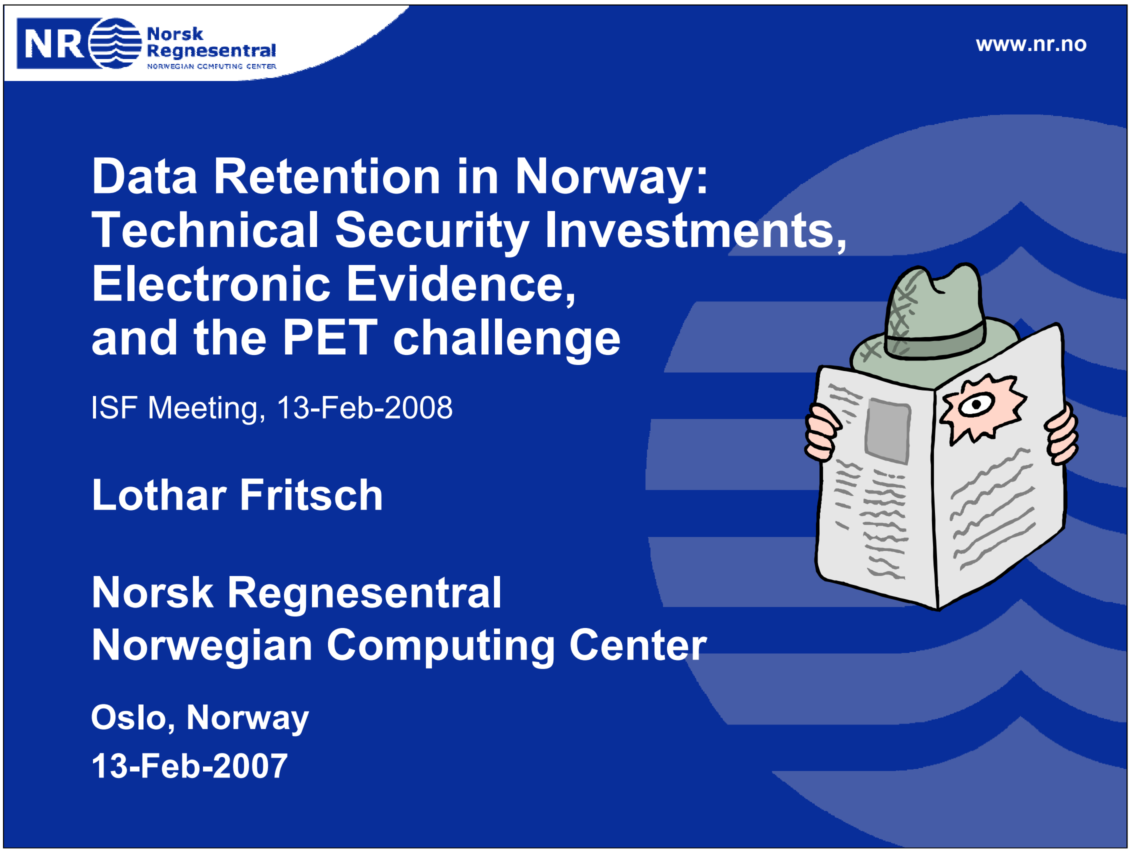


NR Norsk Regnesentral NORWEGIAN COMPUTING CENTER

www.nr.no

Data Retention in Norway: Technical Security Investments, Electronic Evidence, and the PET challenge

ISF Meeting, 13-Feb-2008

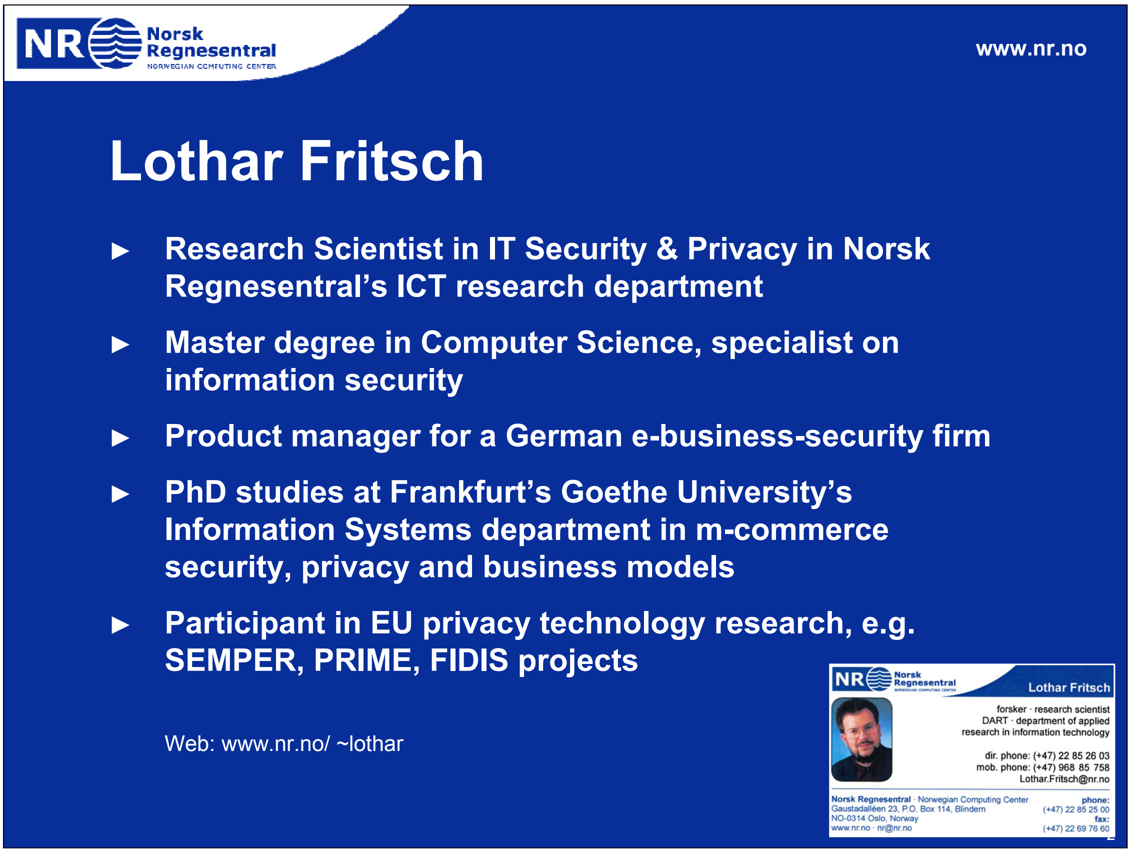
Lothar Fritsch

Norsk Regnesentral
Norwegian Computing Center

Oslo, Norway
13-Feb-2007

Norsk Regnesentral

Norsk Regnesentral (Norwegian Computing Center, NR) is a private, independent, non-profit foundation established in 1952. NR carries out contract research and development projects in the areas of information and communication technology and applied statistical modeling. The clients are a broad range of industrial, commercial and public service organizations in the national as well as the international market. Our scientific and technical capabilities are further developed in co-operation with The Research Council of Norway and key customers. The results of our projects may take the form of reports, software, prototypes, and short courses. A proof of the confidence and appreciation our clients have for us is given by the fact that most of our new contracts are signed with previous customers.



Norsk Regnesentral
NORWEGIAN COMPUTING CENTER

www.nr.no

Lothar Fritsch

- ► Research Scientist in IT Security & Privacy in Norsk Regnesentral’s ICT research department
- ► Master degree in Computer Science, specialist on information security
- ► Product manager for a German e-business-security firm
- ► PhD studies at Frankfurt’s Goethe University’s Information Systems department in m-commerce security, privacy and business models
- ► Participant in EU privacy technology research, e.g. SEMPER, PRIME, FIDIS projects

Web: www.nr.no/ ~lothar

Norsk Regnesentral
NORWEGIAN COMPUTING CENTER
Lothar Fritsch

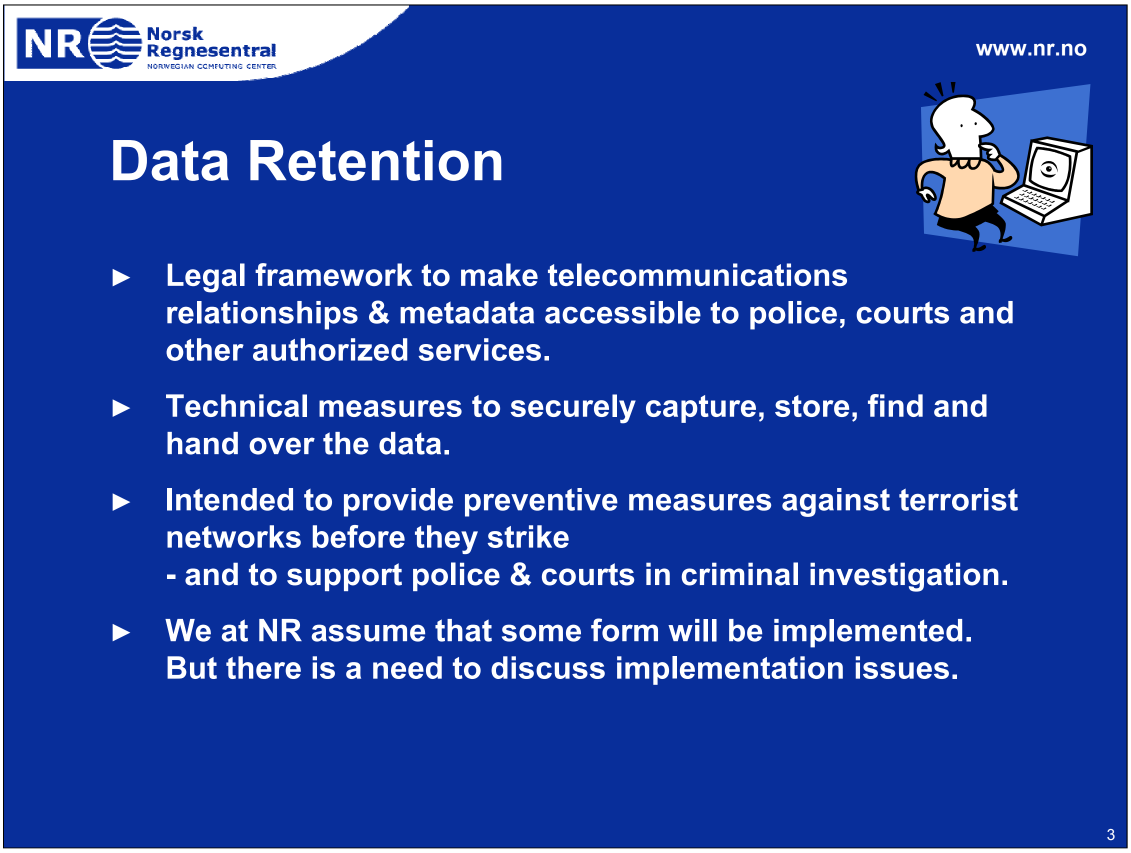
forsker · research scientist
DART · department of applied
research in information technology

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

Lothar Fritsch is a research scientist with Norsk Regnesentral. Lothars work focuses on the analysis of security and privacy requirements in upcoming application areas. Particularly he has experience on the deployment of privacy functionality and privacy-enhancing technology (PET) into new systems with respect to requirements engineering and verification. He used to work as a researcher at the T-Mobile Chair for Mobile Commerce & Multilateral Security at Frankfurt’s Johann Wolfgang Goethe – University in Germany from 2002-2007. Before this, he was employed as a product manager in IT security by fun communications GmbH, Karlsruhe, Germany where he was responsible for IT security product definitions in the areas of PKI, signature law application and secure e-payment, and additionally working on ITSEC security certification. He has received his diploma degree from the University of Saarland in Saarbrücken where he graduated with a specialization in computer security and cryptography.



