Technology and Methods for Information Privacy

Dr. Lothar Fritsch

Norsk Regnesentral
Norwegian Computing Center

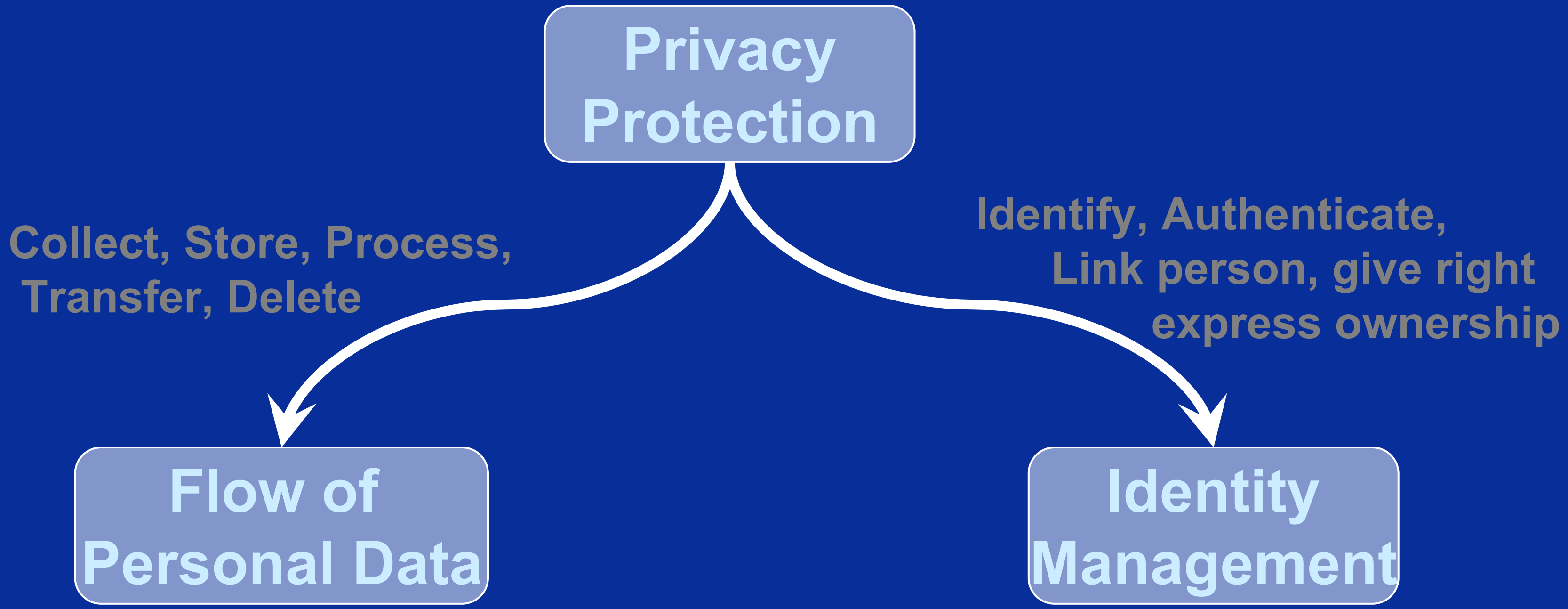
Oslo

ID-tyveri conference, 11-Oct-2010

Contents

- Information Privacy
  - Concept
  - Legal background
  - User perspective
- Privacy enhancing techology (PET)
  - History
  - Relevance
  - Examples
- Identity management & privacy

Privacy Protection in IT



Privacy Protection

Collect, Store, Process, Transfer, Delete

Identify, Authenticate, Link person, give right express ownership

Flow of Personal Data

Identity Management

Legal view: Fundamental Principles

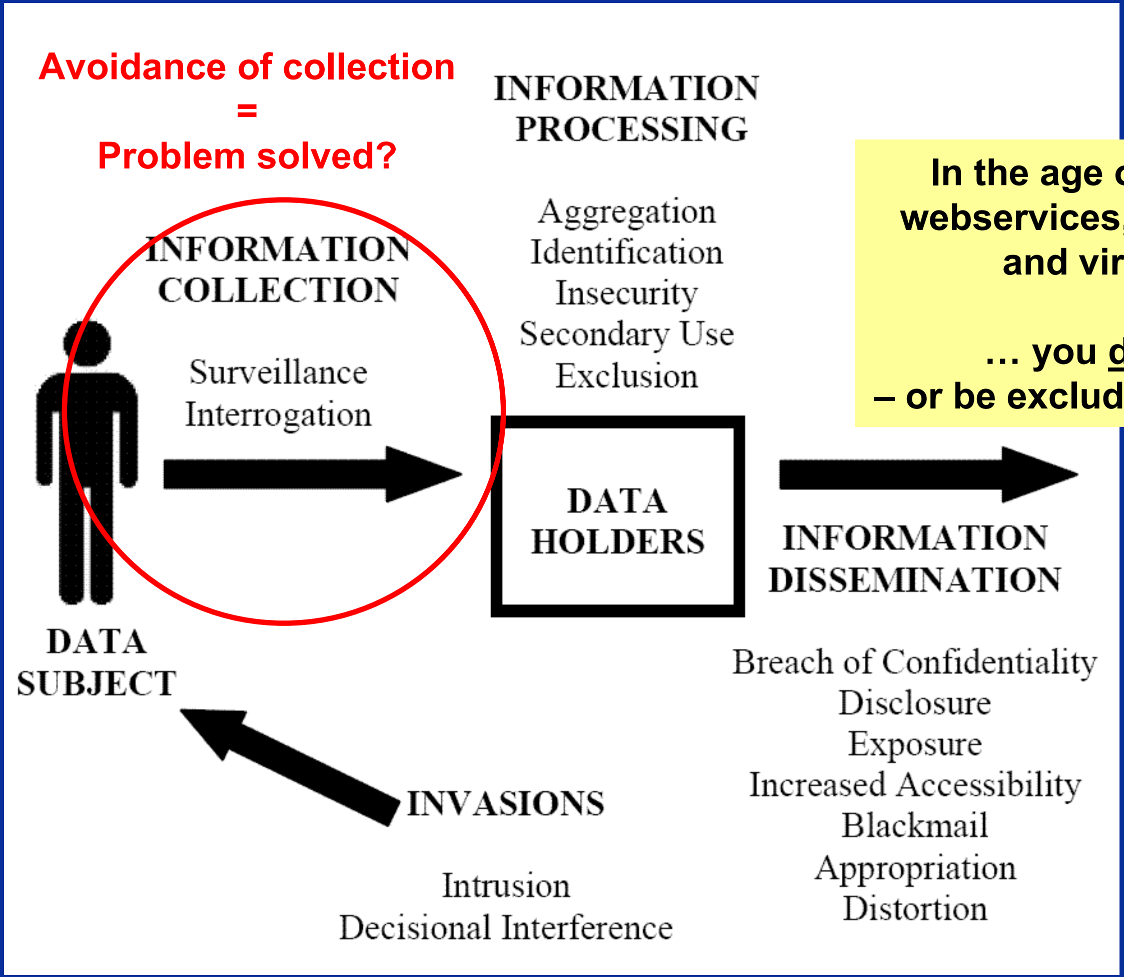
- Principles concerning the fundamental design of products and applications:
  - Data minimization, Transparency of processing, Security

- Principles concerning the lawfulness of processing:
  - Legality, Special categories of personal data,
  - Finality and purpose limitation, Data quality

- Rights of the data subject:
  - Information requirements, Access, correction, erasure, blocking, Objection to processing

- Data traffic with third countries
- Notification requirements
- Processing by a processor – responsibility and control
- Other specific requirements resulting from the Directive on Privacy and Electronic Communications 2002/58/EC/, Data Retention Directive 2006/24/EC and the national legislation.

