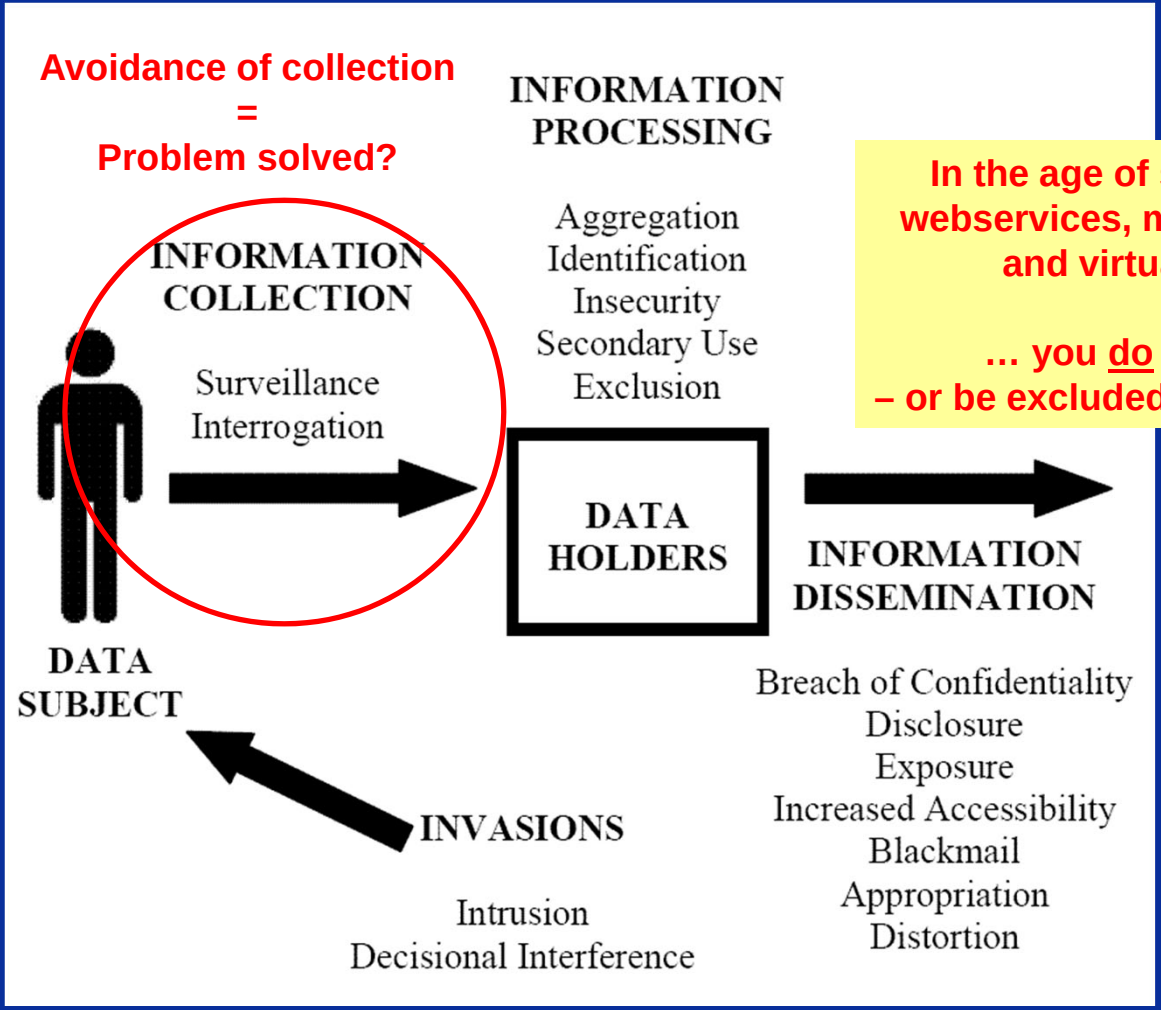
Application of Data protection laws

- Complex issue:
  - Analysis of various, possibly contradictory laws
  - Future introduction of new laws
  - Cross-border service or system mobility
  - User experience should not be impaired
  - Privacy management cost can be significant
- Privacy design vs. Business Model is a difficult challenge!
- Data minimization might be the «best guess».

Privacy Protection in IT Systems



Solove's privacy threat taxonomy



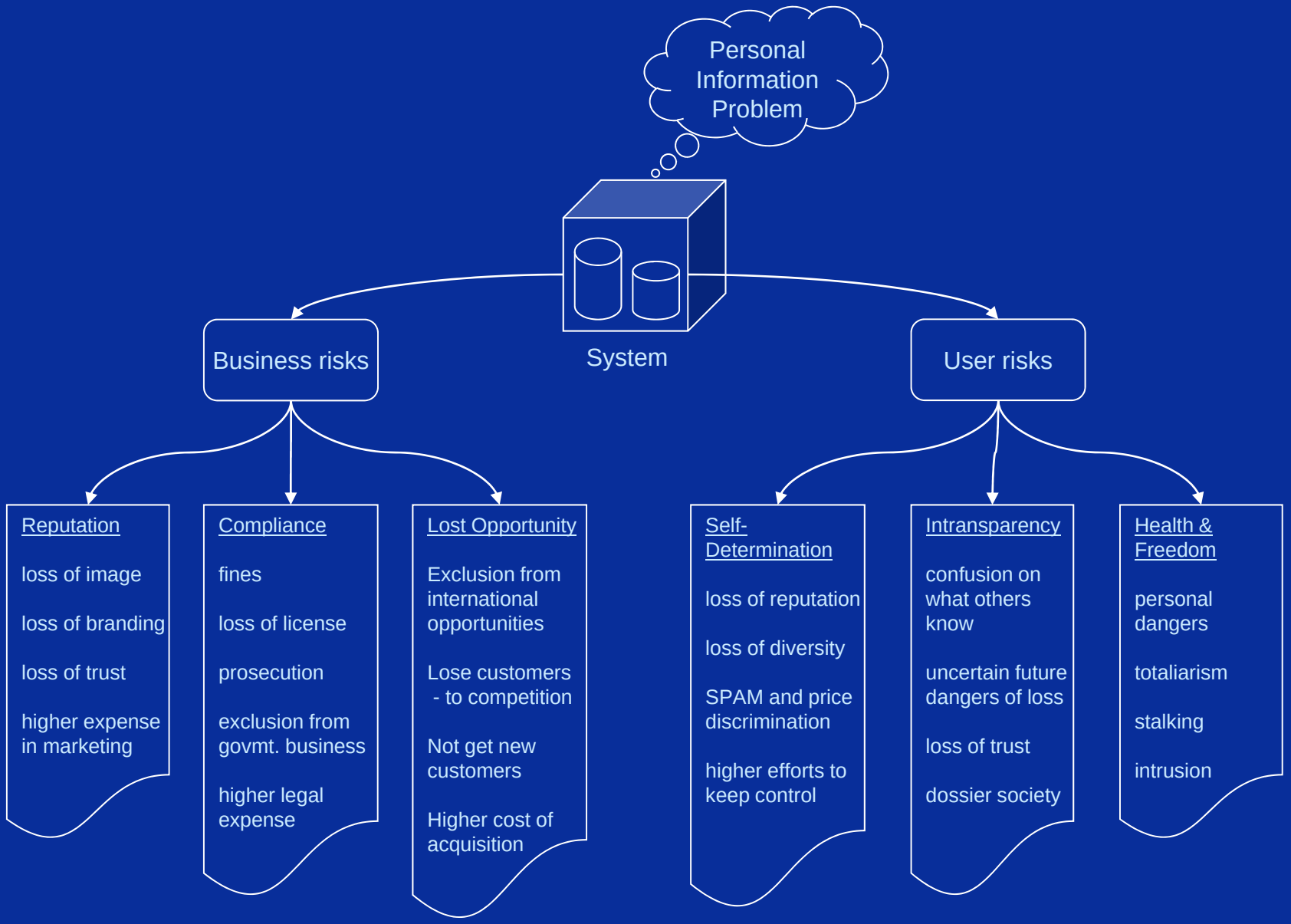
In the age of social networks, webservices, mesh-ups, Web 2.0 and virtual society….

… you do provide data – or be excluded from participation.

Solove, Daniel (2006) A taxonomy of privacy, : GWU Law School Public Law Research Paper No.129." *University of Pennsylvania Law Review* (154:3), pp. 477.