Data Retention

- Legal framework to make telecommunications relationships & metadata accessible to police, courts and other authorized services.
- Technical measures to securely capture, store, find and hand over the data.
- Intended to provide preventive measures against terrorist networks before they strike
  - and to support police & courts in criminal investigation.
- We at NR assume that some form will be implemented. But there is a need to discuss implementation issues.

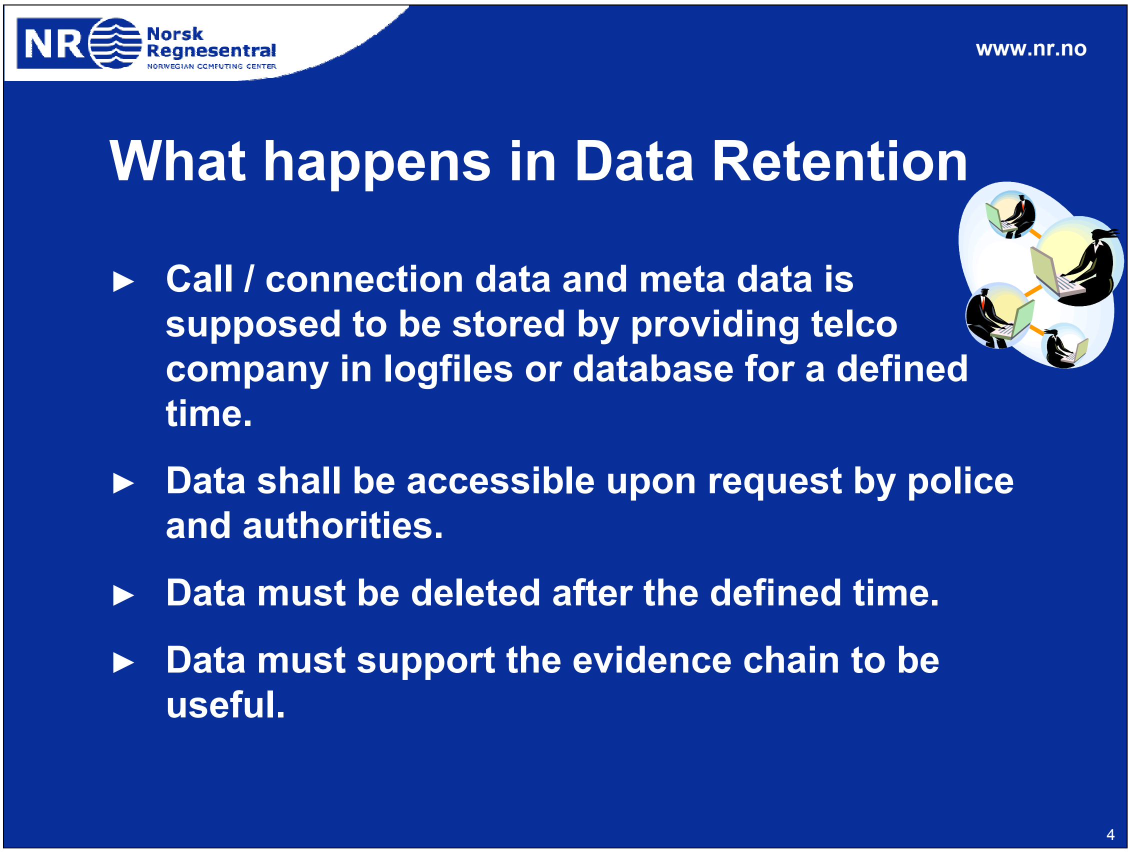
Data retention is a contemporary topic of political and scientific debate. For information security and privacy, the law initiative in Norway concerning data retention might be highly relevant for a number of reasons:

How is telecommunication secrecy and privacy guaranteed?

How is the collected data preserved as electronic evidence usable in courts?

Who is in charge of auditing and enforcing the security of data retention systems?

What are the conditions of changes in the retention data use policy?

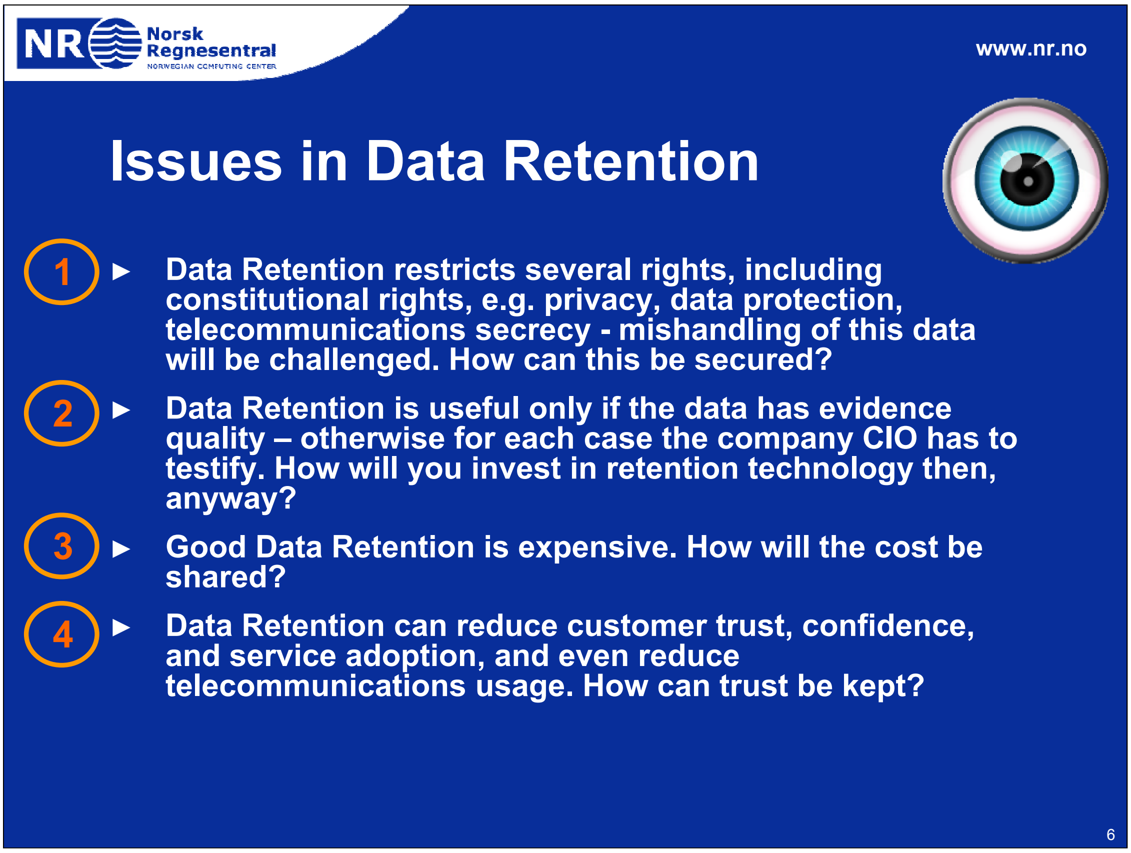


What happens in Data Retention

- ► Call / connection data and meta data is supposed to be stored by providing telco company in logfiles or database for a defined time.
- ► Data shall be accessible upon request by police and authorities.
- ► Data must be deleted after the defined time.
- ► Data must support the evidence chain to be useful.

Benefits of Data Retention

- ► Police can catch up with investigations after a crime has been committed using telecommunications.
- ► Evidence about communication events and relationships can be provided to court.
- ► Possibly, courts can work faster, more efficient, and provide better justice.
- ► Some people claim that terrorists can be caught before they strike. No one has proven this, though, as there is a too low number of successful cases.



NR Norsk Regnesentral NORWEGIAN COMPUTING CENTER

www.nr.no

Issues in Data Retention

1 ▶ Data Retention restricts several rights, including constitutional rights, e.g. privacy, data protection, telecommunications secrecy - mishandling of this data will be challenged. How can this be secured?

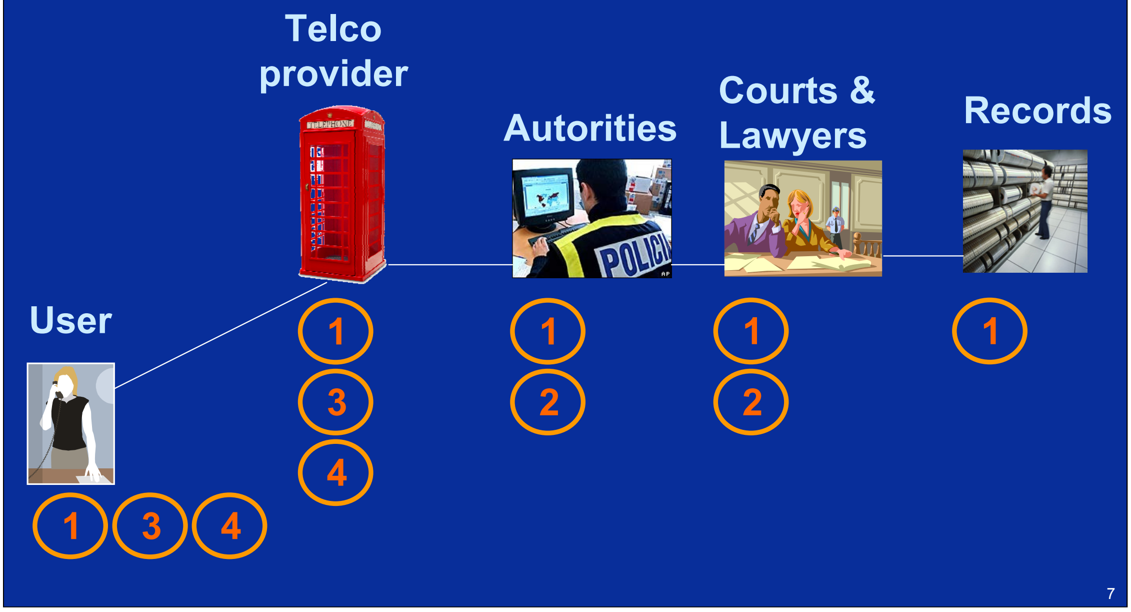
2 ▶ Data Retention is useful only if the data has evidence quality – otherwise for each case the company CIO has to testify. How will you invest in retention technology then, anyway?

3 ▶ Good Data Retention is expensive. How will the cost be shared?

4 ▶ Data Retention can reduce customer trust, confidence, and service adoption, and even reduce telecommunications usage. How can trust be kept?

Different storage strategies bring different risks and different cost. There is a need for risk & cost analysis.