Solove’s privacy threat taxonomy



Avoidance of collection
=
Problem solved?

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

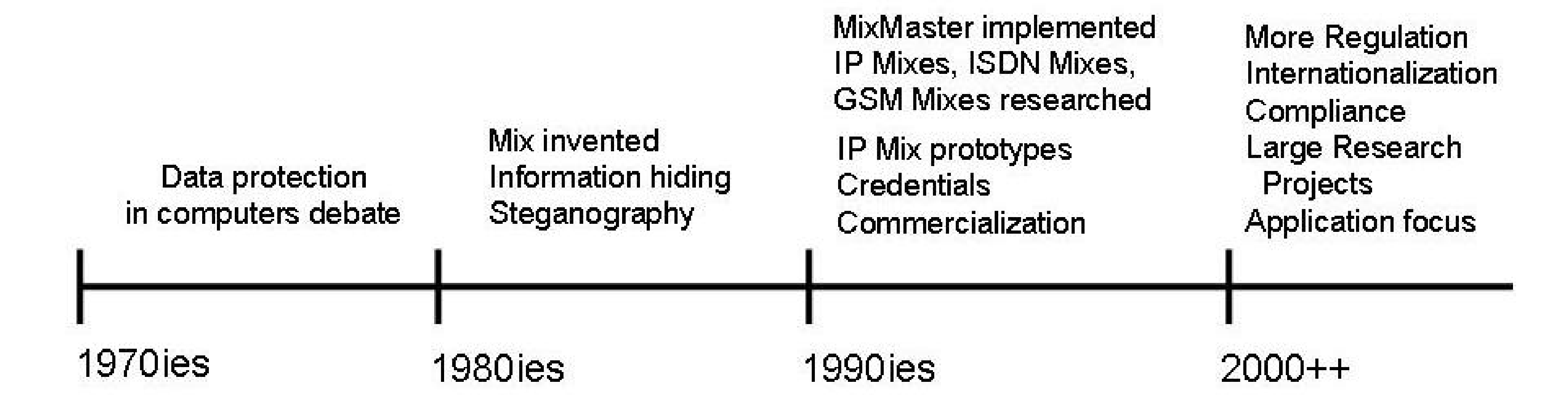
… you <u>do</u> provide data
– or be excluded from participation.

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

User perspective

- Users of on-line information systems feel invreasingly exposed to other parties' information processing
- Users express in surveys both:
  - Transparency on processing and data stored
  - Control and participation on dissemination and treatment of personal information
- Users do have a limited budget for active management of these issues
- There is a clear benefit in offering tool-based transparency and control concerning personal information processing

A brief history of PET



1970ies: Data protection in computers debate

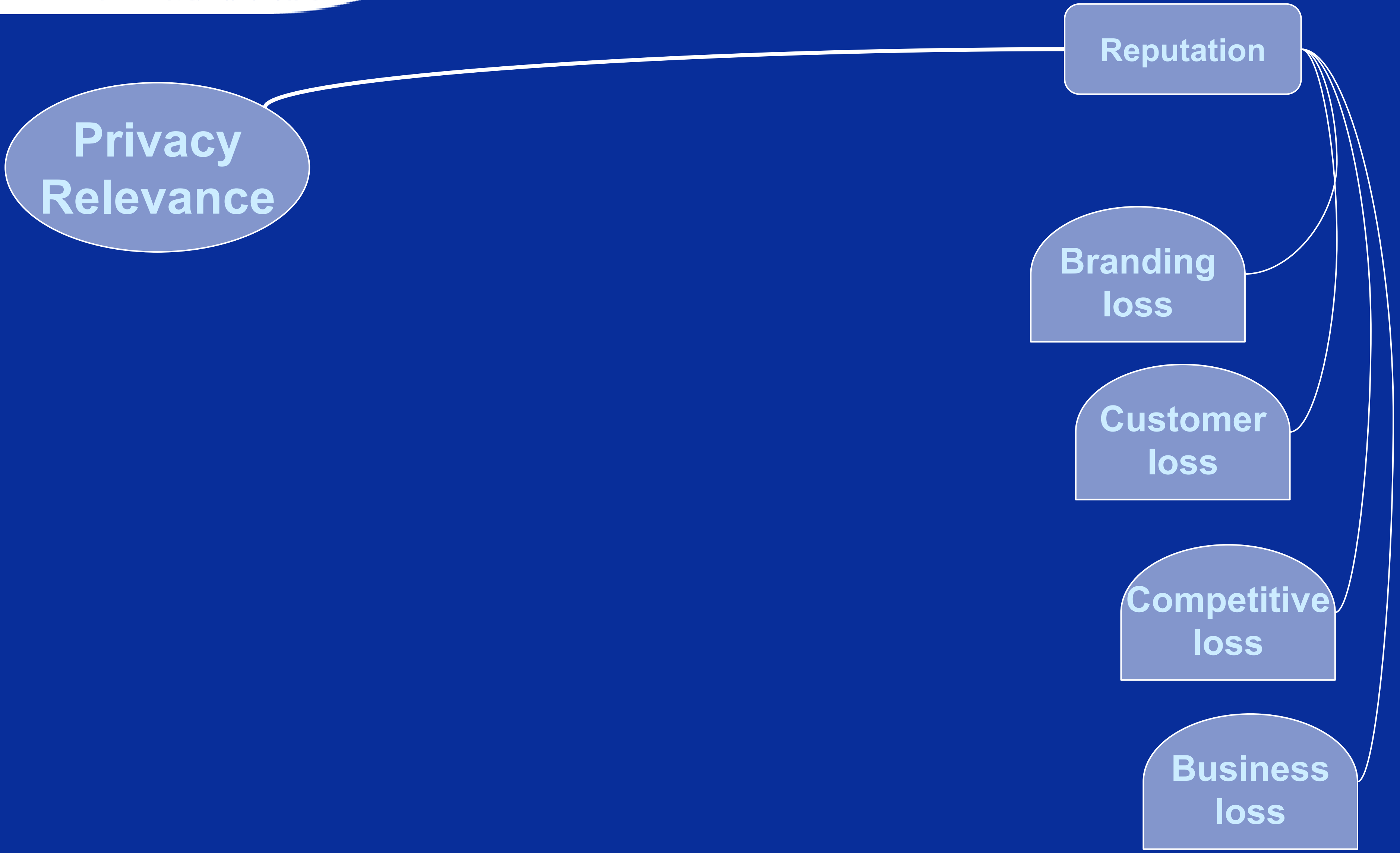
1980ies: Mix invented, Information hiding, Steganography

1990ies: MixMaster implemented, IP Mixes, ISDN Mixes, GSM Mixes researched; IP Mix prototypes, Credentials, Commercialization

2000++: More Regulation, Internationalization, Compliance, Large Research Projects, Application focus

- ► PET development inspired by the legal perspective on basic human rights.
- ► PET research focused on information hiding & control
- ► Technology-centric approach

But there is a lack of deployed PETs in the ”real world”. Why?