Duality of Privacy Risks

www.nr.no



Fritsch, Lothar; Abie, Habtamu: A Road Map to Privacy Management, Oslo, Norway, 2007

Privacy Principles applied to IT

Fundamental legal privacy principles

1.Principles concerning the fundamental design of products and applications :
    1.Data minimization (maximum anonymity and early erasure of data)
    2.Transparency of processing
    3.Security
2.Principles concerning the lawfulness of processing:
    a)Legality (e.g. consent)
    b)Special categories of personal data
    c)Finality and purpose limitation
    d)Data quality
3.Rights of the data subject:
    a)Information requirements
    b)Access, correction, erasure, blocking
    c)Objection to processing
4.Data traffic with third countries
5.Notification requirements
6.Processing by a processor – responsibility and control
7.Other specific requirements resulting from the Directive on Privacy and Electronic Communications 2002/58/EC/, Data Retention Directive 2006/24/EC and the Norwegian legislation.

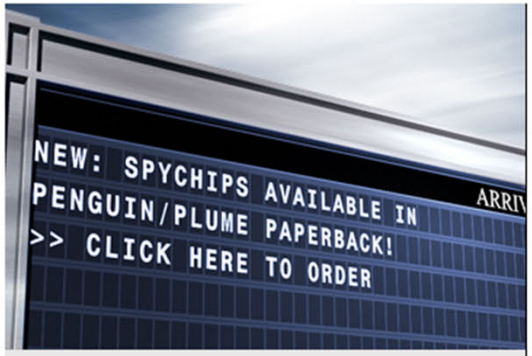
Information security elements in on-line privacy

- Data minimization:
  PETs and Identity Management
- Transparency: Processing policies
- Documented consent: Electronic Signatures
- General security of data:
  - Integrity of data
  - Access control to data collections
  - Obligations audit (review of policy & consent)
  - Deletion

Difficulties

- Laws are neutral concerning technology
  - There is no checklist on today's sufficient solution
  - Laws get interpreted against today's technology and its use
- Legal coherence is created in court
  - Often, legal decisions are made after system deployment
  - Technology and use cases develop faster than legal traditions

Example: RFID



search spychips.com
terms/keywords:
submit

subscribe to our free newsletter!
enter email address:
submit

what you can do as...
A CONSUMER >>
A LAWMAKER >>
A COMPANY >>

VERICHIP IMPLANTS >>

PATENTS

New! Includes IBM's patent application, "Identification and Tracking of Persons Using RFID-Tagged Items"

RFID NINETEEN EIGHTY-FOUR

Spychips: How Major Corporations and Government Plan to Track Your Every Purchase and Watch Your Every Move
by Katherine Albrecht and Liz McIntyre

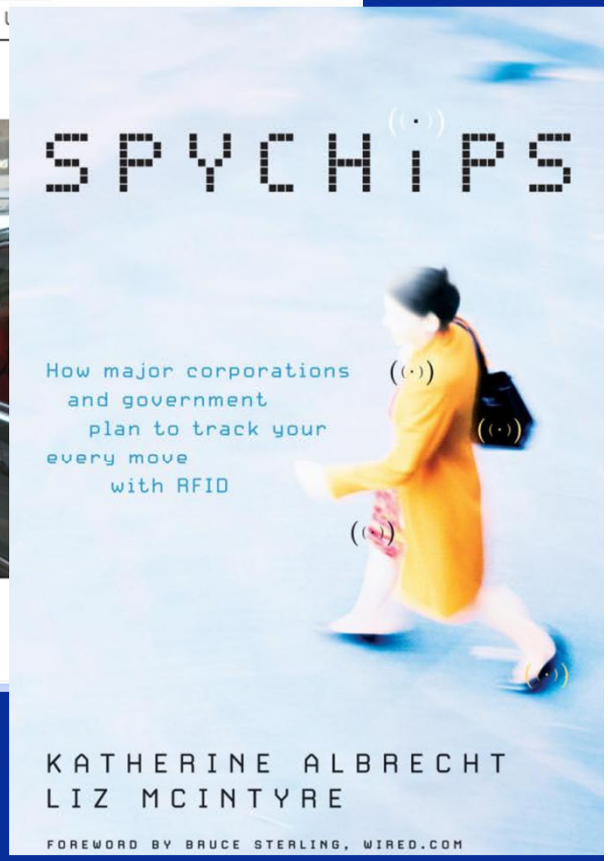
>> click here to order the paperback...
>> click here to learn more about the other books in the "Spychips" series...

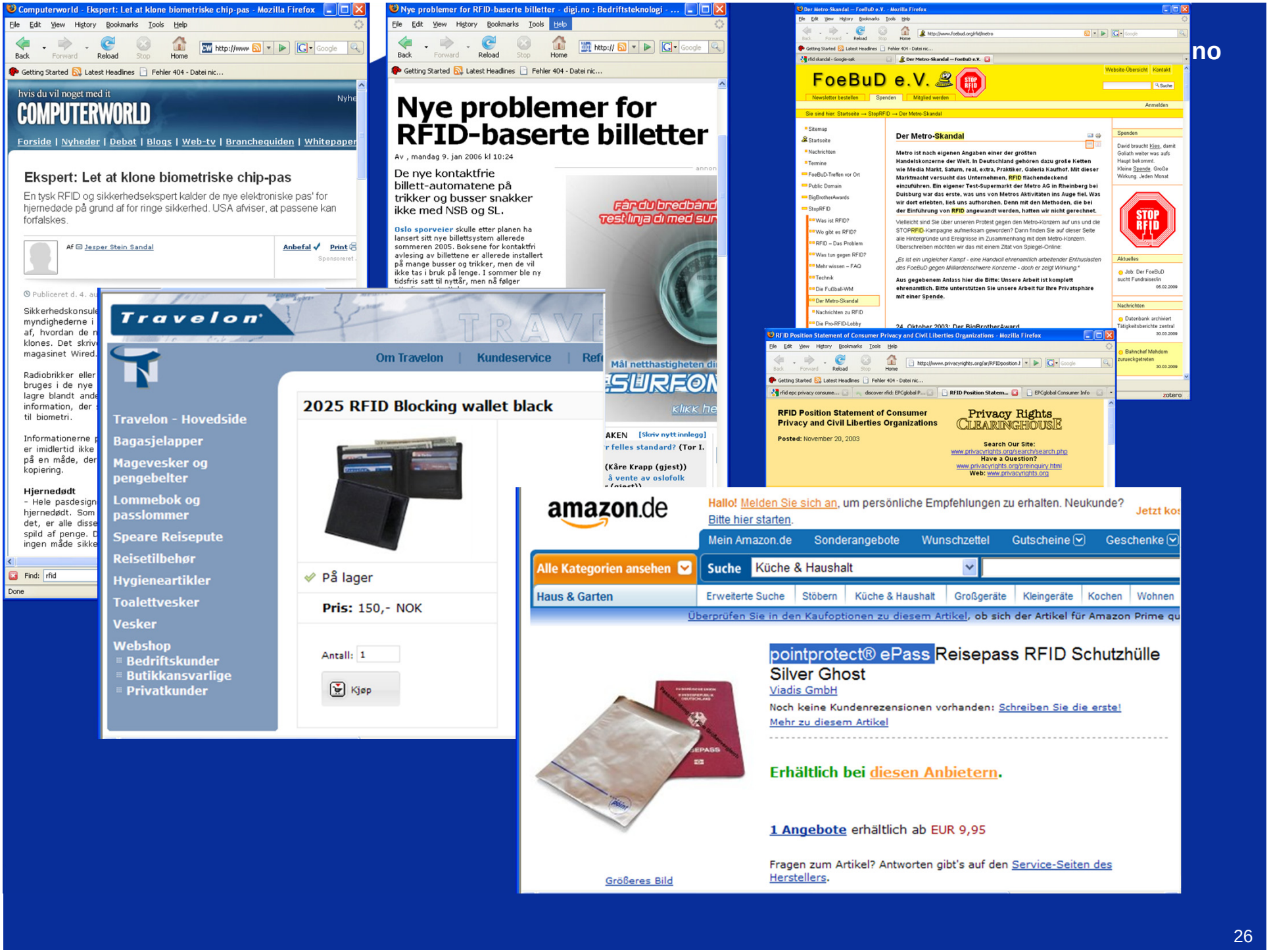
SPYCHIPS.COM

HOME OVERVIEW FAQ BLOG PRESS GET INVOLVED ABOUT

RFID Privacy Issues and News

Our RFID protest in NYC was a huge success! You can check out our original press release, see a local news story, read about the outcome on digg, or go directly to the report (with video) at homeland stupidity