Issues: Incident locations



Telco provider

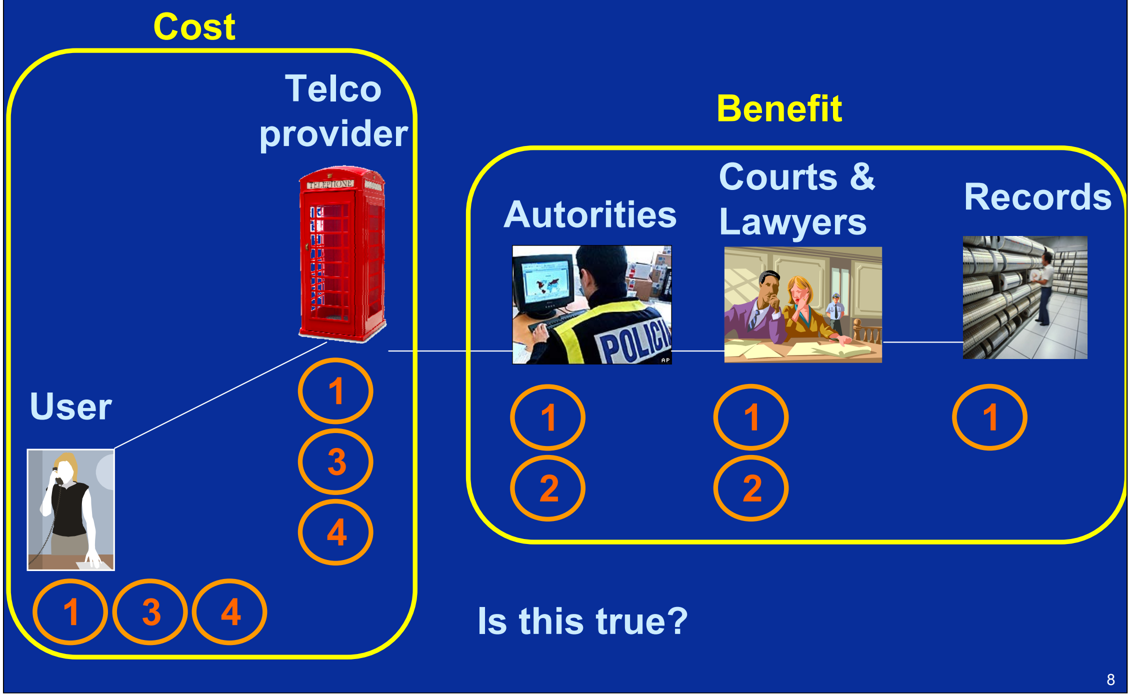
Autorities

Courts & Lawyers

Records

User

Issues: Cost Balance



Cost

Telco provider

1
3
4

User

1 3 4

Benefit

Autorities

1
2

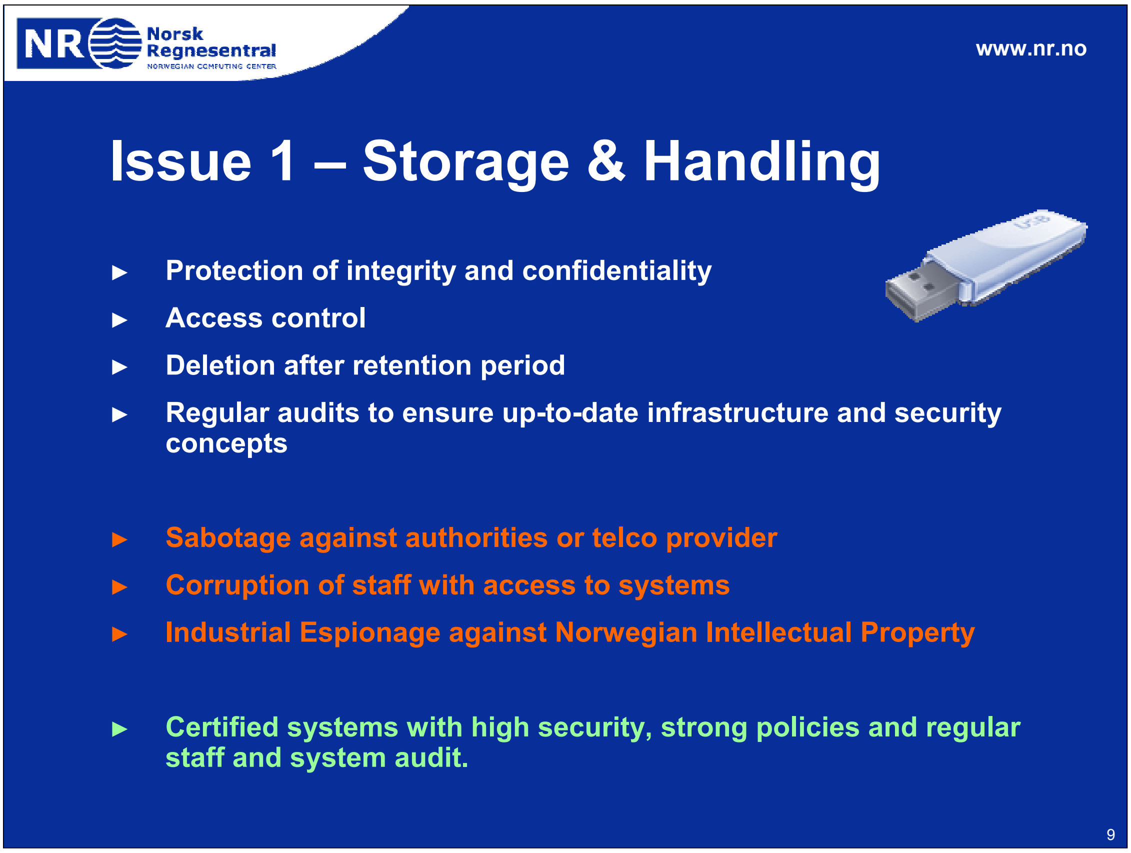
Courts & Lawyers

1
2

Records

1

Is this true?



Norsk Regnesentral
NORWEGIAN COMPUTING CENTER

www.nr.no

Issue 1 – Storage & Handling

- Protection of integrity and confidentiality
- Access control
- Deletion after retention period
- Regular audits to ensure up-to-date infrastructure and security concepts

- Sabotage against authorities or telco provider
- Corruption of staff with access to systems
- Industrial Espionage against Norwegian Intellectual Property

- Certified systems with high security, strong policies and regular staff and system audit.

9

Preservation of fundamental rights in spite of data retention

Data retention will preserve communication relationships, location information and some other data about the whole population and all commercial communications of Norway. Such a data collection contains vast amounts of private data and business secrets unrelated to any crimes. This collection of data might invite large amounts of abuse if the data is available for easy access, resulting in a number of problems such as:

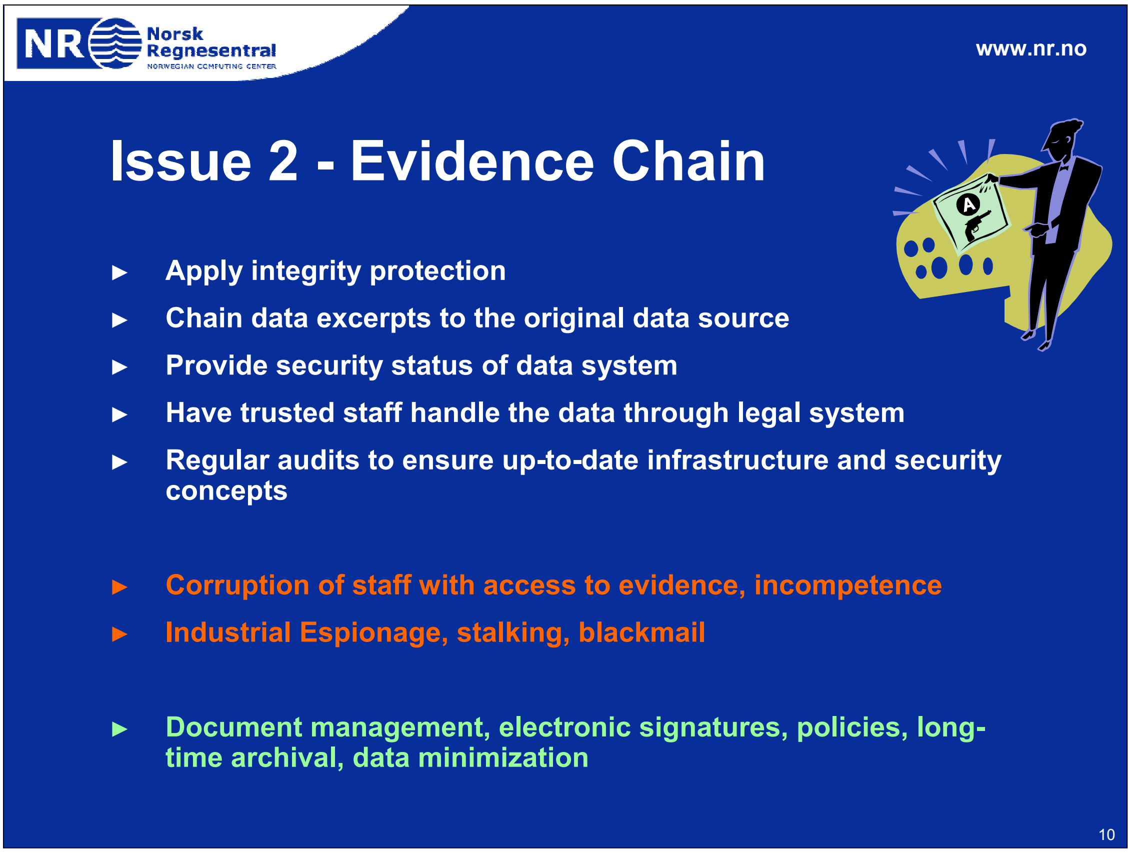
Who will be held liable if, for example, crucial business secrets (e.g. pharmaceutical patents) will be lost due to abuse of data that has been kept under retention?

Who will be held liable if a tabloid journalist exploits retention data to stalk celebrities?

What would criminals pay to gain access to important politician's network of contacts?

Would the security of endangered people be guaranteed although the retention data would be an accurate account of their cell phone location all around the clock?

Obviously, the benefits of exploring criminal's communication networks by data retention could also invite new threats to society by other uses of retention data.



Issue 2 - Evidence Chain

- ▶ Apply integrity protection
- ▶ Chain data excerpts to the original data source
- ▶ Provide security status of data system
- ▶ Have trusted staff handle the data through legal system
- ▶ Regular audits to ensure up-to-date infrastructure and security concepts

- ▶ Corruption of staff with access to evidence, incompetence
- ▶ Industrial Espionage, stalking, blackmail

- ▶ Document management, electronic signatures, policies, long-time archival, data minimization

Let's jump into the future now. Say, into the year 2011. Hard disks and data base indexes with retention data for voice, mobile, data, DSL etc. have filled up with 12 months worth of communication data. A case is will be taken into court with retention data that will date back into the year before. Some data base at some telco company will have to produce 12-months-old data in a way that satisfies several conditions:

It shall be unaltered, and original.

It shall have been kept absolutely confidential over 12 months

It shall be released only to authorized parties

It shall have warning mechanisms that will enable data abuse detection

The data shall not be usable for any other purpose than investigation and proof in court.

With today's security technology, one can imagine ALL retention data being electronically signed with signatures that are based on qualified certificates from accredited certificate authorities according to the EU directive on electronic signatures. Additionally, there must me encryption, key updates, access control and fraud management – on EVERY node of the data retention infrastructure. This might cause heavy investment for telco companies that will certainly be subject of debate. However, effective solutions might be useful for the future, as the use of retention data might spark major innovation[1] in the legal sector.

In practice, there is a large risk of cheap, ad-hoc implementation of security measures which results in logfiles being written to regular hard drives in a telecommunications computing center. What happens to such data once it is required by police and courts? Some chain of evidence must be available to have confidence about the originality of the retention data, otherwise any defending lawyer will show up in court with a logfile printout of his own and claim that his copy is the real file. So definitely, a high level of security and integrity will keep the courts efficient.

Concerning privacy, the handling of retention data might create privacy risks for a long time. A data retention file taken as a whole into court files might be available in court archives for many years – thus exposing communication connections of many people to future readers of the court files. Here, secure evidence handling procedures might be necessary to extract the retention data that is relevant for the case.

[1] I like to think data retention will be one of the major innovative tools for law enforcement and the European legal system of the near future. Not because of the tens of thousands of lives that will be saved from terrorists. What will happen is that a large number of laws-in-existence that cannot be economically enforced now all the sudden will be enforceable through data retention. Think of:

Prosecution of unwanted advertising calls

Prosecution of libel and other offense in on-line communities

Using mobile phone location tracks from retention data to prove that a suspect-to-corruption politician actually met with the Mafia men.