Privacy Relevance

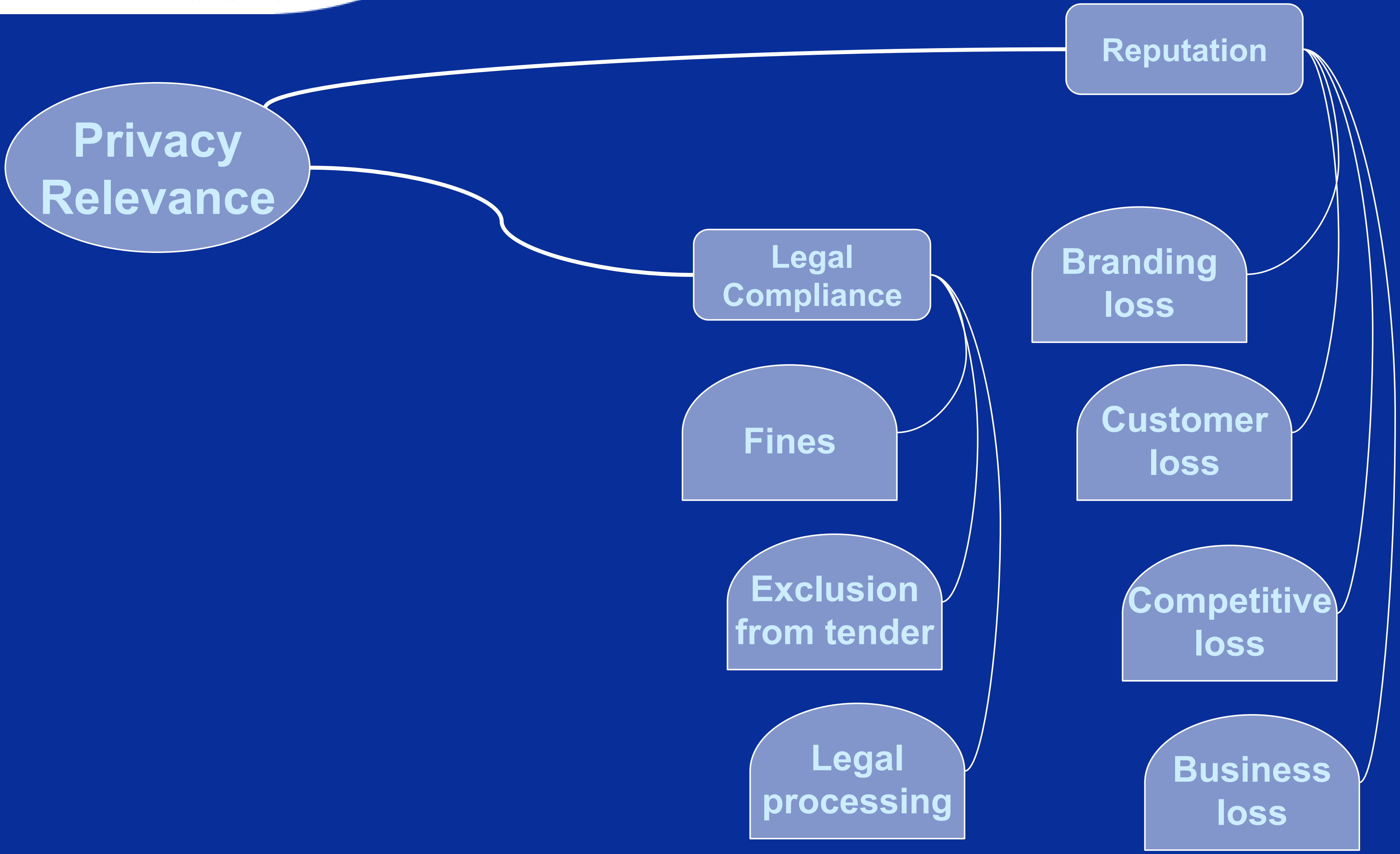
Reputation

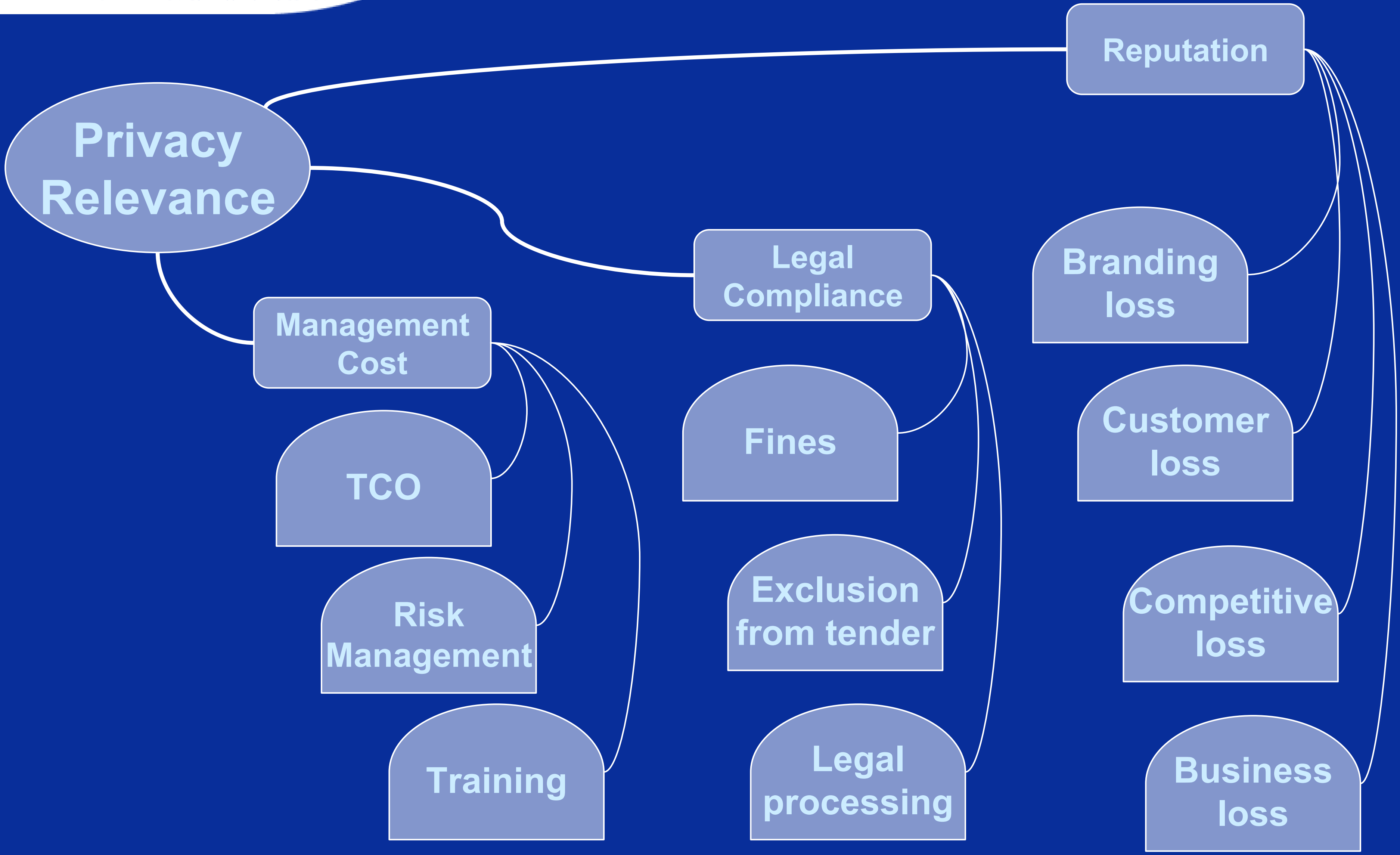
Branding loss

Customer loss

Competitive loss

Business loss


Privacy Relevance
Reputation
Legal Compliance
Branding loss
Fines
Customer loss
Exclusion from tender
Competitive loss
Legal processing
Business loss