Computerworld - Ekspert: Let at klone biometriske chip-pas - Mozilla Firefox
COMPUTERWORLD
Ekspert: Let at klone biometriske chip-pas
Nye problemer for RFID-baserte billetter - digi.no : Bedriftsteknologi - ...
Nye problemer for RFID-baserte billetter
Av , mandag 9. jan 2006 kl 10:24
De nye kontaktfrie billett-automatene på trikker og busser snakker ikke med NSB og SL.
Der Metro-Skandal – FoeBuD e.V. - Mozilla Firefox
FoeBuD e.V.
Der Metro-Skandal
RFID Position Statement of Consumer Privacy and Civil Liberties Organizations - Mozilla Firefox
RFID Position Statement of Consumer Privacy and Civil Liberties Organizations
Posted: November 20, 2003
Privacy Rights Clearinghouse
Travelon
Travelon - Hovedside
Bagasjelapper
Magevesker og pengebelter
Lommebok og passlommer
Speare Reisepute
Reisetilbehør
Hygieneartikler
Toalettvesker
Vesker
Webshop
Bedriftskunder
Butikkansvarlige
Privatkunder
2025 RFID Blocking wallet black
På lager
Pris: 150,- NOK
Antall: 1
Kjøp
amazon.de
Hallo! Melden Sie sich an, um persönliche Empfehlungen zu erhalten. Neukunde?
Bitte hier starten.
Mein Amazon.de
Sonderangebote
Wunschzettel
Gutscheine
Geschenke
Alle Kategorien ansehen
Suche
Küche & Haushalt
Haus & Garten
Erweiterte Suche
Stöbern
Küche & Haushalt
Großgeräte
Kleingeräte
Kochen
Wohnen
pointprotect® ePass Reisepass RFID Schutzhülle Silver Ghost
Viadis GmbH
Noch keine Kundenrezensionen vorhanden: Schreiben Sie die erste!
Mehr zu diesem Artikel
Erhältlich bei diesen Anbietern.
1 Angebote erhältlich ab EUR 9,95
Fragen zum Artikel? Antworten gibt's auf den Service-Seiten des Herstellers.
Größeres Bild

EPCglobal Guidelines on EPC for Consumer Products

1. Consumer Notice

Consumers will be given clear notice of the presence of EPC on products or their packaging and will be informed of the use of EPC technology. This notice will be given through the use of an EPC logo or identifier on the products or packaging.

2. Consumer Choice

Consumers will be informed of the choices that are available to discard or remove or in the future disable EPC tags from the products they acquire. It is anticipated that for most products, the EPC tags would be part of disposable packaging or would be otherwise discardable. EPCglobal, among other supporters of the technology, is committed to finding additional efficient, cost effective and reliable alternatives to further enable customer choice.

3. Consumer Education

Consumers will have the opportunity easily to obtain accurate information about EPC and its applications, as well as information about advances in the technology. Companies using EPC tags at the consumer level will cooperate in appropriate ways to familiarise consumers with the EPC logo and to help consumers understand the technology and its benefits. EPCglobal would also act as a forum for both companies and consumers to learn of and address any uses of EPC technology in a manner inconsistent with these Guidelines.

4. Record Use, Retention and Security

The Electronic Product Code does not contain, collect or store any personally identifiable information. As with conventional barcode technology, data which is associated with EPC will be collected, used, maintained, stored and protected by the EPCglobal member companies in compliance with applicable laws. Companies will publish, in compliance with all applicable laws, information on their policies regarding the retention, use and protection of any personally identifiable information associated with EPC use.

Revised September 2005, Source: http://www.epcglobalinc.org/public/ppsc_guide

Ontario's RFID privacy guide lines

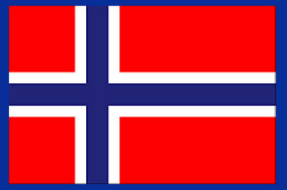
- **Focus on RFID information systems, not technologies:** The problem does not lie with RFID technologies themselves, but rather, the way in which they are deployed that can have privacy implications. The *Guidelines* should be applied to RFID information systems as a whole, rather than to any single technology component or function;
- **Build in privacy and security from the outset – at the design stage:** Just as privacy concerns must be identified in a broad and systemic manner, so, too, must the technological *solutions* be addressed systemically. A thorough privacy impact assessment is critical. Users of RFID technologies and information systems should address the privacy and security issues early in the design stages, with a particular emphasis on data minimization. This means that wherever possible, efforts should be made to minimize the identifiability, observability and linkability of RFID data; and
- **Maximize individual participation and consent**: Use of RFID information systems should be as open and transparent as possible, and afford individuals with as much opportunity as possible to participate and make informed decisions.

Ontario's privacy commissioner, Ann Cavoukian, 2006-2008

EU draft recommendations

1. RFID operators shall conduct privacy risk assessment!
2. Risk assessments should honor stakes, and cover all stakeholders!
3. Mandatory to take appropriate technical and organizational measures to mitigate the privacy risks!
4. Assign a responsible person for audit and adaption of the above!
5. Privacy & security risk management shall be aligned.
6. The privacy risk assessment summary must be published latest upon deployment of the RFID application.

Norwegian Regulation



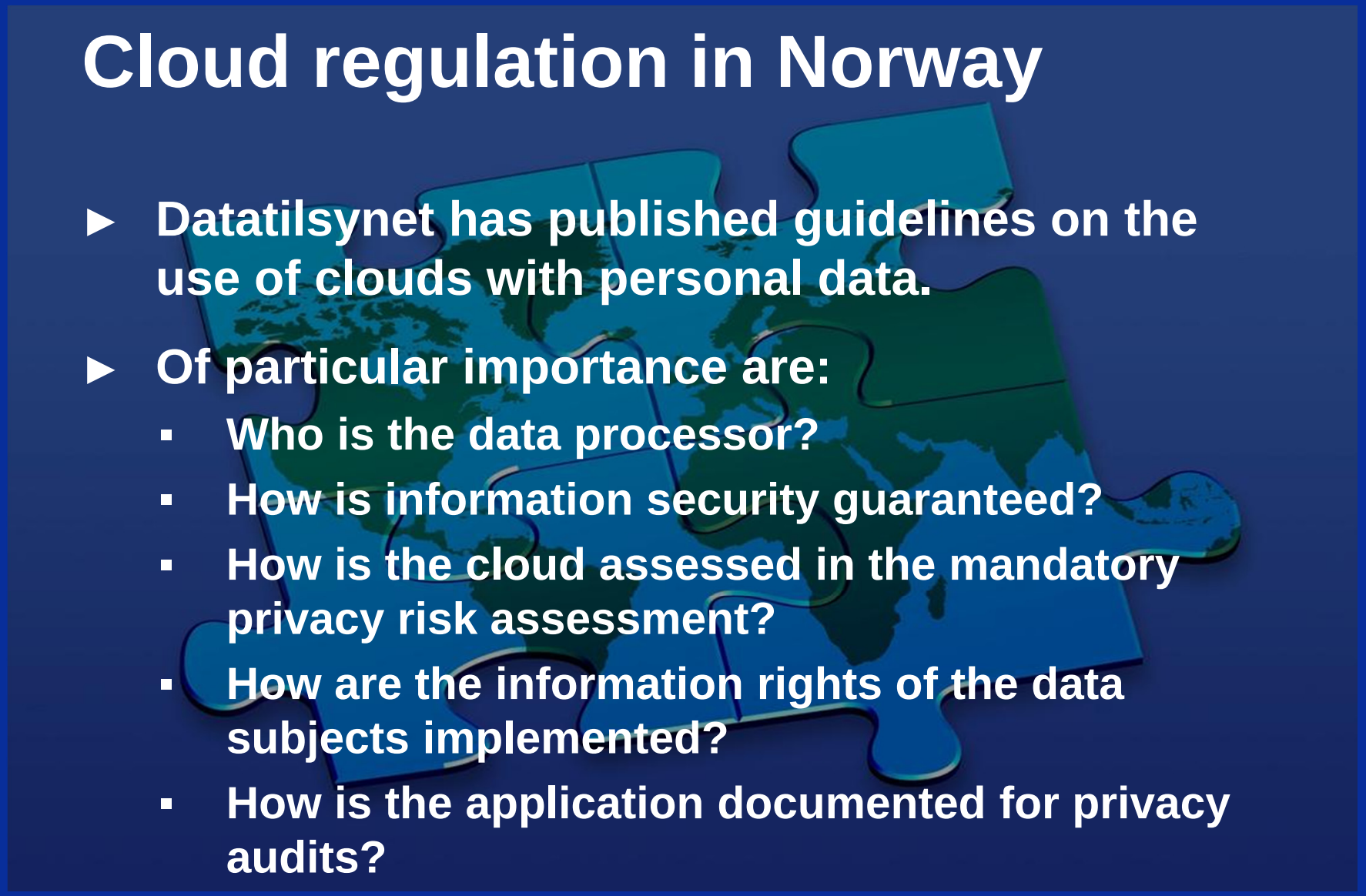
- General rules in ”personopplysningsloven” apply to RFID applications. No specific regulation has been implemented.
- BUT: Datatilsynet has already commented several RFID-based projects and formulated stringent requirements, e.g. in the case of passports:
  - Politidirektoratet shall assess privacy risks of biometric passport handling with repsect to §13 personopplysningsloven (POL) og §2-4 personopplysningsforskriften.
  - Politidirektoratet shall provide all necessary information to applicants and holders of biometric passports acc. to §19 POL.
  - Politidirektoratet must design and implement an internal privacy controlling system according to §14 POL. The system must not be outsourced.