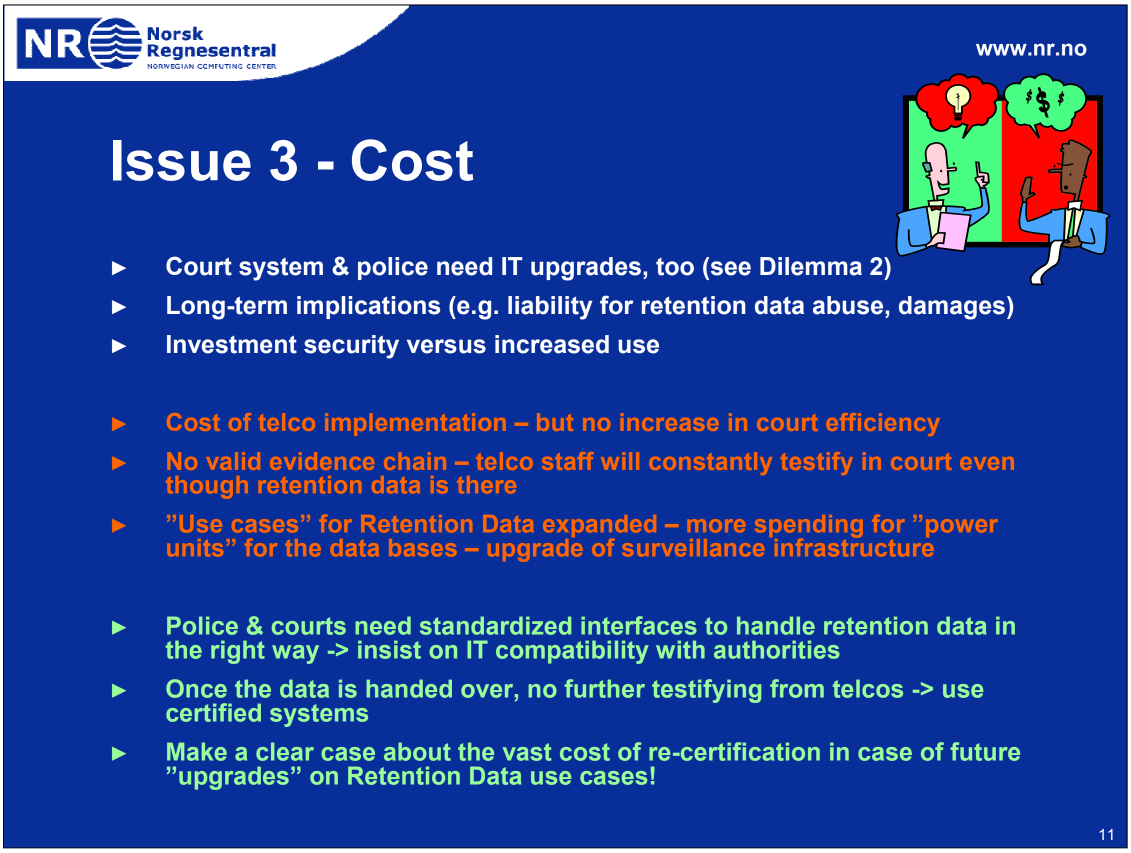
Prosecution of 0900 fraud with diallers and lottery fraud

Civil legal battles, e.g. over divorce cases and adultery can all the sudden access data retention data

Doping offence prosecution upon Tour the France doping scandals (aka Jan Ullrich's SMS to his Spanish doctor)

Consumer protection law suits (imaging a laptop vendor claiming he didn't know about a problem with the burning batteries… while retention data has all the prior complaints about them on the record)

While some of these uses are ethically questionable, they will inevitably occur some day in the future. The consequence for data retention can be that the number of requests to find and release data from a telco's data base could be higher than expected by several degrees of magnitude. Any claim of a few thousand people under terrorist observation will be easily exceeded by several 100,000 unwanted marketing calls per month.
Buy Oracle stock, too, if you want.



Norsk Regnesentral
NORWEGIAN COMPUTING CENTER

www.nr.no

Issue 3 - Cost

- ► Court system & police need IT upgrades, too (see Dilemma 2)
- ► Long-term implications (e.g. liability for retention data abuse, damages)
- ► Investment security versus increased use

- ► Cost of telco implementation – but no increase in court efficiency
- ► No valid evidence chain – telco staff will constantly testify in court even though retention data is there
- ► ”Use cases” for Retention Data expanded – more spending for ”power units” for the data bases – upgrade of surveillance infrastructure

- ► Police & courts need standardized interfaces to handle retention data in the right way -> insist on IT compatibility with authorities
- ► Once the data is handed over, no further testifying from telcos -> use certified systems
- ► Make a clear case about the vast cost of re-certification in case of future ”upgrades” on Retention Data use cases!

I like to think data retention will be one of the major innovative tools for law enforcement and the European legal system of the near future. Not because of the tens of thousands of lives that will be saved from terrorists. What will happen is that a large number of laws-in-existence that cannot be economically enforced now all the sudden will be enforceable through data retention. Think of:

Prosecution of unwanted advertising calls

Prosecution of libel and other offense in on-line communities

Using mobile phone location tracks from retention data to prove that a suspect-to-corruption politician actually met with the Mafia men.

Prosecution of 0900 fraud with diallers and lottery fraud

Civil legal battles, e.g. over divorce cases and adultery can all the sudden access data retention data

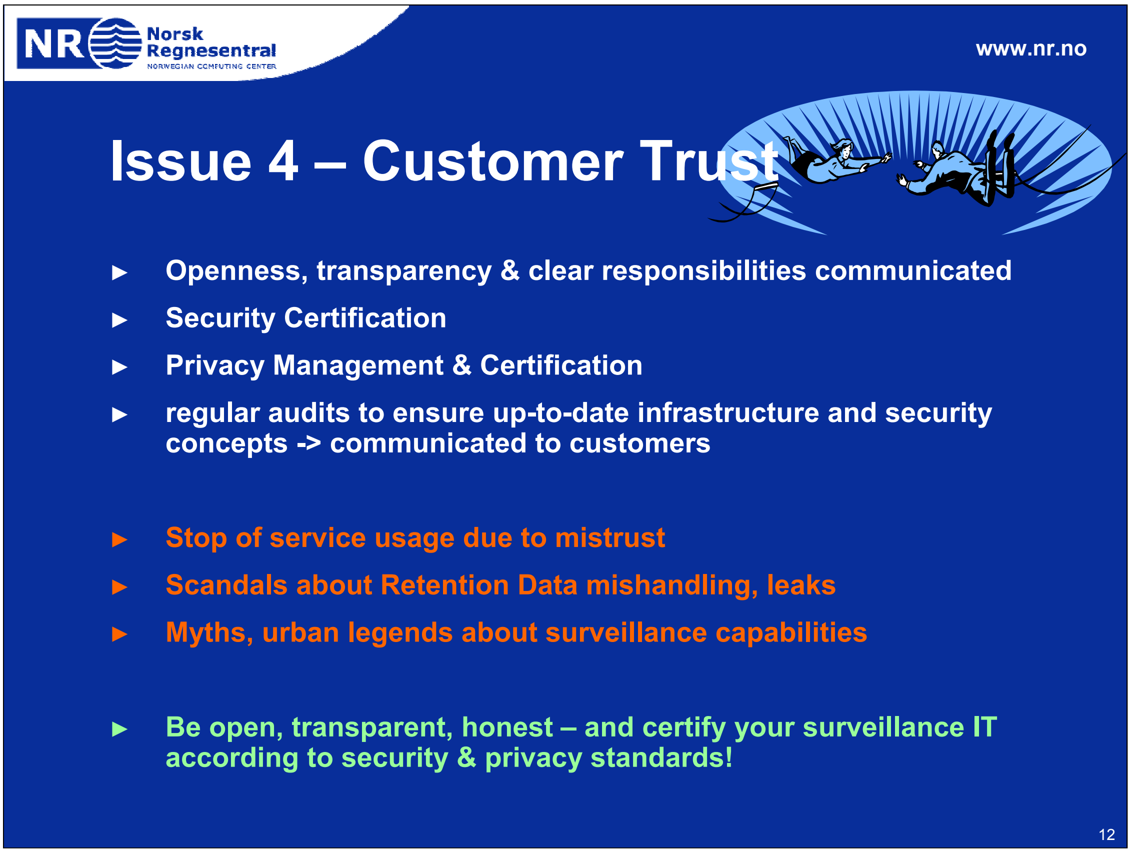
Doping offence prosecution upon Tour the France doping scandals (aka Jan Ullrich’s SMS to his Spanish doctor)

Consumer protection law suits (imaging a laptop vendor claiming he didn’t know about a problem with the burning batteries… while retention data has all the prior complaints about them on the record)

While some of these uses are ethically questionable, they will inevitably occur some day in the future. The consequence for data retention can be that the number of requests to find and release data from a telco’s data base could be higher than expected by several degrees of magnitude. Any claim of a few thousand people under terrorist observation will be easily exceeded by several 100,000 unwanted marketing calls per month.

The first thing that should be done upon implementation of data retention is a personal, vast financial investment in mass storage and database vendor stock. Every single node of any kind of communications network will require hard disks, hard disks, hard disks, and a searchable index of them.

Next, when the true financial dimensions of data retention implementation will hit telecommunication providers, solutions to minimize data collection and handling will be sought after by the market. Many of today’s implementations of wiretapping leave the cost of digging through a call-connection database with the telecommunications company. If the company is big enough, there will be a big database to search through for a particular authority’s request. Enter Oracle “power units”. The cost of the extra power of the data base to satisfy the police’s requests can be enormous. ISDN wiretapping in Germany requires each provider to install a government-certified crypto box on a dedicated line, connected to a data base for searching. The box, the data base, and the technician for 24/7 availability of the wiretapping line are paid for by the Telco.



Norsk Regnesentral
NORWEGIAN COMPUTING CENTER

www.nr.no

Issue 4 – Customer Trust

- Openness, transparency & clear responsibilities communicated
- Security Certification
- Privacy Management & Certification
- regular audits to ensure up-to-date infrastructure and security concepts -> communicated to customers

- Stop of service usage due to mistrust
- Scandals about Retention Data mishandling, leaks
- Myths, urban legends about surveillance capabilities