Privacy Relevance

Reputation

Branding loss

Customer loss

Competitive loss

Business loss

Legal Compliance

Fines

Exclusion from tender

Legal processing

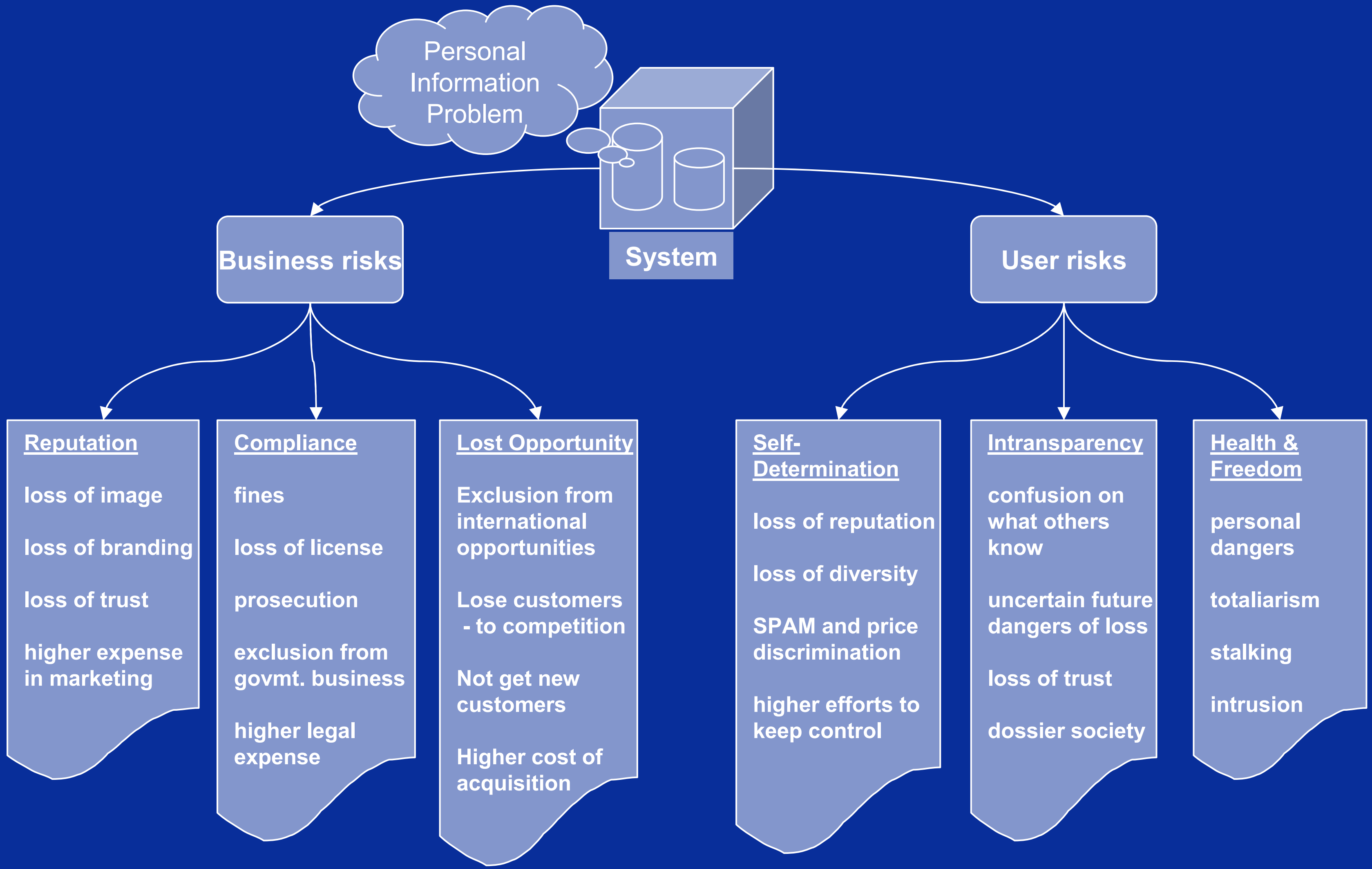
Management Cost

TCO

Risk Management

Training

Duality of Privacy Risks



Personal Information Problem

System

Business risks

Reputation

loss of image

loss of branding

loss of trust

higher expense in marketing

Compliance

fines

loss of license

prosecution

exclusion from govmt. business

higher legal expense

Lost Opportunity

Exclusion from international opportunities

Lose customers
 - to competition

Not get new customers

Higher cost of acquisition

User risks

Self-Determination

loss of reputation

loss of diversity

SPAM and price discrimination

higher efforts to keep control

Intransparency

confusion on what others know

uncertain future dangers of loss

loss of trust

dossier society

Health & Freedom

personal dangers

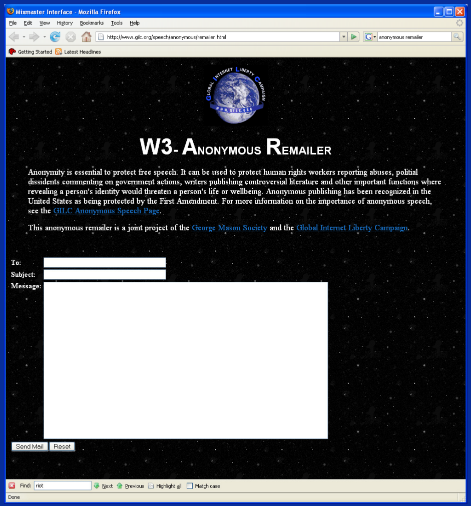
totaliarism

stalking

intrusion

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

Technology view: PETs



Mixmaster Interface - Mozilla Firefox

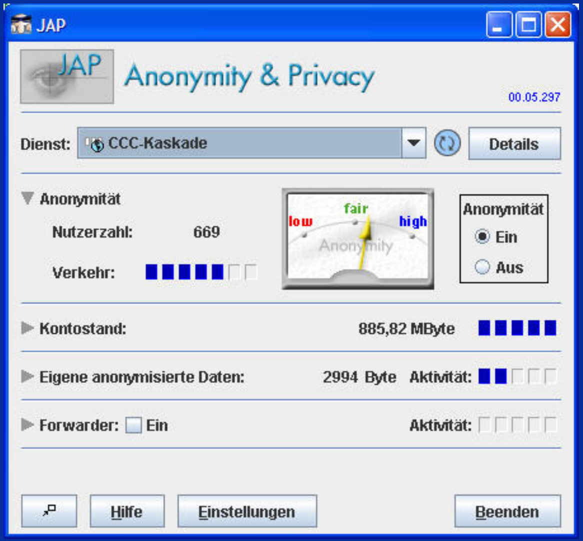
http://www.gilc.org/speech/anonymous/remailer.html

W3- Anonymous Remailer

Anonymity is essential to protect free speech. It can be used to protect human rights workers reporting abuses, politial dissidents commenting on government actions, writers publishing controversial literature and other important functions where revealing a person's identity would threaten a person's life or wellbeing. Anonymous publishing has been recognized in the United States as being protected by the First Amendment. For more information on the importance of anonymous speech, see the GILC Anonymous Speech Page.

This anonymous remailer is a joint project of the George Mason Society and the Global Internet Liberty Campaign.