►http://www.datatilsynet.no/upload/Dokumenter/saker/2006/passflvarsel.pdf

Example: Cloud Computing

- Cloud Computing is used here as outsourcing of physical computer operations to standardized «computing clouds» elsewhere.
- Cloud computing has issues concerning data ownership, physical control, cross-border data protection, espionage, and availability.
- Many businesses choose servers in the «cloud» over own infrasturcture.

Cloud regulation in Norway



- Datatilsynet has published guidelines on the use of clouds with personal data.
- Of particular importance are:
  - Who is the data processor?
  - How is information security guaranteed?
  - How is the cloud assessed in the mandatory privacy risk assessment?
  - How are the information rights of the data subjects implemented?
  - How is the application documented for privacy audits?

http://www.datatilsynet.no/upload/Dokumenter/veiledere/Veileder%20Cloud%20Computing%20ver%201.0_med_forside.pdf

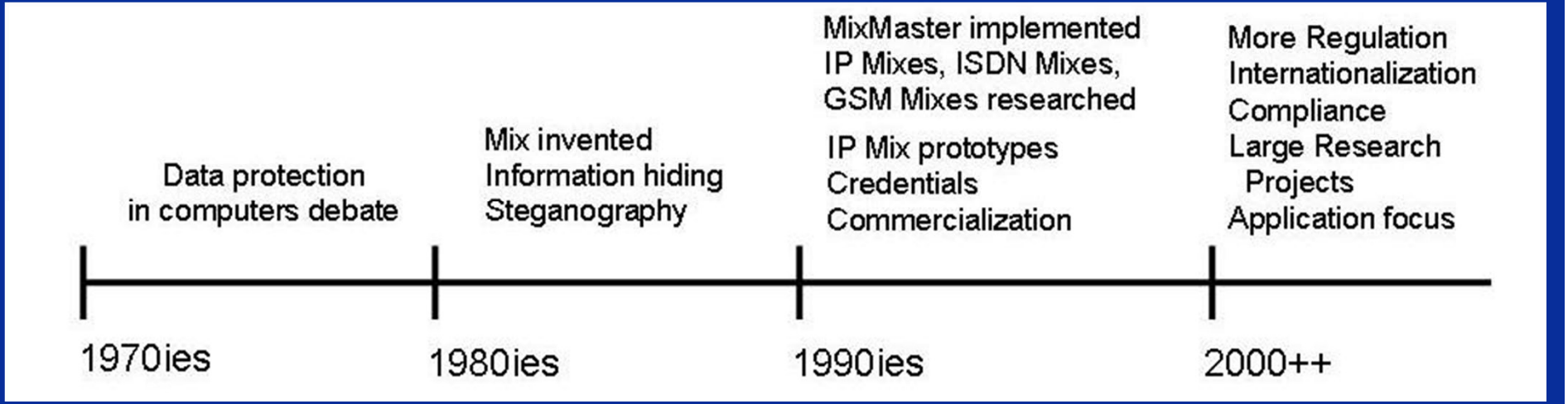
Privacy enhancing technology

- What are PETs?
- What PETs are available?
- How does «Privacy by design» work?
- Challenges for PETs

Privacy Enhancing Technology (PET): Definition

- A collection of IT artifacts that are used to minimize personal data, secure the use and storage of personal data, and enable the secure and privacy-preserving management of personal data.
- Many flavors and purposes, ranging from self-defense to corporate information management.
- Encryption is a building block for PET, but not enough to provide pseudonymity, anonymity or unlinkability of transactions.

A brief history of PET



- PET development inspired by the legal perspective on basic human rights.
- Technology-centric approach.
- PET research focused on information hiding & control.
- Much focus on the end user and his action options.

Taxonomy of PET

Category	Subcategory	Description
Privacy Protection	Pseudonymizer Tools	Enabling e-business transactions without requiring private information.
	Anonymizer Products and Services	Providing browsing and email capability without revealing the user's address and identity.
	Encryption Tools	Protecting email, documents and transactions from being read by other parties.
	Filters and Blockers	Preventing unwanted email and web content from reaching the user.
	Track and evidence erasers	Removing electronic traces of the user's activity.
Privacy Manage-ment	Informational tools	Creating and checking Privacy Policies.
	Administrative Tools	Managing user identity and permissions.

Privacy protection classification from (Meta Group, 2005).

Norsk Regnesentral
NORWEGIAN COMPUTING CENTER

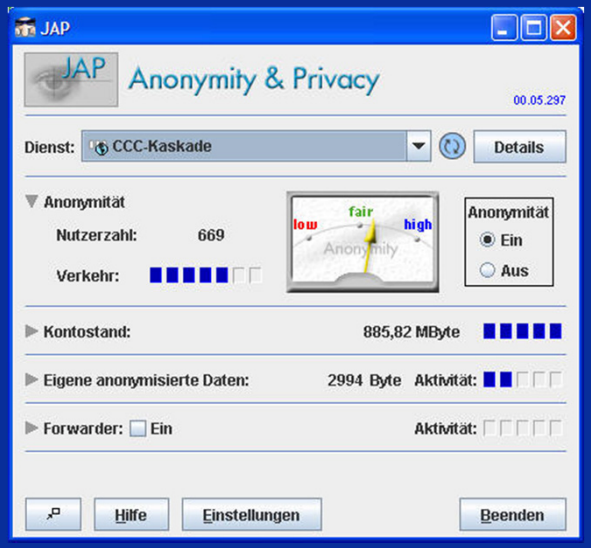
PET classification

www.nr.no

	Transparency tool	Opacity tools
Definiton	Tools that show clearly to a person what personal data is being processed, how it is processed, and by whom it is processed.	Tools that hide a person's identity or his relationship to data as it is processed by someone else.
Non-technical example	• Legal rights to be informed about data processing; • Privacy audits.	• Pseudonymous access to on-line services; • Election secrecy.
Technical example	• Database audit interfaces; • Audit Agents, • Log files.	• MixMaster anonymous e-mail; • TOR anonymizing web surfing; • Pseudonyms.

Fritsch, Lothar: State of the Art of Privacy-enhancing Technology (PET) - Deliverable D2.1 of the PETweb project. No. 1013, ISBN 978-82-53-90523-5, pp. 34, November 22, 2007.