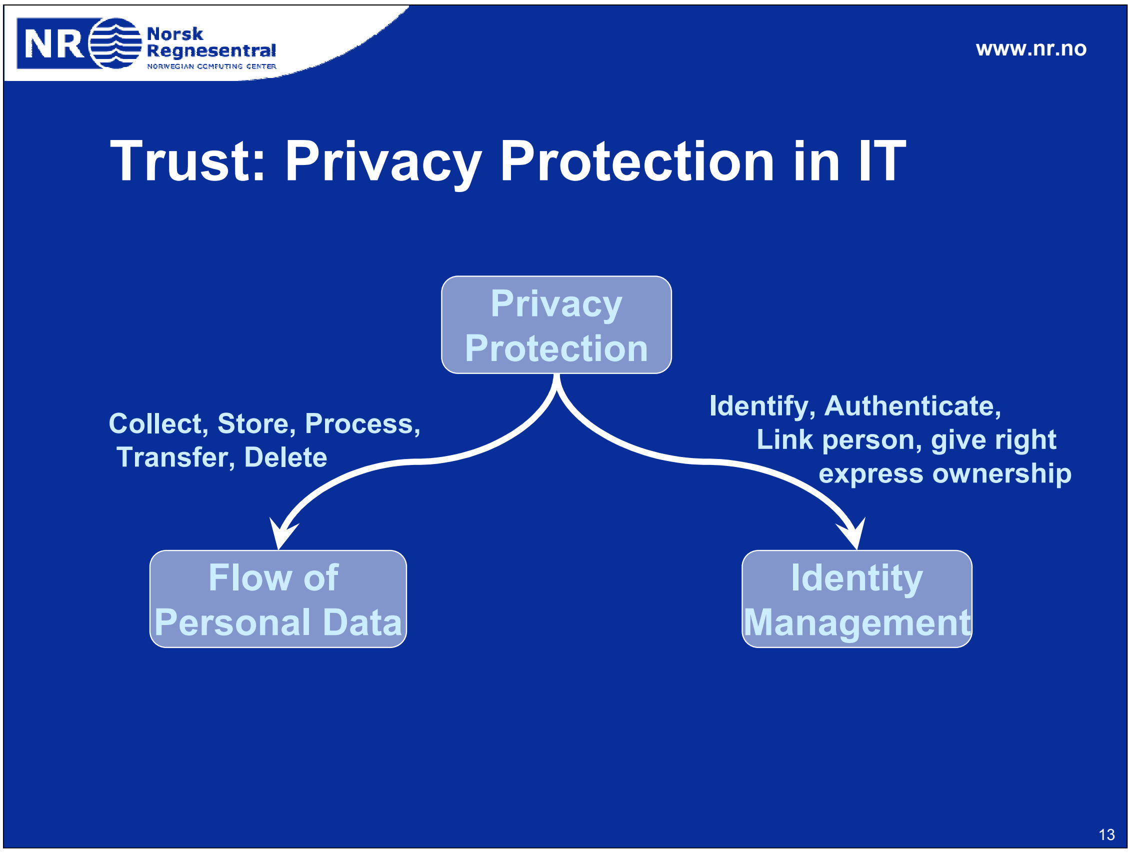
- Be open, transparent, honest – and certify your surveillance IT according to security & privacy standards!

If you carefully look at the bullet list above, you can imagine a trusted platform with policy-enforcing systems that manage retention data in a secure and reliable (and auditable) way. Many of the components developed in PET research can contribute to these functions. What, if a full deployment of a privacy management system can be used to

Provide secure, enforced, policy-based personal data handling to telecommunications providers that are subject to data retention?

Provide Identity Management, Privacy management and data control functions to the same companies along with the retention management for the purpose of data minimization and cost-effectiveness?

In our opinion, once data retention is in-place, it provides an unseen opportunity for PET technology to be deployed to all major players in telecommunications.



Trust: Privacy Protection in IT

Privacy Protection

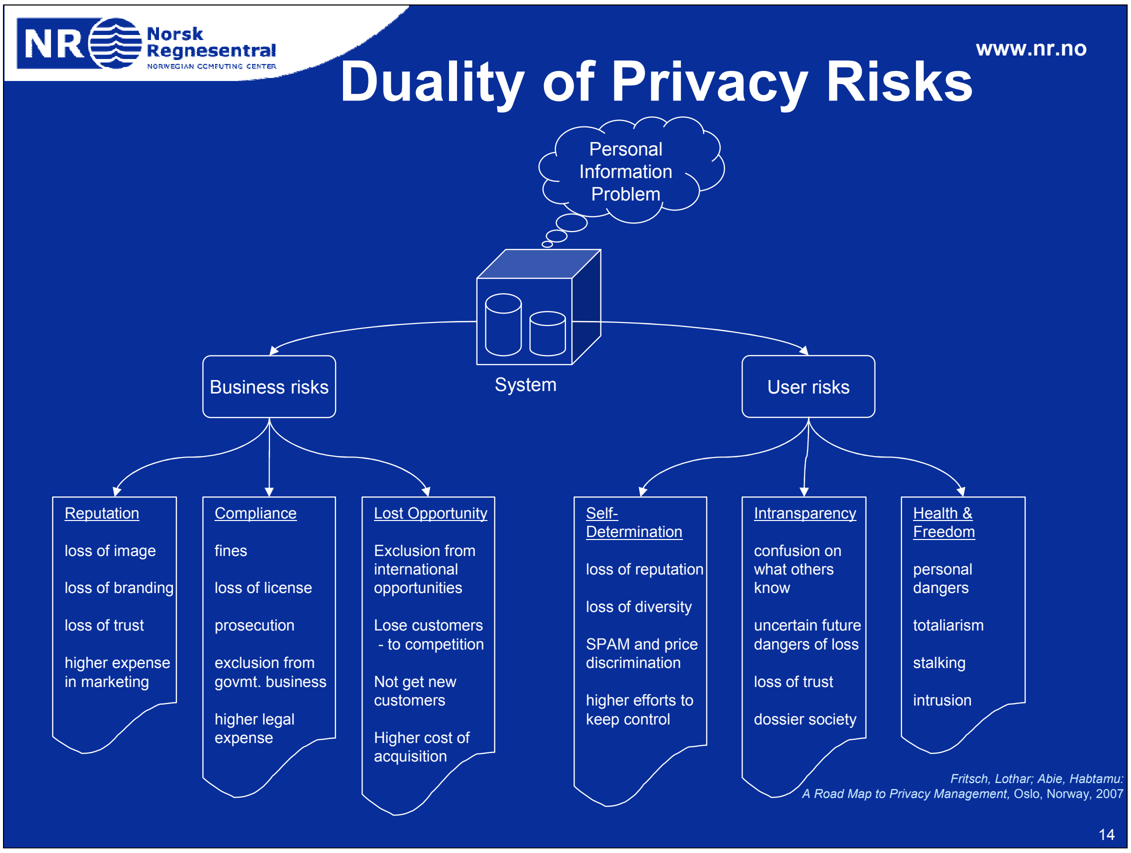
Collect, Store, Process, Transfer, Delete

Flow of Personal Data

Identify, Authenticate, Link person, give right express ownership

Identity Management

Private information occurs either in work flows in the privace information processing life cycle, or in form of identity information where identities are processed for various reasons.



Duality of Privacy Risks

Personal Information Problem

System

Business risks

User 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

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

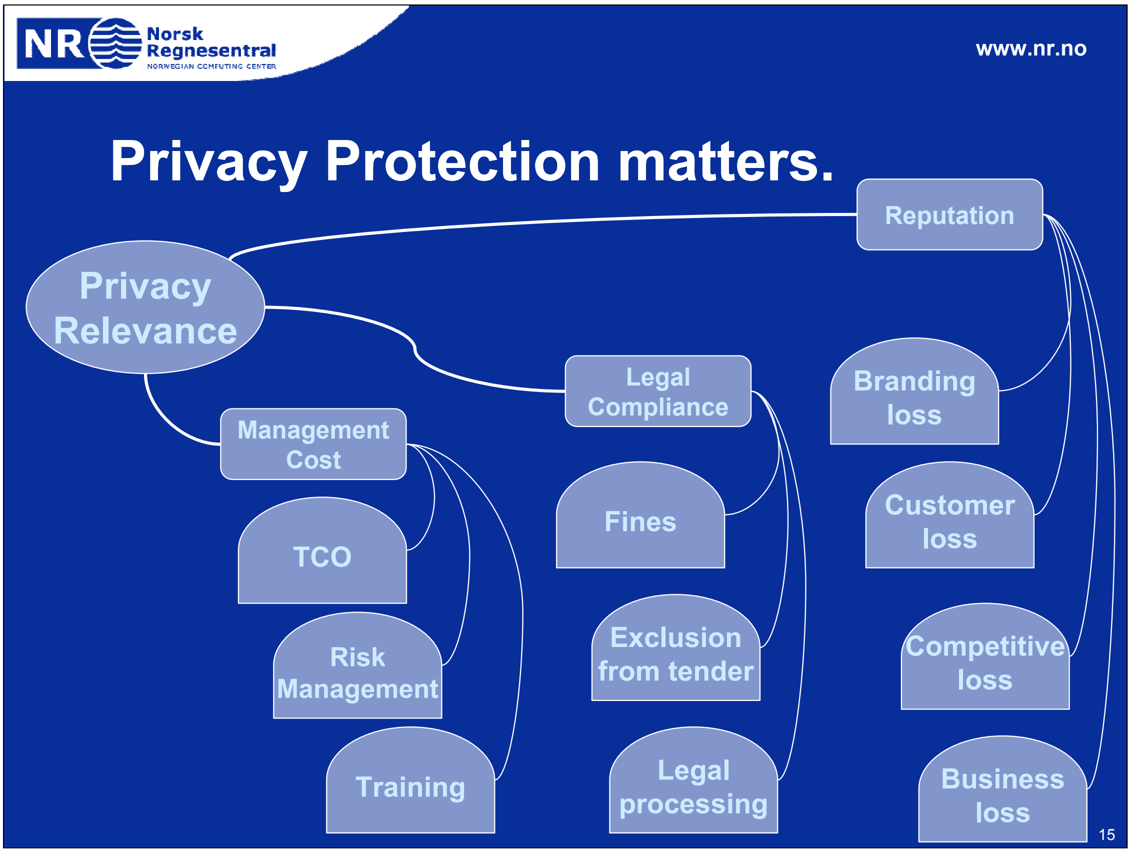
personal dangers

totaliarism

stalking

intrusion

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



Norsk Regnesentral

NORWEGIAN COMPUTING CENTER

www.nr.no

Privacy Protection matters.

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

15

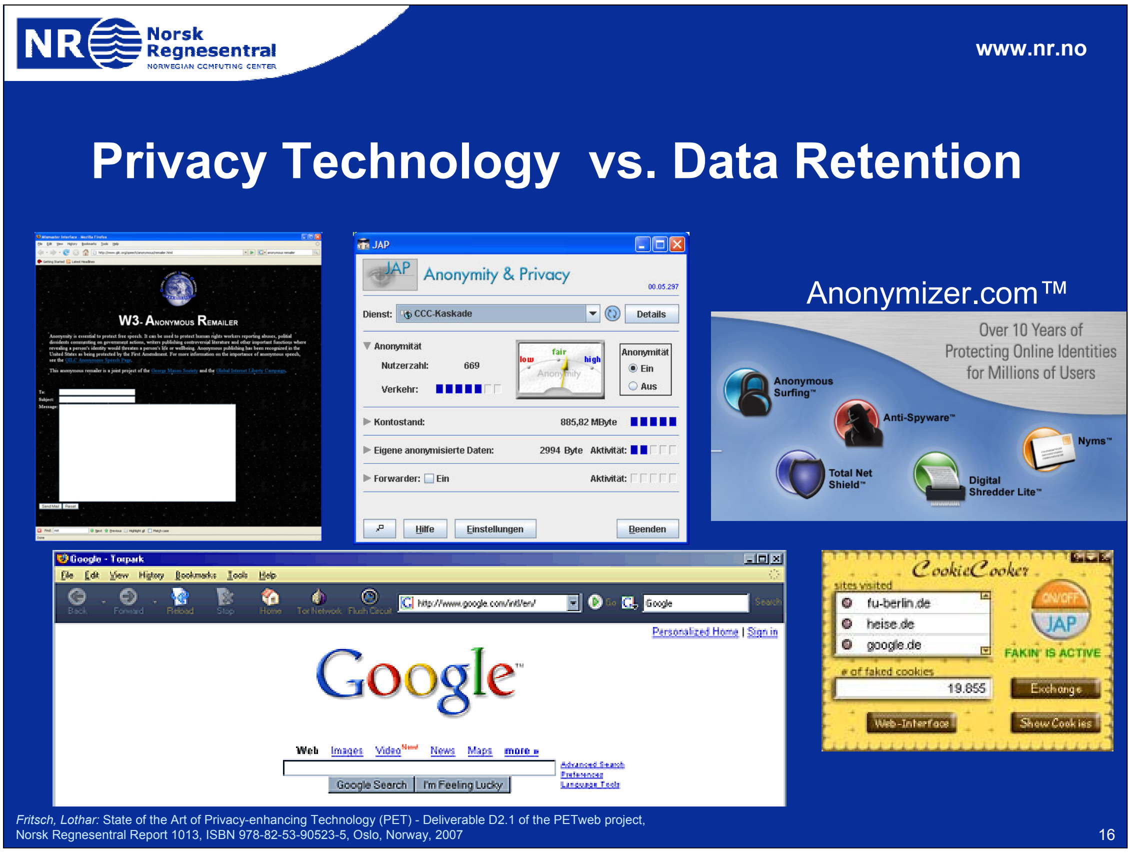
Privacy protection is a ICT management issue. It causes cost-of-ownership, no matter whether a sophisticated privacy concept is implemented, or not. In 2004, the Ponemon Institute conducted a study for IBM (Ponemon Institute (2004) The Cost of Privacy Study, The Ponemon Institute, Tucson, Arizona). It provides a cost factor model and provides some insight into corporate spending patterns for privacy management in large corporations. The authors define a "total privacy cost framework". The approach is to compare the cost of non-compliance to privacy requirements to the cost of investing in privacy management with respect to its effect. The assumption is that the optimum in privacy spending is where the expenditure equals the non-compliance cost. This results in the calculation of privacy protection cost not with the goal of maximum privacy, but cheapest compliance.