To:
Subject:
Message:



JAP Anonymity & Privacy 00.05.297

Dienst: CCC-Kaskade

Anonymität
Nutzerzahl: 669
Verkehr:

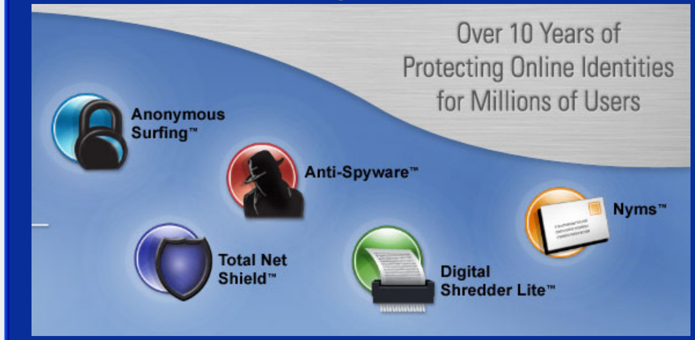
Anonymität
● Ein
○ Aus

Kontostand: 885,82 MByte

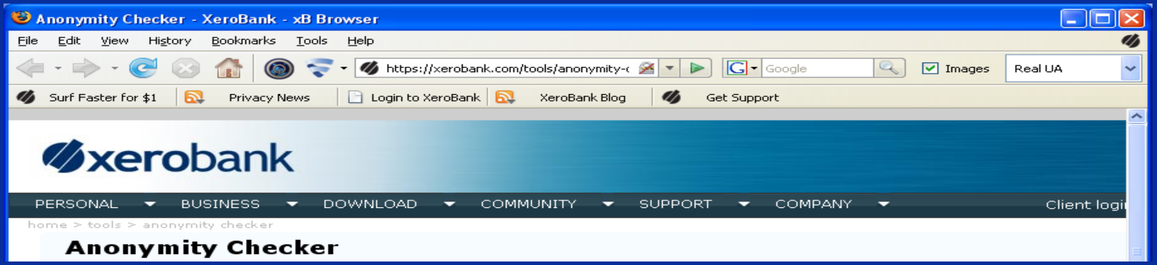
Eigene anonymisierte Daten: 2994 Byte Aktivität:

Forwarder: □ Ein Aktivität:

Anonymizer.com™



Over 10 Years of Protecting Online Identities for Millions of Users

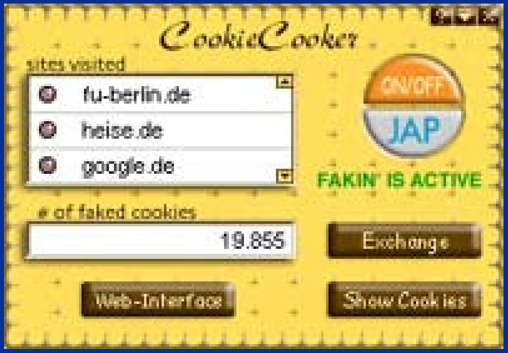


Anonymity Checker - XeroBank - xB Browser

https://xerobank.com/tools/anonymity-c

home > tools > anonymity checker

Anonymity Checker



CookieCooker

sites visited

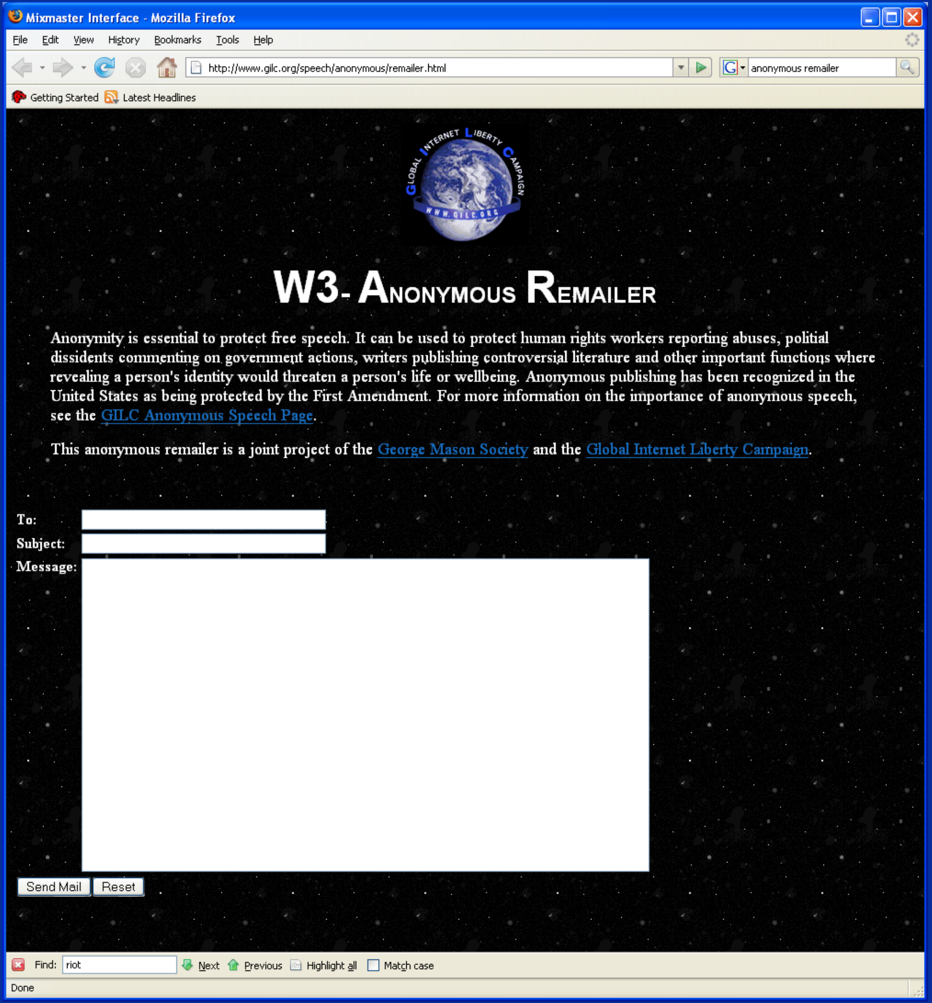
- fu-berlin.de
- heise.de
- google.de

# of faked cookies: 19.855

FAKIN' IS ACTIVE

Fritsch, Lothar: State of the Art of Privacy-enhancing Technology (PET) - Deliverable D2.1 of the PETweb project, Norsk Regnesentral Report 1013, ISBN 978-82-53-90523-5, Oslo, Norway, 2007

MixMaster: Anonymous E-Mail


Mixmaster Interface - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www.gilc.org/speech/anonymous/remailer.html
anonymous remailer
Getting Started Latest Headlines
Global Internet Liberty Campaign
WWW.GILC.ORG
Send Mail
Reset
Find: riot
Next Previous Highlight all Match case
Done

W3- Anonymous Remailer

Anonymity is essential to protect free speech. It can be used to protect human rights workers reporting abuses, politial dissidents commenting on government actions, writers publishing controversial literature and other important functions where revealing a person's identity would threaten a person's life or wellbeing. Anonymous publishing has been recognized in the United States as being protected by the First Amendment. For more information on the importance of anonymous speech, see the GILC Anonymous Speech Page.

This anonymous remailer is a joint project of the George Mason Society and the Global Internet Liberty Campaign.