PETs as Opacity Tools

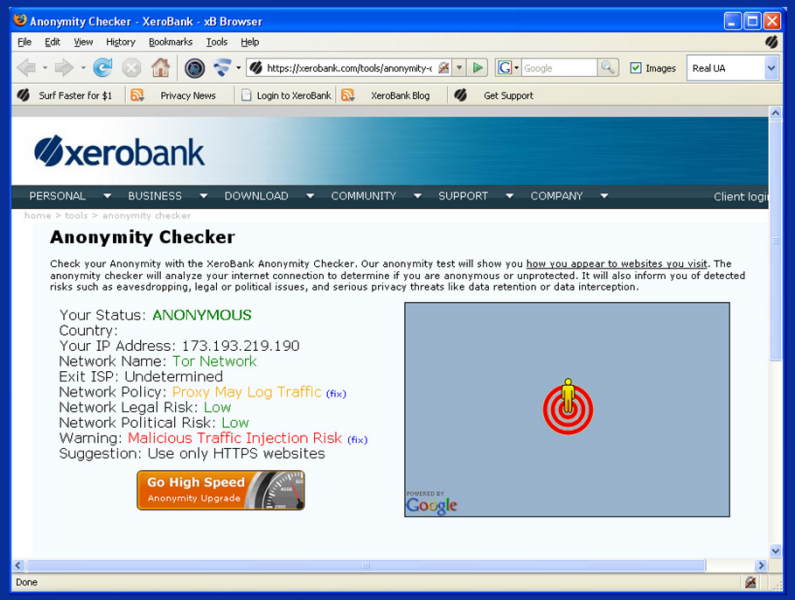


Anonymizer.com™

MixMaster: Anonymous E-Mail

- Cloud of dedicated mail-forwarders
- Cyrptographic protocol with multiple layers of encryption
- Mail-forwarding in mixed batches
- MIX-principle (D. Chaum)

Unobservable Webbrowsing

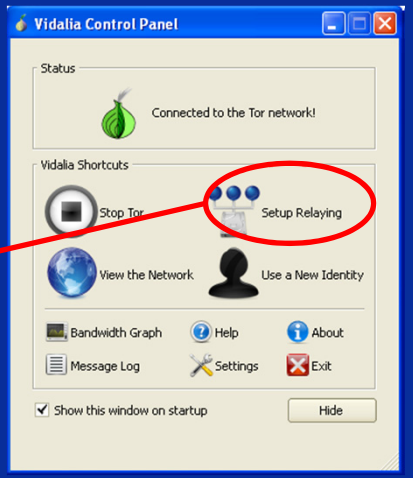


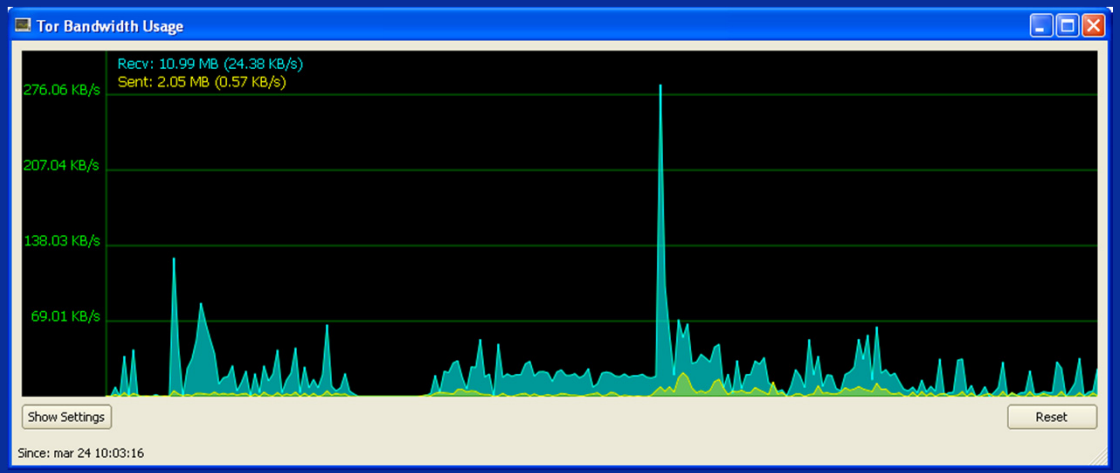
- MIX principle implemented for websurfing and web-based applications
- ANON and TOR networks operative with crypto protocols and extensive router networks
- User-friendly browser ”XeroBank” based on Firefox

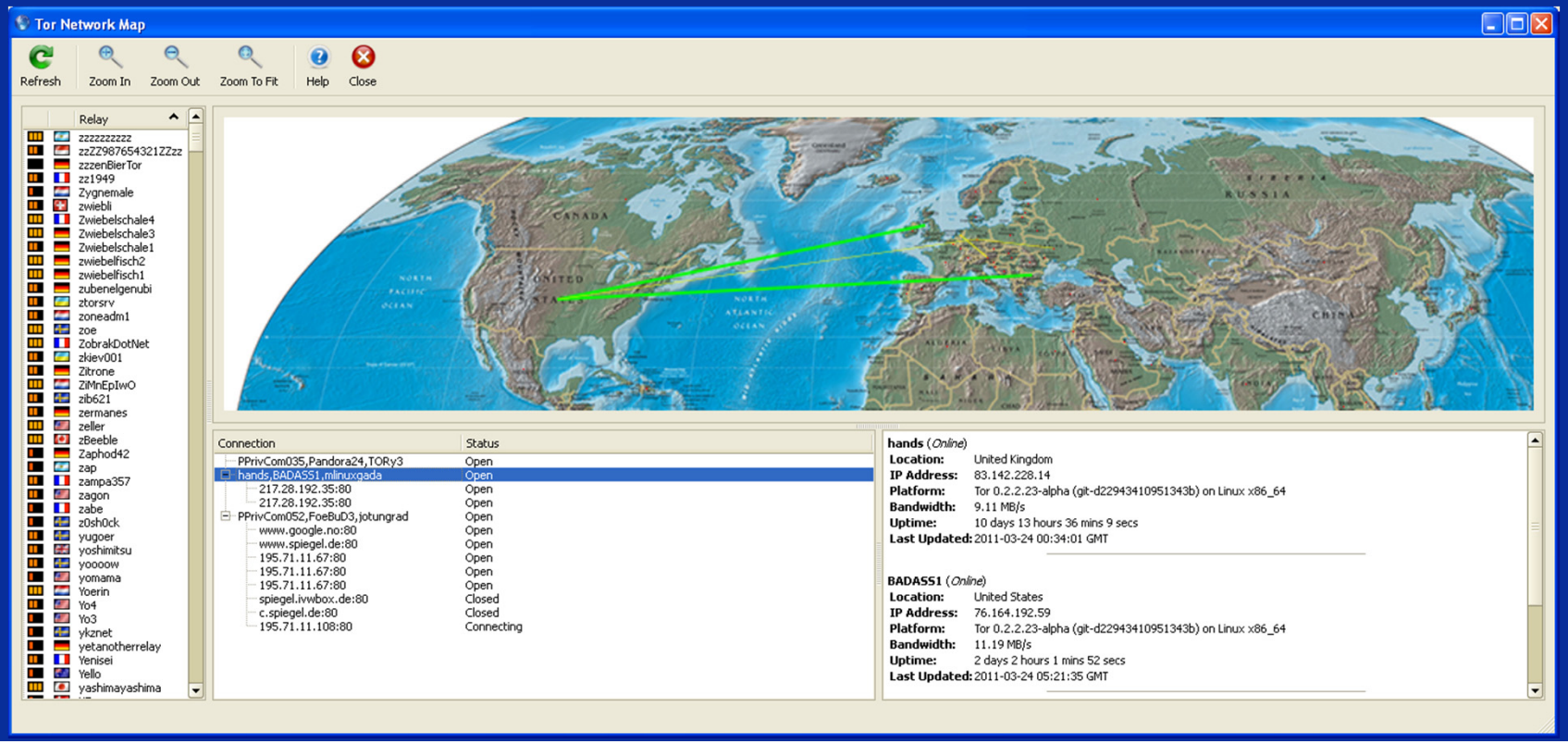
TOR Vidalia Bundle 0.2.10 (Win XP)

www.nr.no

Peer to Peer







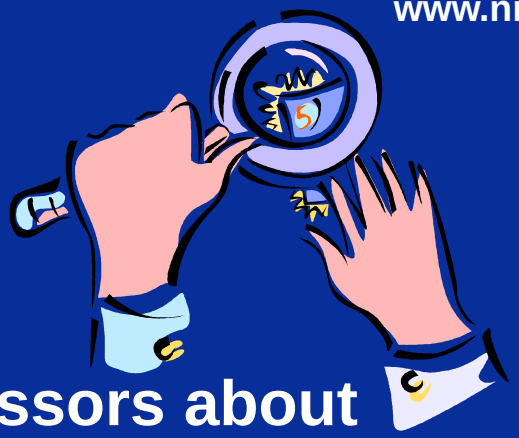
Browser cookie manipulation

- Swaps and manages cookies
- Random cookie exchange with other users
- Goal:
  - control sending and storage of own broser cookies
  - Attack user profiling websites through fake cookies or other people's cookies – creates entropy, destroys database value
- Configurable rulesets

Anonymous credential systems

- IDEMIX system invented by IBM research lab
  - provides zero-knowledge proofs and other cryptographic mechanisms that can assert ID information without showing it
  - Part of Eclipse/Higgings environment
- Microsoft U-PROVE-IT – build into Vista
  - Available funcitonality for anonymous credentials and secure, ID-protected remote attestation (demo release 2 on 18.2.2011)
- Based on advanced multi-party zero-knowledge cryptography and specialized Brands' signatures.