Business side cost factors

1. *Privacy Office*: Costs associated with dedicated staff, office overhead, travel and business equipment.
2. *Policy & Procedures*: Costs associated with the creation, review, publication and dissemination of the privacy policy (and privacy notice when applicable).
3. *Downstream Communications*: Costs associated with the communication and outreach activities for the privacy program both within the company and to outside stakeholders.
4. *Training & Awareness*: Costs associated with the education of employees and other key company stakeholders about the privacy policy, program and related concepts.
5. *Enabling Technologies*: Costs associated with technologies that help mitigate privacy risk, enhance responsible information management, or protect the critical data infrastructure.
6. *Employee Privacy*: Costs associated with the protection of sensitive employee records, including heath care and OSHA claims.
7. *Legal Activities*: Costs associated with legal review and counsel concerning the privacy program as well as legal defence costs in the event of a privacy violation.
8. *Audit & Control*: Costs associated with the monitoring, verification and independent audit of the privacy program, including use of controlled self-assessment tools.
9. *Redress & Enforcement*: Costs incurred to provide upstream communication of a privacy or data protection breach to appropriate parties within the organization, including the cost of investigation and collaboration with law enforcement. In addition to the above cost center activities, the current research captured additional information

(Cost of privacy from Ponemon Institute (2004) The Cost of Privacy Study, The Ponemon Institute, Tucson, Arizona.*)*

From this, some significant insight can be gained. The survey lists the privacy costs ranked by direct cost. IT systems (e.g. PET or IDM), are on the third position of the most expensive cost factors, amounting about one-third of the cost of privacy office, and less than 50% of the cost for training. Beyond PET, there eight other cost factors exist that are policy-intense or involve specialized employees, e.g. lawyers. As a conclusion, privacy technology by itself is not a main cost driver – policies, enforcement, legal counsel and many other factors outnumber the cost of PET used.



www.nr.no

Privacy Technology vs. Data Retention

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

Google - Torpark

http://www.google.com/intl/en/

CookieCooker

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

# of faked cookies: 19.855

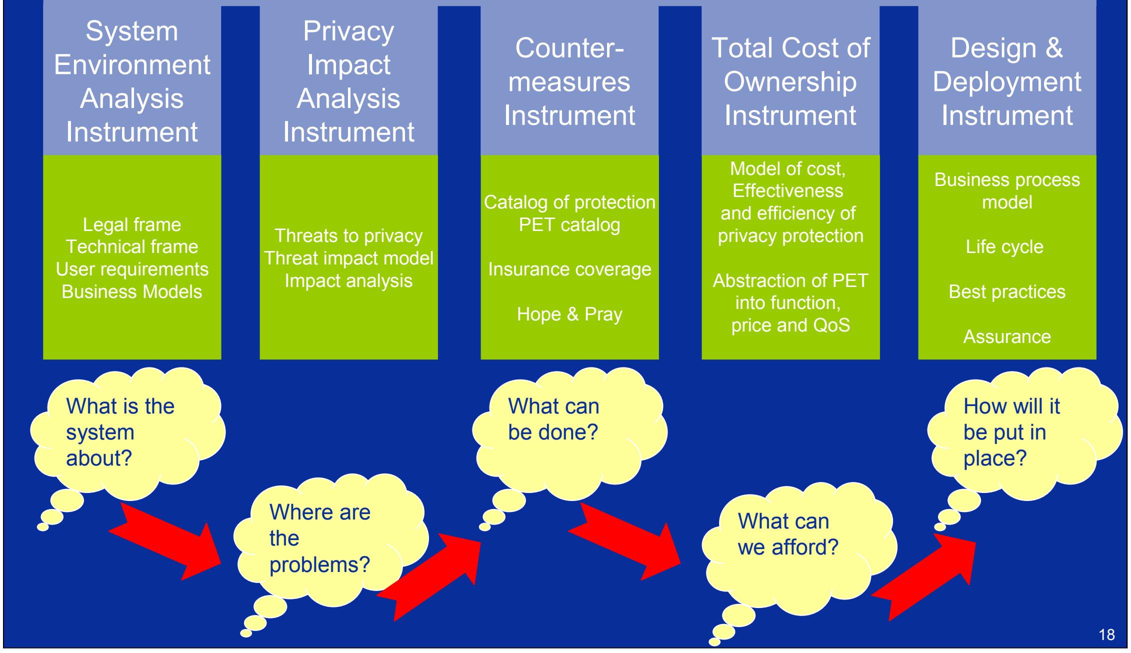
Fritsch, Lothar: State of the Art of Privacy-enhancing Technology (PET) - Deliverable D2.1 of the PETweb project, Norsk Regnesentral Report 1013, ISBN 978-82-53-90523-5, Oslo, Norway, 2007

Division of tools in opacity tools and transparency tools.

Privacy Technology vs. Data Retention

- Hide communication connections with MIXes (MixMaster, TOR, Anon)
- Use proxies (e.g. Anonymizer.com, freedom.net)
- Use Skype / private VoIP with VPNs
- Swap steganographic images on Flickr
- Trade SIM-cards on with others
- Encrypt your hard disk & e-mail

Privacy Investment Decision Instruments



System Environment Analysis Instrument

Legal frame
Technical frame
User requirements
Business Models

Privacy Impact Analysis Instrument

Threats to privacy
Threat impact model
Impact analysis

Counter-measures Instrument

Catalog of protection
PET catalog

Insurance coverage

Hope & Pray

Total Cost of Ownership Instrument

Model of cost, Effectiveness and efficiency of privacy protection

Abstraction of PET into function, price and QoS

Design & Deployment Instrument

Business process model

Life cycle

Best practices

Assurance

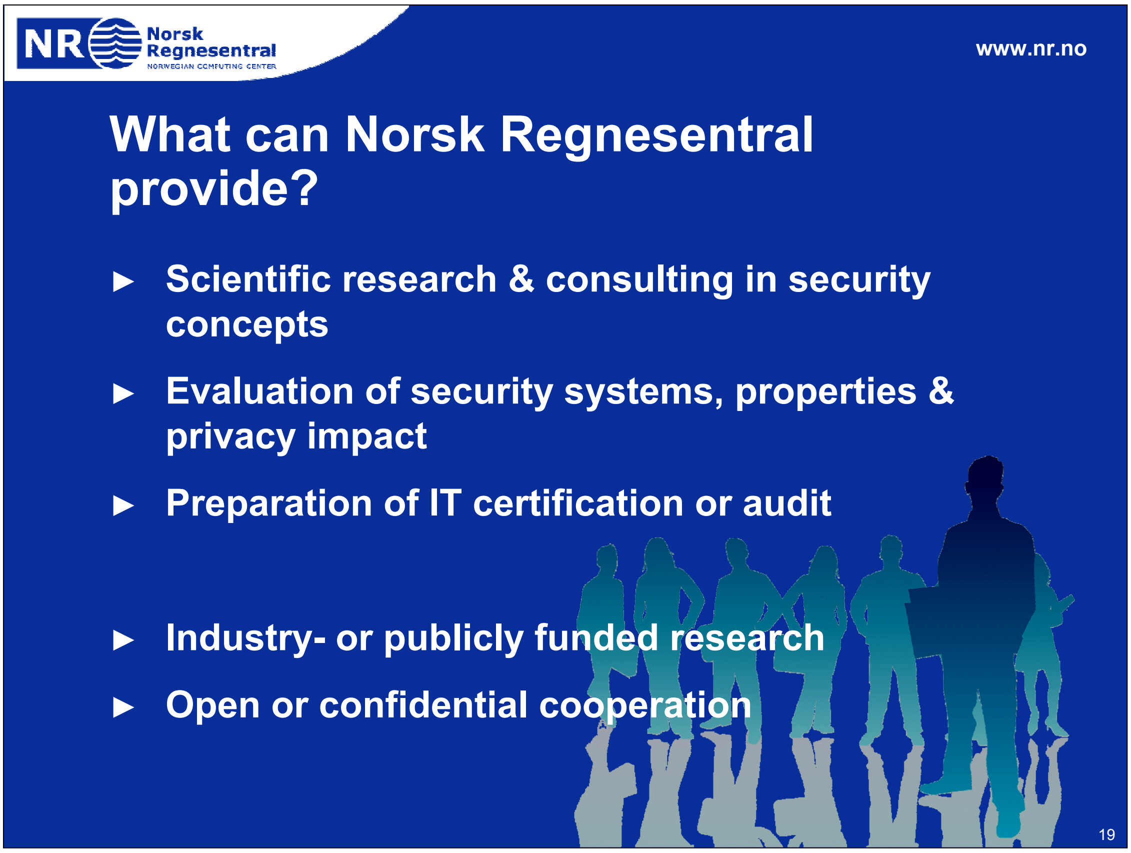
What is the system about?

Where are the problems?

What can be done?

What can we afford?

How will it be put in place?



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

DART - Department of Applied Research in Information Technology

Research director: Åsmund Skomedal
Assistant research director: Knut Holmqvist

www.nr.no

ICT research at NR in the area of Information and Communication Technology has its main basis in Internet technology and applications as well as software engineering. Founded on our strength in object-oriented programming, we cover both basic methodology and applications.

Contact us if you need answers to questions such as the following:

How can IT security systems be improved?

How can images and videos be transferred on low bandwidth?

How can ICT systems be designed so that all members of society will be able to use them?

How can multimedia, multichannel server technology be improved?

Can Internet gaming be more than just entertainment?

How can complex distributed systems be handled by better architecture and server technology?

How can existing information be presented best on mobile devices or PCs?

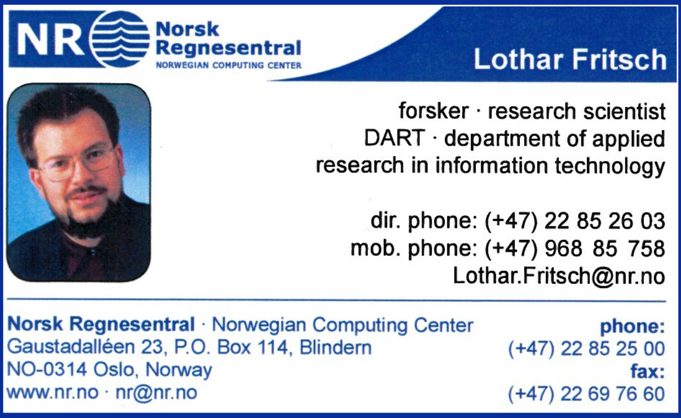
How can modelling and analyzes improve the work flow or activity in an organization?