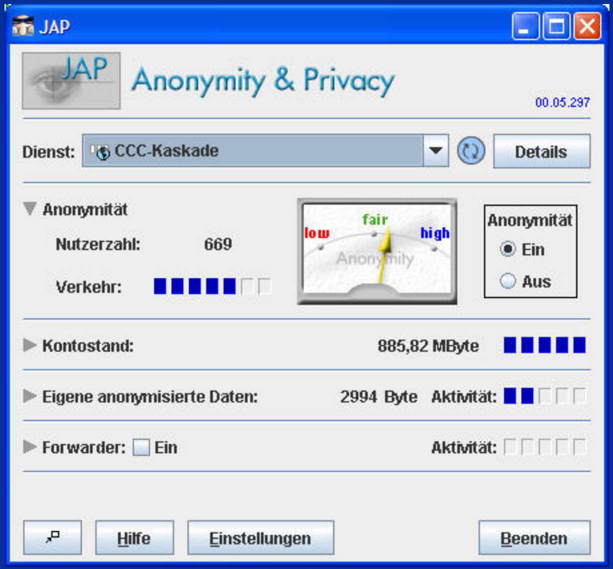
To:

Subject:

Message:

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

Unobservable Webbrowsing



Dienst: CCC-Kaskade

▼ Anonymität

Nutzerzahl: 669

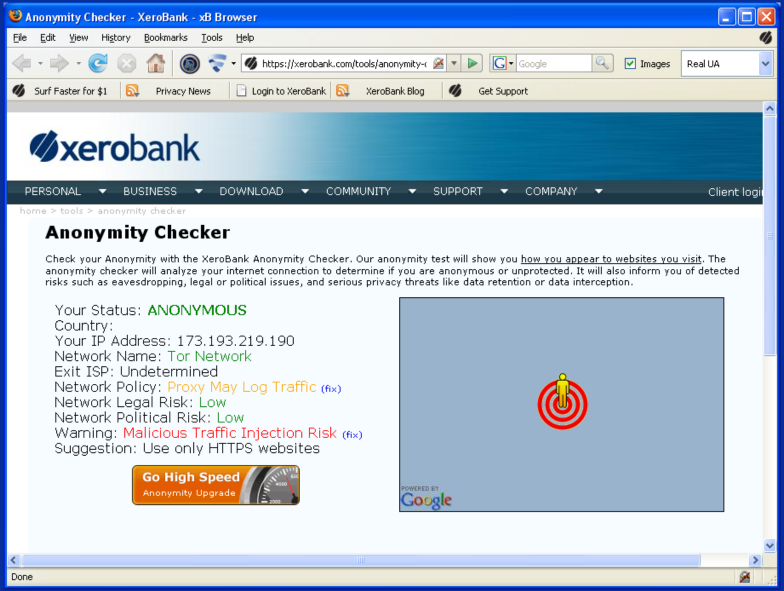
Verkehr: ■■■■■□□

Anonymität ● Ein ○ Aus

▶ Kontostand: 885,82 MByte ■■■■■

▶ Eigene anonymisierte Daten: 2994 Byte Aktivität: ■■□□□

▶ Forwarder: □ Ein Aktivität: □□□□□



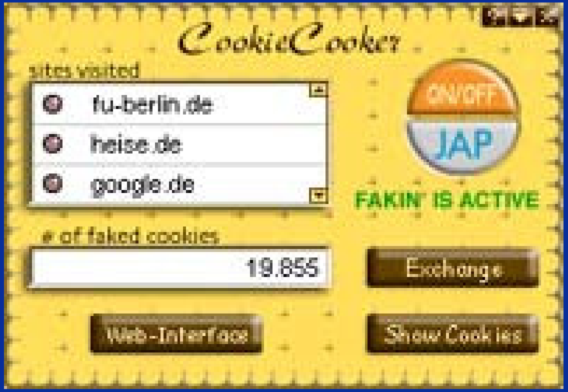
Anonymity Checker

Check your Anonymity with the XeroBank Anonymity Checker. Our anonymity test will show you how you appear to websites you visit. The anonymity checker will analyze your internet connection to determine if you are anonymous or unprotected. It will also inform you of detected risks such as eavesdropping, legal or political issues, and serious privacy threats like data retention or data interception.

Your Status: ANONYMOUS
Country:
Your IP Address: 173.193.219.190
Network Name: Tor Network
Exit ISP: Undetermined
Network Policy: Proxy May Log Traffic (fix)
Network Legal Risk: Low
Network Political Risk: Low
Warning: Malicious Traffic Injection Risk (fix)
Suggestion: Use only HTTPS websites

- 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

Browser cookie manipulation



CookieCooker

sites visited
- fu-berlin.de
- heise.de
- google.de

# of faked cookies: 19.855

- Swaps and manages cookies
- Random cookie exchange with other users
- Goal:
  - control sending and storage of own broser cookies
  - Attack server profiling databases by sending fake cookies or other people’s cookies
- Configurable rulesets

Anonymous credential systems

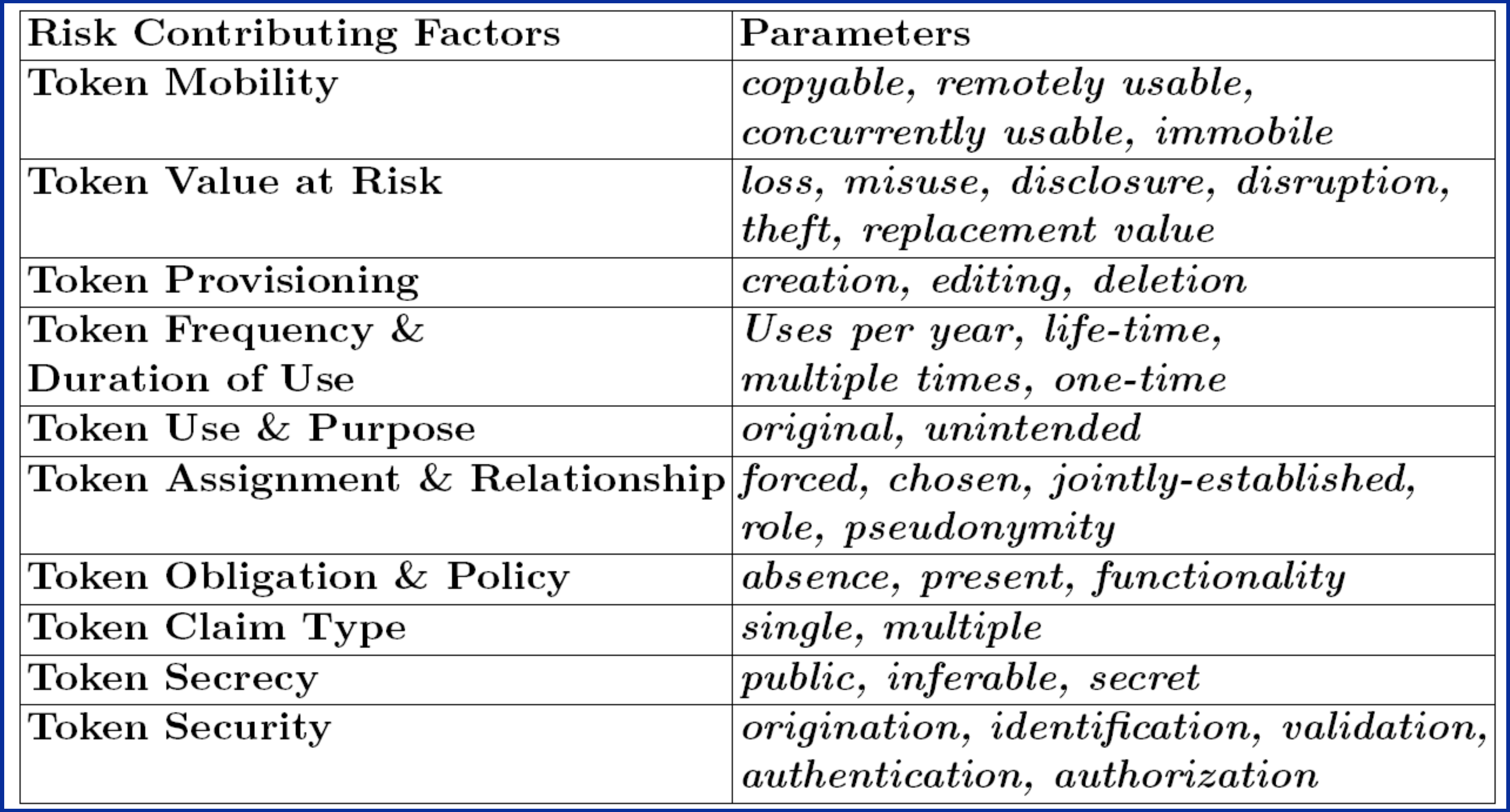
- IDEMIX system invented by IBM research lab
  - provides zero-knowledge proofs and other cryptographic mechanisms that can assert ID information without showing it
  - Part of Eclipse/Higgings environment