Transparency Tools



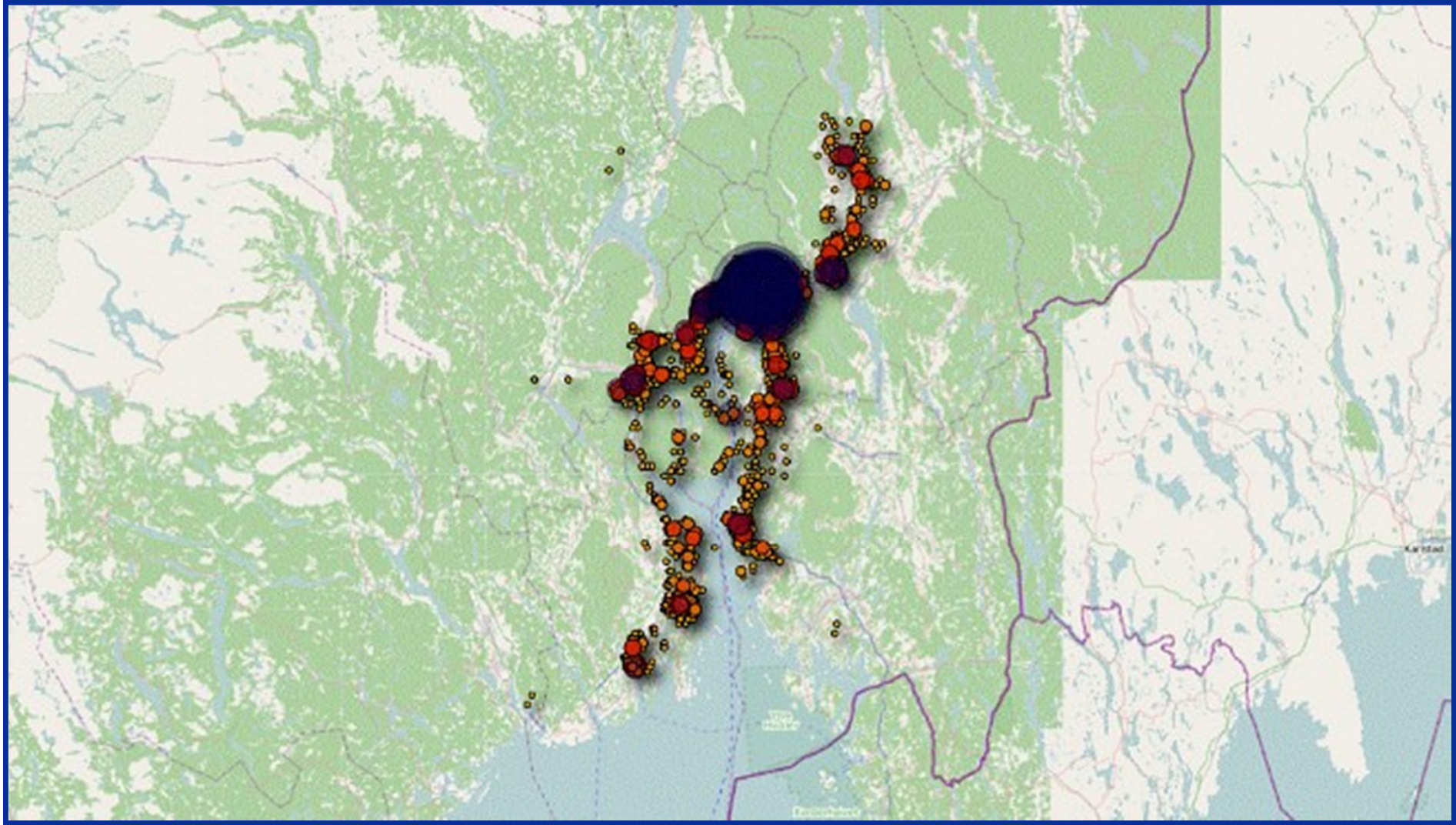
- Help to inform user & data processors about what is to be done with personal data.
  Example: P3P, X.509 signature policy
- Advanced systems from research:
  - «Sticky Policies» travel with the data to enfore correct processing (EU FP7 ICT PRIME Project)
  - «Obligations» are managed at processors to ensure correct long-time handling according to the promised policy & given consent (EU FP7 ICT PrimeLife Project)

Is privacy different from security?

- Privacy protection uses most known security methods to build protocols.
- The goals of privacy, however, are more than integrity, confidentiality, availability and non-repudiation:
  - Unobservability
  - Unlikability
  - Unidentifiability
  - Anonymity

Pfitzmann, Andreas und Hansen, Marit: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management – A Consolidated Proposal for Terminology