What is universal design of ICT?

How can pedagogical principles be integrated into e-learning systems?

Questions?

Contact



Norsk Regnesentral
NORWEGIAN COMPUTING CENTER

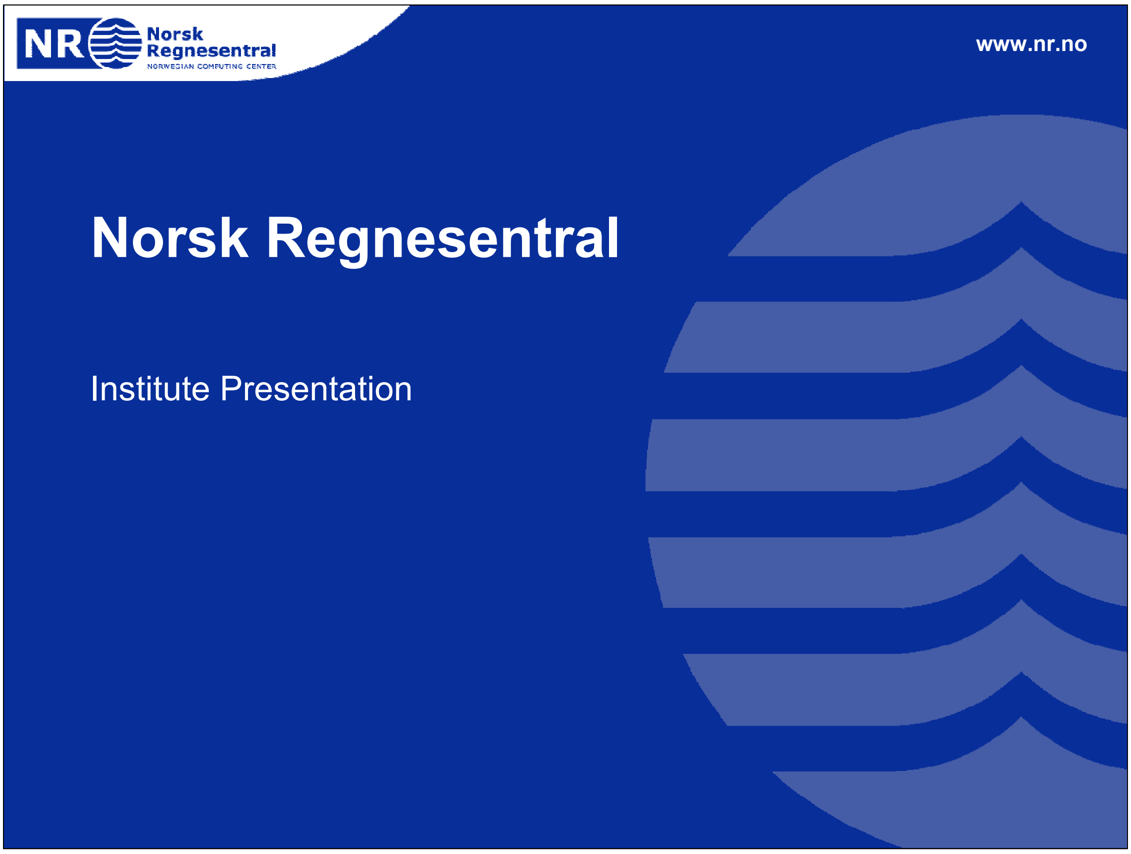
Lothar Fritsch

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

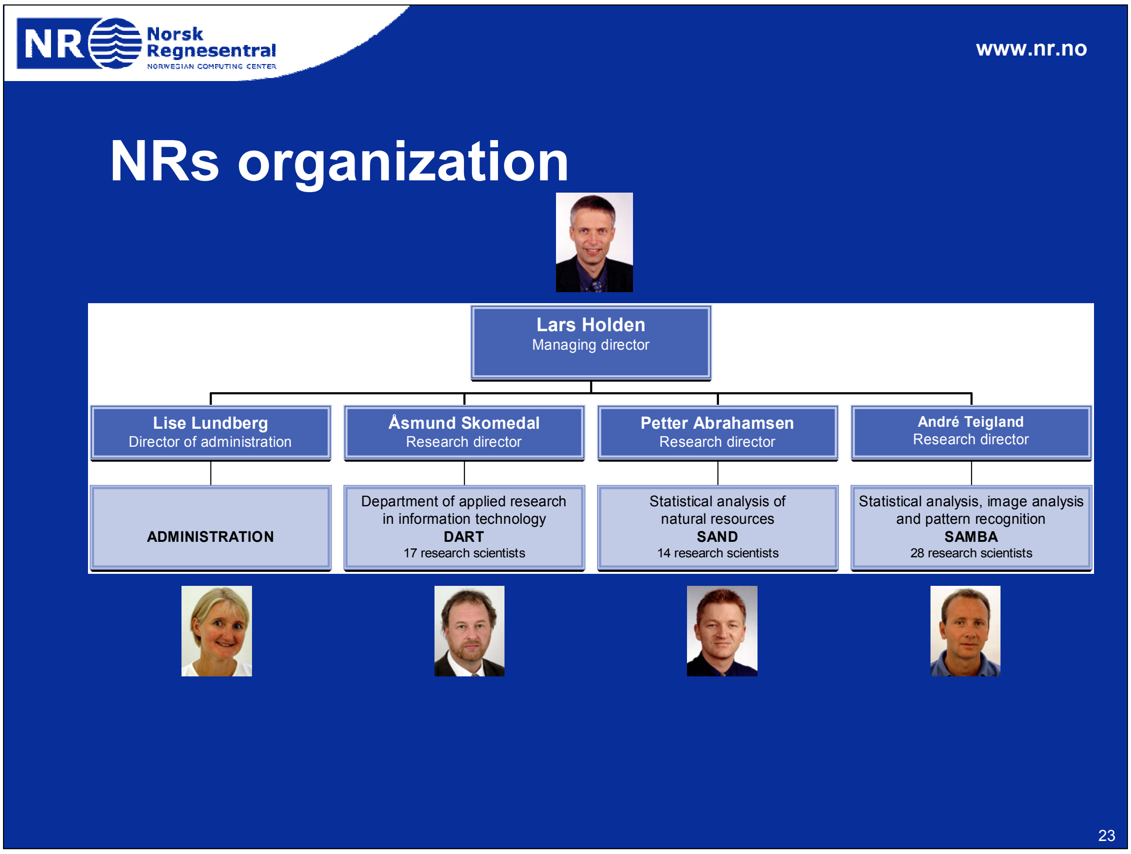
phone:
(+47) 22 85 25 00
fax:
(+47) 22 69 76 60



www.nr.no

Norsk Regnesentral

Institute Presentation



NRs organization

Lars Holden
Managing director

Lise Lundberg
Director of administration

ADMINISTRATION

Åsmund Skomedal
Research director

Department of applied research in information technology
DART
17 research scientists

Petter Abrahamsen
Research director

Statistical analysis of natural resources
SAND
14 research scientists

André Teigland
Research director

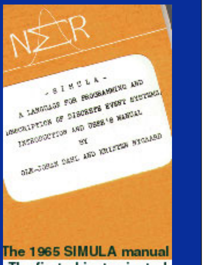
Statistical analysis, image analysis and pattern recognition
SAMBA
28 research scientists

History: organization

1952	Established as center
1958	Institute under Norwegian Council f Science and Industrial Research
1958-1970	“Computing center” with R&D within operation analysis, statistics and data processing
1971-1985	Method-oriented research institute
1985	Independent research foundation

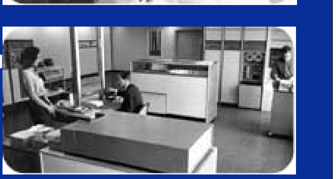
R&D milestones

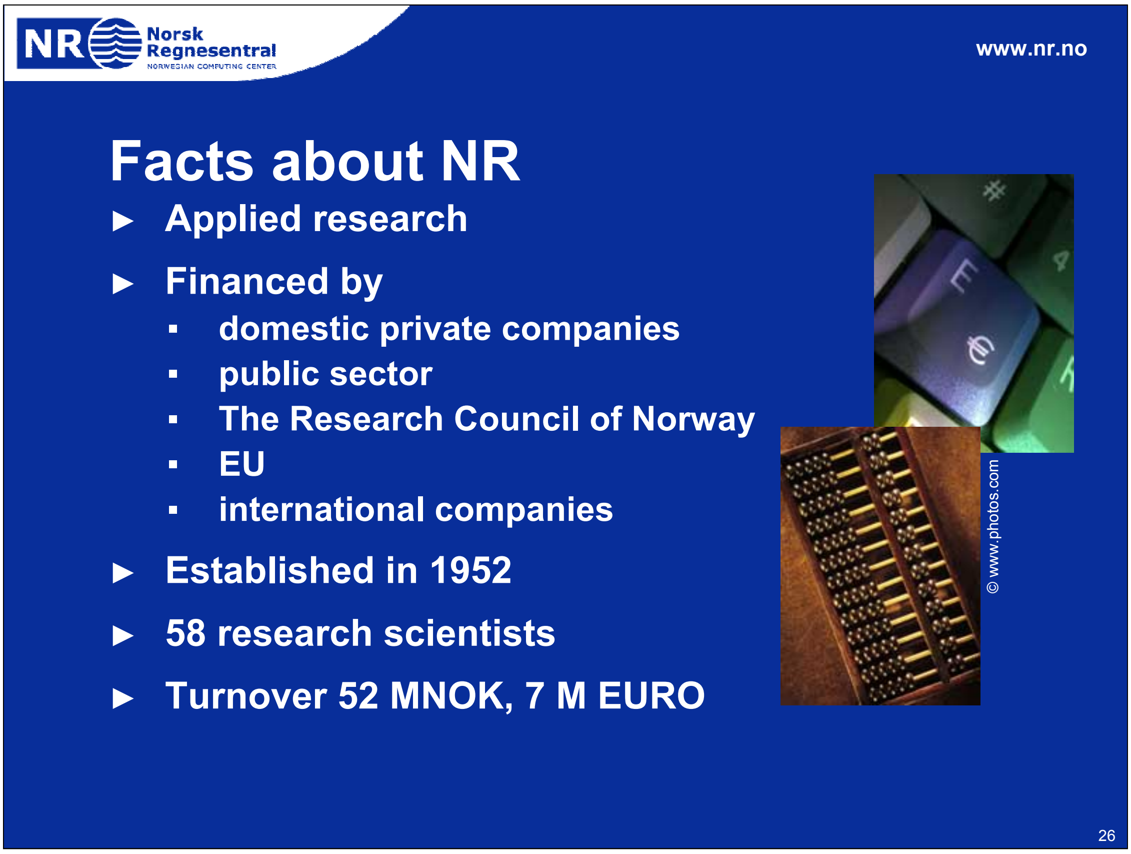
1952	Calculations for professors and later Nobel laureates Frich and Hassel
1954	Nusse, first digital computer built in Norway, industrial “number crunching”
1960	Mathematical statistics, operation analysis
1963	Univac 1107 (the largest civil computer in Europe)
1965	SIMULA I (first version, simulation language)
1966	OPTIMA (project control)
1967	SIMULA 67 (first object-oriented programming language, A.M. Turing Award 2001, IEEE John von Neuman Medal, 2002)
1970	Trade union projects (employee participation)
1971	Distributed computing
1974	Remote sensing ➔ image analysis
1981	Mach-S computer, object oriented hardware
1984	Geostatistics ➔ petroleum (Establ. Odin a.s. in 1992, Statoil prize 199
1985	BETA-programming language
1988	Multimedia
1992	Object-oriented System Description Language, OSDL (Telenor prize 1
1996	Minke whale project
2001	Large financial risk projects
2002	Climate monitoring by use of satellite
2007	Statistics for innovation, Centre for research based innovation