- Microsoft UPROVEIT – build into Vista
  - Available funcitonality for anonymous credentials and secure, ID-protected remote attestation

Identity Management & Privacy

- Choice of an IDM scheme has implications for privacy
- Sudden change in IDM or application strategy can cause side effects for privacy and security (e.g. ID theft)
- IDM scheme should be part of risk analysis and privacy impact analysis cycles

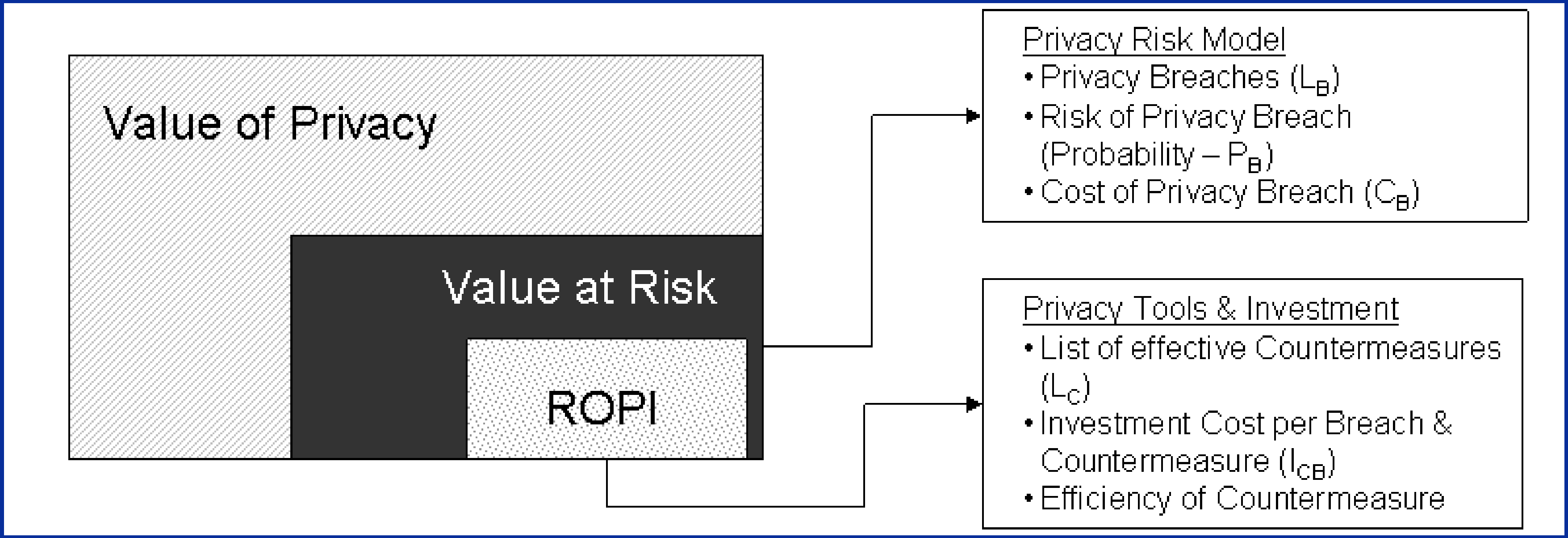
Risks created by IDM systems



Risk Contributing Factors	Parameters
Token Mobility	*copyable, remotely usable, concurrently usable, immobile*
Token Value at Risk	*loss, misuse, disclosure, disruption, theft, replacement value*
Token Provisioning	*creation, editing, deletion*
Token Frequency & Duration of Use	*Uses per year, life-time, multiple times, one-time*
Token Use & Purpose	*original, unintended*
Token Assignment & Relationship	*forced, chosen, jointly-established, role, pseudonymity*
Token Obligation & Policy	*absence, present, functionality*
Token Claim Type	*single, multiple*
Token Secrecy	*public, inferable, secret*
Token Security	*origination, identification, validation, authentication, authorization*