Apps & location

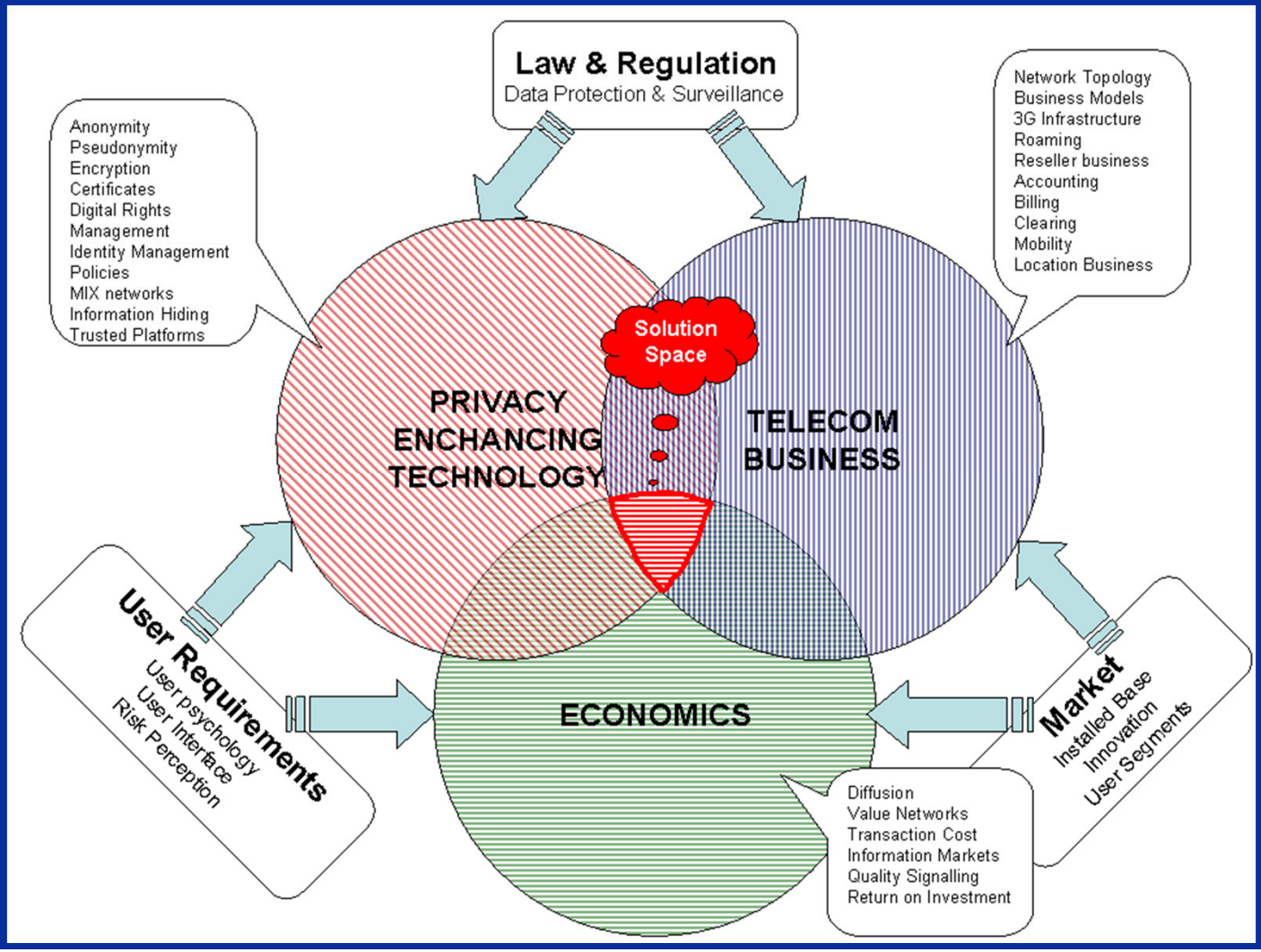


Source: NRK

Privacy for mobile location services

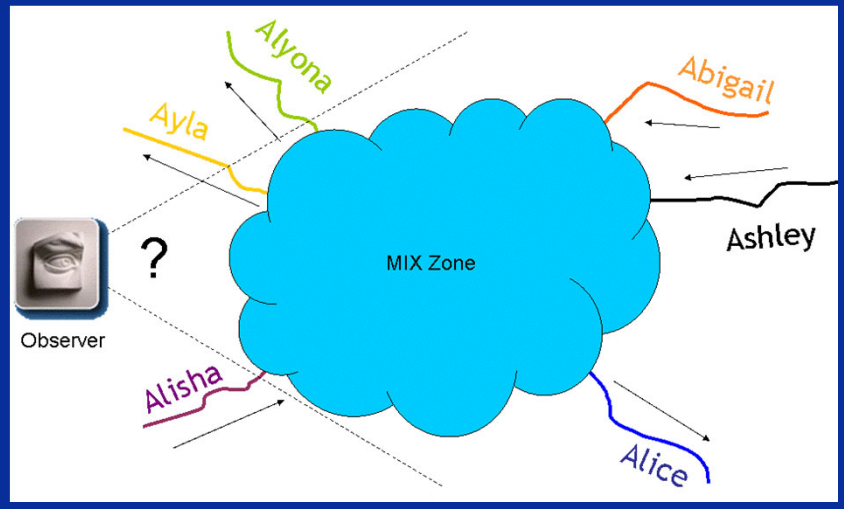
- Imagine: A mobile phone app following its users, gathering their positions for service provisioning and sharing.
- Challenge: Comply with data protection legislation.
- Issues:
  - Who is the data controller?
  - Has the user been informed?
  - What did the user give consent to?
  - How can policies be set differently for different sercvice providers?

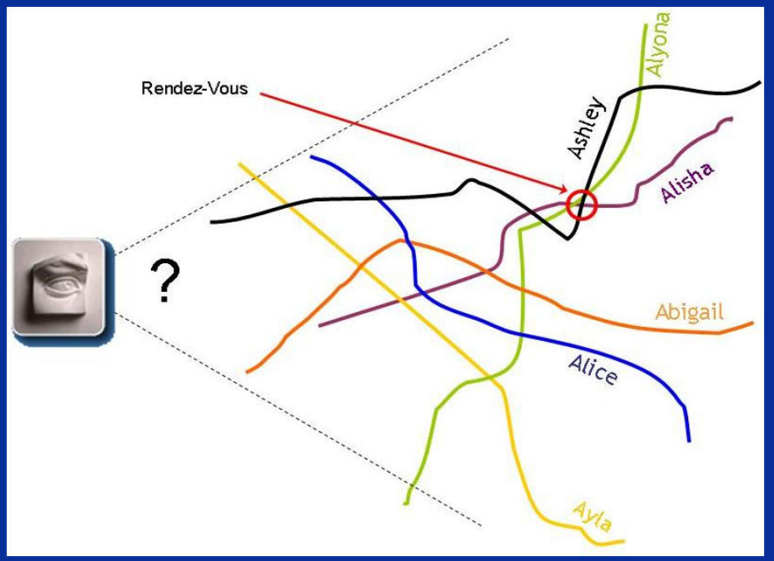
Mobile location apps: Stakeholders



Location privacy

- Implementation using Privacy-enhancing Technology (PET) and privacy-enhancing identity management (IDM)
- Definition of access control policies & enforcement
- Location Mixing





Fritsch, Lothar (2008) Profiling and Location-Based Services, in: M. Hildebrandt und S. Gutwirth (Eds.): *Profiling the European Citizen - Cross-Disciplinary Perspectives,* April 2008, Dordrecht, Springer Netherlands, pp. 147-160

Requirements

- The mobile network acts as a data controller against location service providers.
- Revocable policies and consent for each of the service providers set by the users.
- Unlinkability of service use between the service providers.
- Pseudonymity of user against service providers
- Billing against mobile phone possible.

T-Mobile prototype

www.nr.no

policy negotiation, consent
personal settings, payment
notification

LBS Server

L
LBS_S
IDM

sub-profile, payment
matching result

LBS Client

U
LBS_C
IDM

policy negotiation
consent

I
LM
IDM

Location Matcher

request location, payment
location of U

T-Mobile

O
LS
IDM

Location Source

policy negotiation
consent

Identity Management System

PRIME
Privacy and Identity Management for Europe

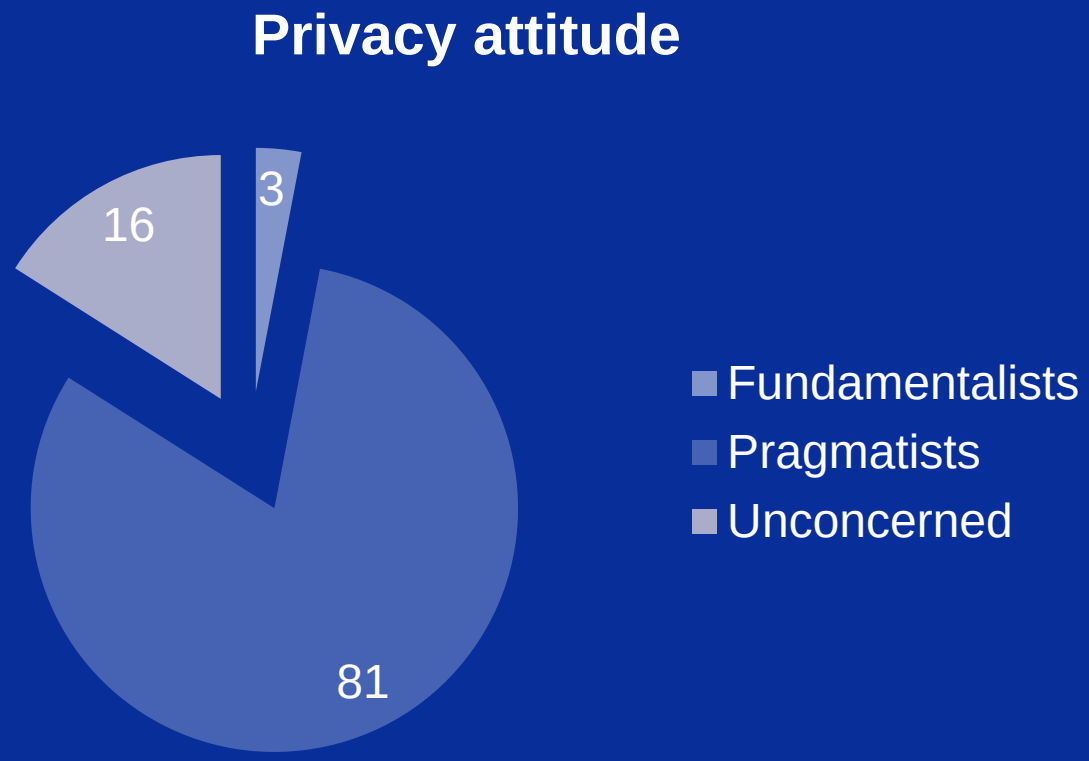
(Jan Camenisch, Lothar Fritsch, Markulf Kohlweiss, Mike Radmacher, and Dieter Sommer:
LBS Application Prototype, "Requirements and Concepts", PRIME internal presentation, 2005)

Where are the PETs, then?

- Do YOU use anonzmiyers like TOR?
- Have you ever registered with a fake or one-time e-mail address?
- Did you ever enter fake data in registration forms?

Where are all the PETs?