Fritsch, Paintsil, IFIP Summer School 2010, results from the PETweb II project

Business view:
Return On Privacy Investment ROPI



Value of Privacy

Value at Risk

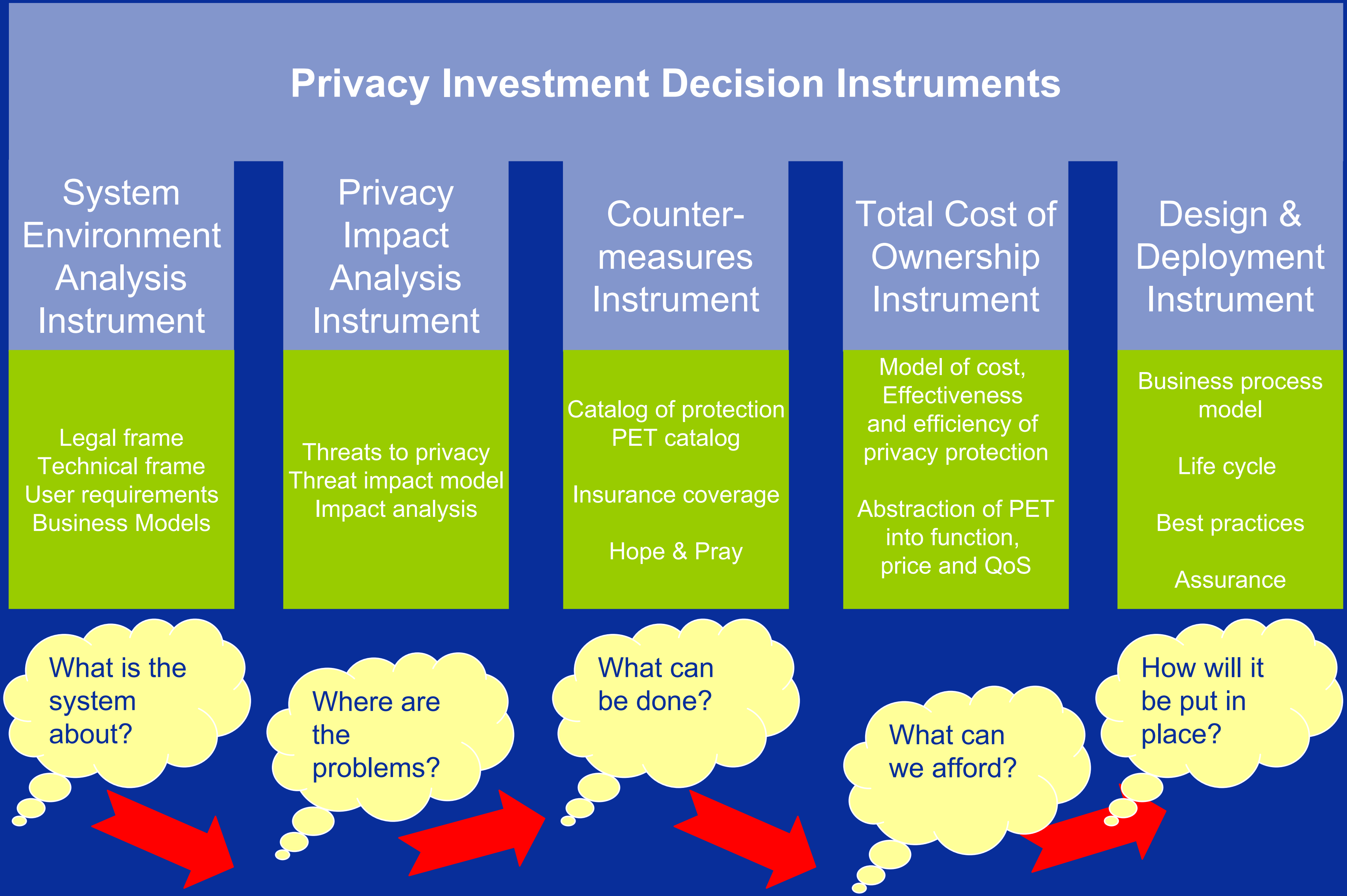
ROPI

Privacy Risk Model
- Privacy Breaches (L_B)
- Risk of Privacy Breach (Probability – P_B)
- Cost of Privacy Breach (C_B)

Privacy Tools & Investment
- List of effective Countermeasures (L_C)
- Investment Cost per Breach & Countermeasure (I_{CB})
- Efficiency of Countermeasure

Fritsch, Lothar und Abie, Habtamu. (2008) A Road Map to the Management of Privacy Risks in Information Systems, in: Gesellschaft f. Informatik (GI) (Eds.): *Konferenzband Sicherheit 2008, Lecture Notes in Informatics LNI 128,* 2-Apr-2007, Bonn, Gesellschaft für Informatik, pp. 1-15.

Privacy Investment Decision Instruments



System Environment Analysis Instrument

Legal frame
Technical frame
User requirements
Business Models

What is the system about?

Privacy Impact Analysis Instrument

Threats to privacy
Threat impact model
Impact analysis

Where are the problems?

Counter-measures Instrument

Catalog of protection
PET catalog

Insurance coverage

Hope & Pray

What can be done?

Total Cost of Ownership Instrument

Model of cost, Effectiveness and efficiency of privacy protection

Abstraction of PET into function, price and QoS

What can we afford?

Design & Deployment Instrument

Business process model

Life cycle

Best practices

Assurance

How will it be put in place?

Identity Management & ID theft

- identifiers can tell many stories.
- The most simple approach is a person number indexed in a data base.
  BUT: Who owns the data base, and how will it be protected from unauthorized use?
- IDM systems move some of the data to a token. But then, the token is out of the security perimeter of the vendor.
- The use of anonymizing schemes, cryptographic methods, randomized numbering schemes and zero-knowledge-protocols for identifier handling should be considered.
- Identifiers should be analyzed for information leakage and possible risks.

Access Control & Information Flow

- ► Multi-level and role-based access control models are used in server & mainframe computing for more than three decades.
- ► Security models implemented on a ”need to know” basis.
- ► But today’s e-ID approaches aim for maximum transparency, efficient identification, and global standardization.
- ► Information flow analysis and access control models are essential to protect e-IDs.

Checklist

- Are you aware of all contextual information that can be correlated to your e-IDs?
  - Use frequency & destinations
  - Person names & other personal data
  - predictable identifiers (e.g. serial number sequences)
- Countermeasures:
  - Identifier management
  - Encryption from token to application level
  - Use tags without individual numbers/names
  - One-time identifiers and anonymous credentials

Checklist

- Do your tokens contain interpretable information?
  - product keys
  - customer information
  - indications of object value
  - origin information
- Countermeasures:
  - Identifier management & pseudonyms
  - Encryption & Access control
  - Short lifetime of e-ID tokens

Checklist

- Are your identifiers person-relateable?
  - Equipment check-out
  - e-tickets
  - consumer items
  - ID cards, door cards, passports, bank cards
- Countermeasures
  - De-activation (including RFID chip serial number!)
  - Identity management
  - Privacy risk assessment & audits
  - Privacy-enhancing technology (PET)

Checklist

- Are your e-IDs securely bound to the legitimate user or person?
- Countermeasures
  - Multi-factor authentication
  - ”Biometrics” derived from the person (extra privacy challenges!)

Summary

- Privacy management is part of IT management
- Privacy-enhancing technology is available & should be part of IT plan
- Identity management should be part of the privacy concepts
- Some of the business implications are not well researched

IFIP IDMAN 2010

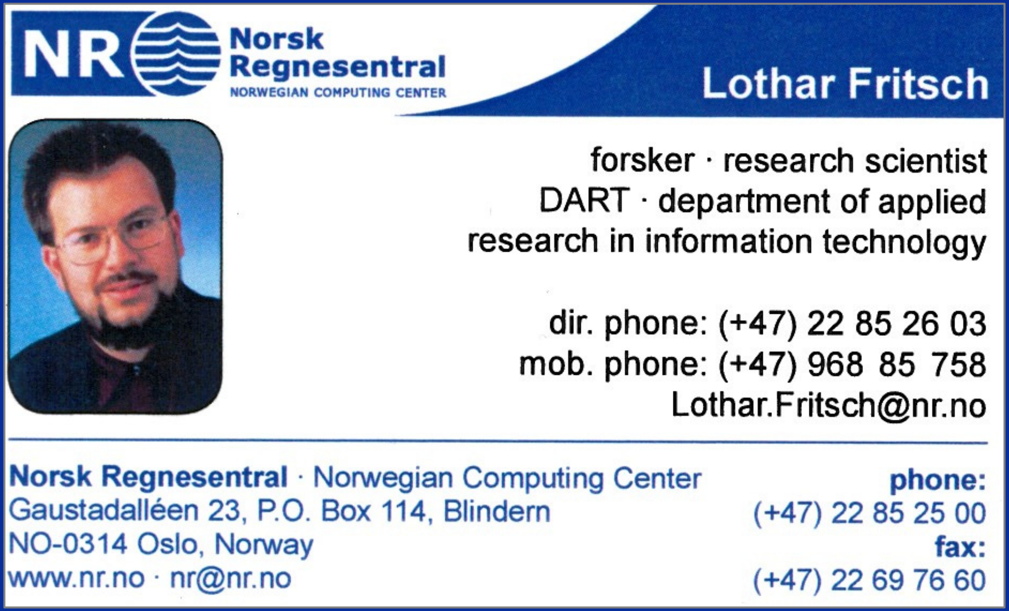
- International conference of IFIP TC 11.6
- Topic: *Identity Management and Society*
- Many international speakers
- Keynotes on e-voting security and identity management
- 18.-19. 11. 2010 in Oslo, Norway
- Program & registration under http://ifipidman2010.nr.no

What can Norsk Regnesentral provide?

- Scientific research & consulting in security concepts
- Evaluation of security systems, properties & privacy impact
- Preparation of IT certification or audit

- Industry- or publicly funded research
- Open or confidential cooperation

Contact



Norsk Regnesentral
NORWEGIAN COMPUTING CENTER

Lothar Fritsch

forsker · research scientist
DART · department of applied
research in information technology

dir. phone: (+47) 22 85 26 03
mob. phone: (+47) 968 85 758
Lothar.Fritsch@nr.no

Norsk Regnesentral · Norwegian Computing Center
Gaustadalléen 23, P.O. Box 114, Blindern
NO-0314 Oslo, Norway
www.nr.no · nr@nr.no

phone:
(+47) 22 85 25 00
fax:
(+47) 22 69 76 60