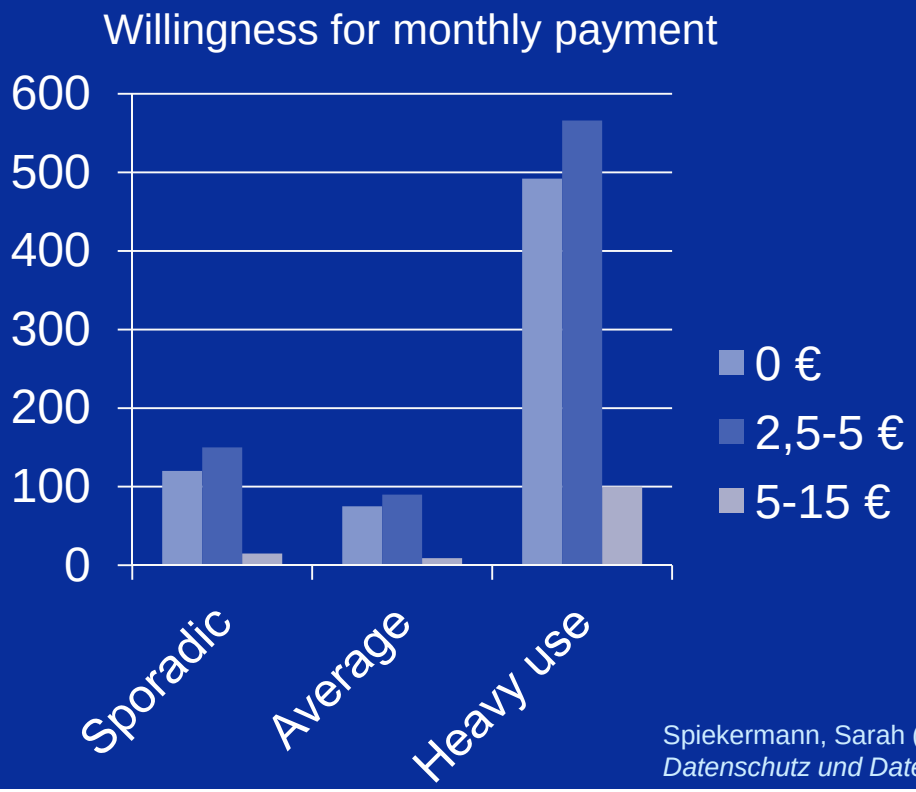
- In surveys, less than ~6-8% of Internet users state that they are always concerned about privacy.

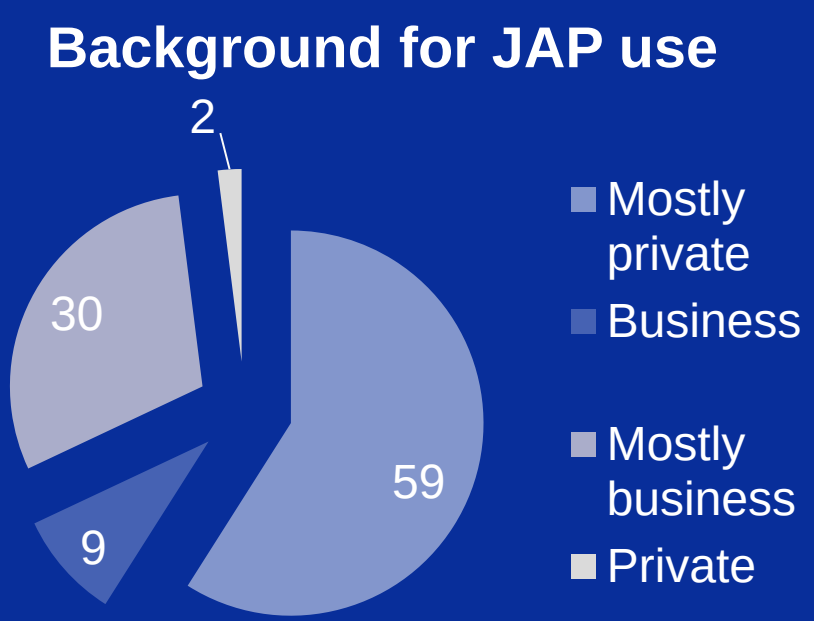


Sheehan, Kim (2002) Toward a Typology of Internet Users and Online Privacy Concerns, *The Information Society* (18:1), pp. 21-32.

Would you pay for your PETs?

- **The willingness of consumers depends on the use case, and on the perceived risks.**
  Users of the JAP anonymization service generally have a higher willingness to pay that others. However, private use dominates.

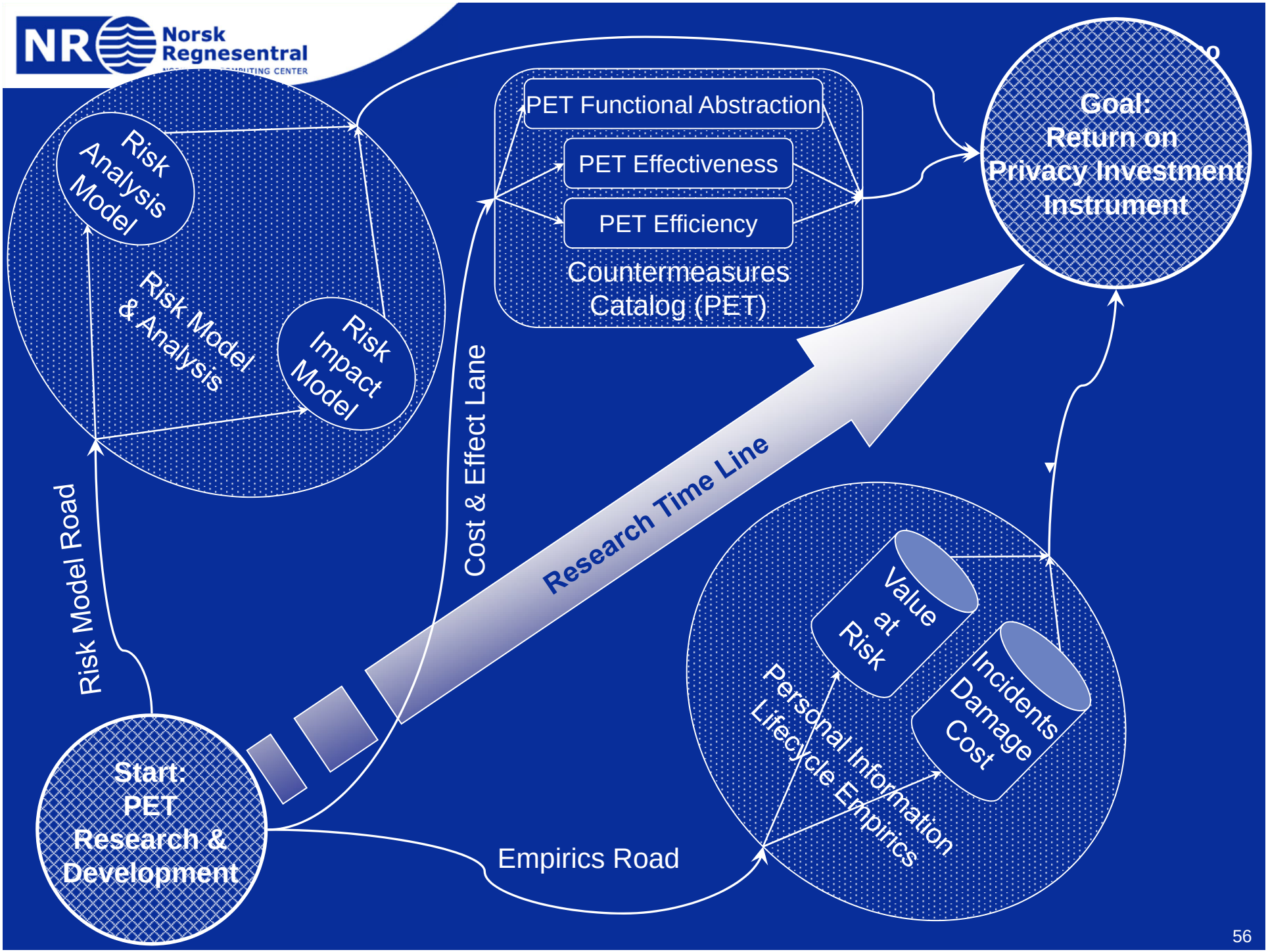




Spiekermann, Sarah (2003) Die Konsumenten der Anonymität, : Wer nutzt Anonymisierungsdienste?" *Datenschutz und Datensicherheit (DuD)* (27:3), pp. 150-154.

Showstoppers (or… Areas to use Research Budgets on)

- Lack of quantified data (cost & occurence of incidents, effectivity & cost of PET)
- Lack of a long-term privacy risk model (duality!)
- Lack of effectiveness studies on procedures, esp. on the end user side (usability, effectivity)
- Much ”expert guessing” necessary
  - Good for expert’s hourly rates
  - Bad for scientific accuracy
- Good for scientists’ careers:
  - More research and experimantation necessary
  - More research funding?


Norsk Regnesentral
Risk Analysis Model
Risk Model & Analysis
Risk Impact Model
PET Functional Abstraction
PET Effectiveness
PET Efficiency
Countermeasures Catalog (PET)
Goal: Return on Privacy Investment Instrument
Cost & Effect Lane
Research Time Line
Risk Model Road
Value at Risk
Incidents Damage Cost
Personal Information Lifecycle Empirics
Start: PET Research & Development
Empirics Road