NΣR

- S I M U L A -
A LANGUAGE FOR PROGRAMMING AND
DESCRIPTION OF DISCRETE EVENT SYSTEMS
INTRODUCTION AND USER'S MANUAL
BY
OLE-JOHAN DAHL AND KRISTEN NYGAARD

The 1965 SIMULA manual
The first object-oriented report





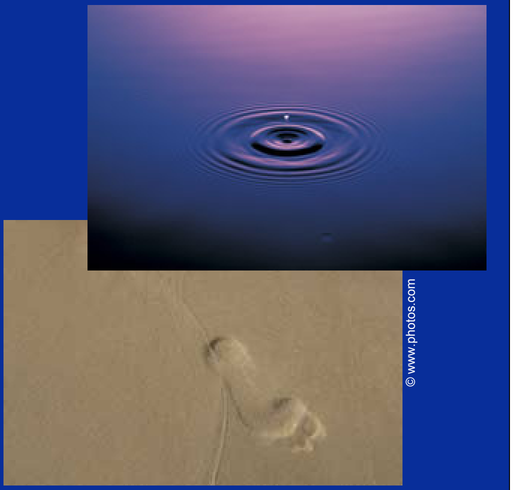
Facts about NR

- Applied research
- Financed by
  - domestic private companies
  - public sector
  - The Research Council of Norway
  - EU
  - international companies
- Established in 1952
- 58 research scientists
- Turnover 52 MNOK, 7 M EURO

© www.photos.com

NR’s strategy

- Improve scientific level
- Internationalization
- Applications depend on market
- Customer relation



© www.photos.com

Research results that are used and visible

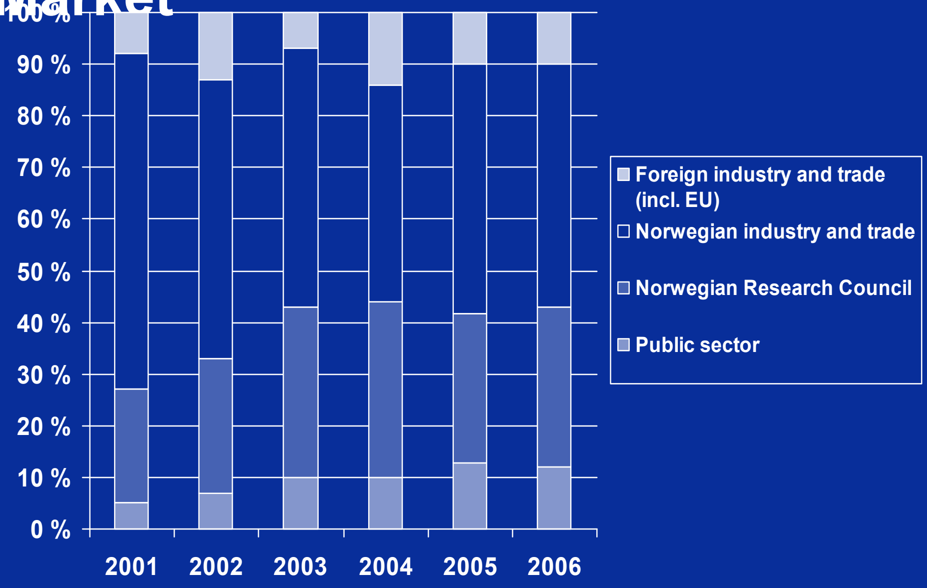
Main areas

- Information and communication technology (ICT)

© www.photos.com

- Statistical-mathematical analysis and modeling

Market


100 %
90 %
80 %
70 %
60 %
50 %
40 %
30 %
20 %
10 %
0 %
2001
2002
2003
2004
2005
2006
▨ Foreign industry and trade (incl. EU)
□ Norwegian industry and trade
▨ Norwegian Research Council
▨ Public sector

Customers

© www.photos.com

Aschehoug & Co.
Astra Zeneca
Avinor
Bankorg. (BBS og BSK)
Bladcentralen ANS
British Gas
ConocoPhillips
Dagbladet AS
DnB NOR ASA
DNO
E-CO Vannkraft
Eramet
ESA
EU
Fiskeridepartementet
Fiskeriforskning AS
Funcom
Gjensidige NOR
Havforskningsinstituttet

Institutt For Grafiske Medier
KLP forsikring
Kopinor
Markeds- og Mediainst.
Nemko AS
Nettfokus
Norges Bank
Norges Forskningsråd
Norges vassdrags- og energiverk
Norsk Gallup
Norsk Hydro ASA
Norsk institutt for vannforskning
Norsk Tipping
NORUT Informasjons-teknologi
OSIS International
Oslo kommune
Pareto Securities ASA
Radiumhospitalet

Rikshospitalet
Ringnes AS
Roxar ASA
Scandpower
Shell
Simula Research Laboratory
Skattedirektoratet
Statens forvaltningstjeneste
Statens vegvesen
Statkraft SF
Statnett
Statoil ASA
Statskonsult
Telenor ASA
Tomra Systems ASA
Total
TV2
Uninett
Universitetet i Oslo
Vegdirektoratet
VG Multimedia AS
Visma
Vital Forsikring ASA

EU projects

(5th and 6th Framework Programme) — examples

- CASENET
  - A platform for risk analysis of security critical systems
- FOREMMS
  - Forest environmental monitoring and management system based om remote sensing
- EUROCLIM
  - Environmental monitoring by remote sensing
- SAIGUP
  - Sensitivity analysis of the impact of geological uncertainties on the production forecasting of clastic hydrocarbon reservoirs
- Geoland
  - Remote sensing
  - Mountain vegetation and snow cover

ENVISYS - remote sensing

Automatic marine oil spill detection

EuroCODE - computer-supported cooperative work

CSCW Open object-oriented development environment

MADE - multimedia documents

Multimedia application development environment

mOOnlight - development kit for computer games

Multimedia object-oriented shell for interactive games

PUNQ & PUNQ 2

Production uncertainty estimation (petroleum reservoirs)

Snowtools

Remote sensing methods with focus on snow hydrology

SPACE

Exchange of citizen data

TRUMPET - network security

Inter-domain management

MADISON

Architecture for distributed interactive simulation

HARP

Security of web technologies and applications

CORAS

A platform for risk analysis of security critical systems

Academic collaboration

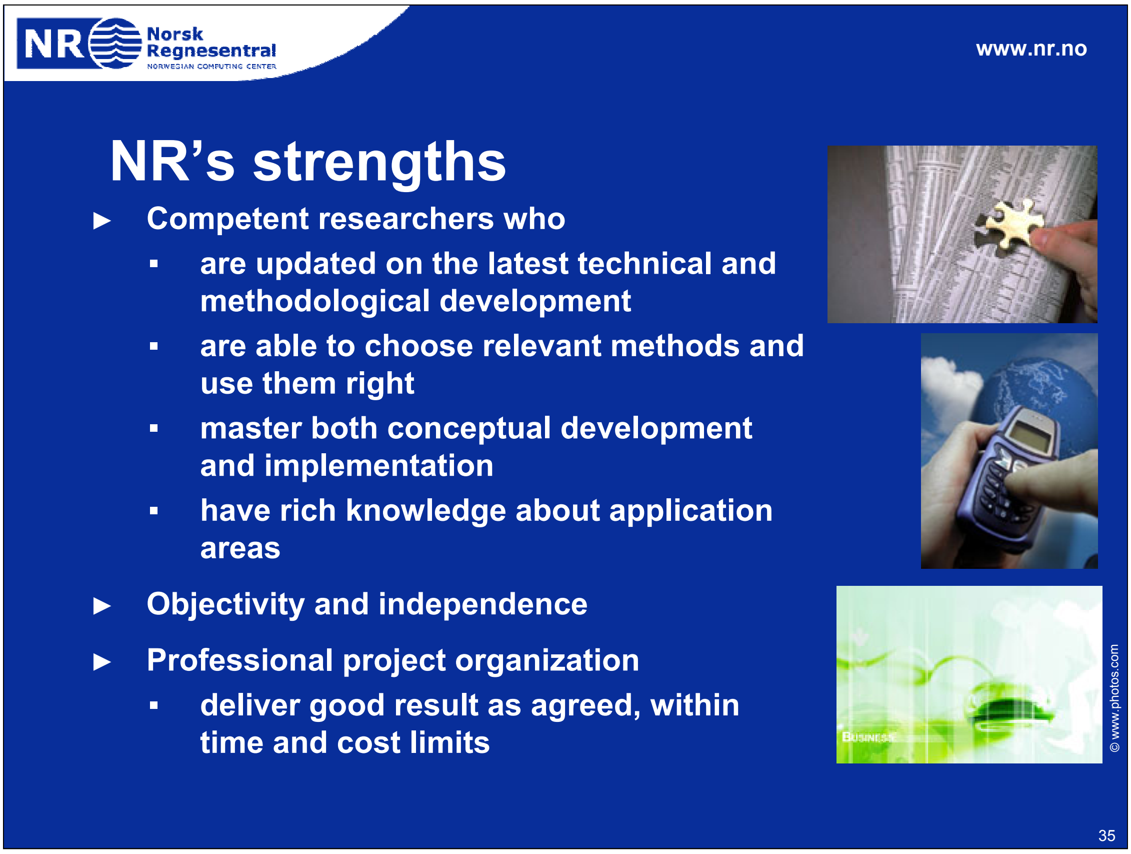
- Teaching, supervising and grading
  - Ph.D and M.Sc levels
- Institute and center collaboration
- Co-projects
  - Both Norwegian and foreign universities
- Mutual part-time positions
  - Adjoint professors at universities
  - Part-time positions/project assistance at NR

© www.photos.com

Academic partners in Norway

- University of Oslo
  - Dep. of Mathematics
  - Dep. of Informatics
  - Dep. of Educational Res.
  - Norwegian Research Center for Computers and Law
- University of Bergen
  - Dep. of Geology
- Institute of Marine Research
- Norwegian Geotechnical Inst.
- Norwegian Meteorological Institute
- NORUT Group
- Norwegian Institute of Fisheries and Aquaculture
- Nansen Environmental and Remote Sensing Center
- Norwegian Institute for Air Research
- NORSAR
- Norwegian Space Centre
- Norwegian University of Science and Technology (NTNU)
- SINTEF
- IFE
- Veritas Research

© www.photos.com

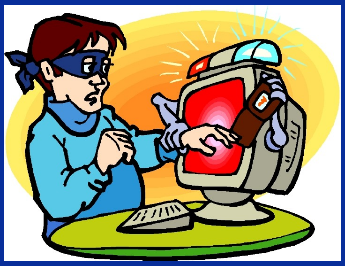


NR’s strengths

- Competent researchers who
  - are updated on the latest technical and methodological development
  - are able to choose relevant methods and use them right
  - master both conceptual development and implementation
  - have rich knowledge about application areas
- Objectivity and independence
- Professional project organization
  - deliver good result as agreed, within time and cost limits

© www.photos.com

ICT



- Security
  - Privacy
  - Digital forensics
  - Risk management
  - Public Key Infrastructure (PKI)
  - Digital Rights Management (DRM)
  - Mandatory Access Control

© www.clipart.com

ICT (cont.)

- Multimedia multichannel
  - Video/Audio Streaming
  - Multimedia Metadata & Databases
  - Mobility
  - Games
  - Digital TV
  - edia e-learning tools

Ill. Ella Okstad

ICT (cont.)

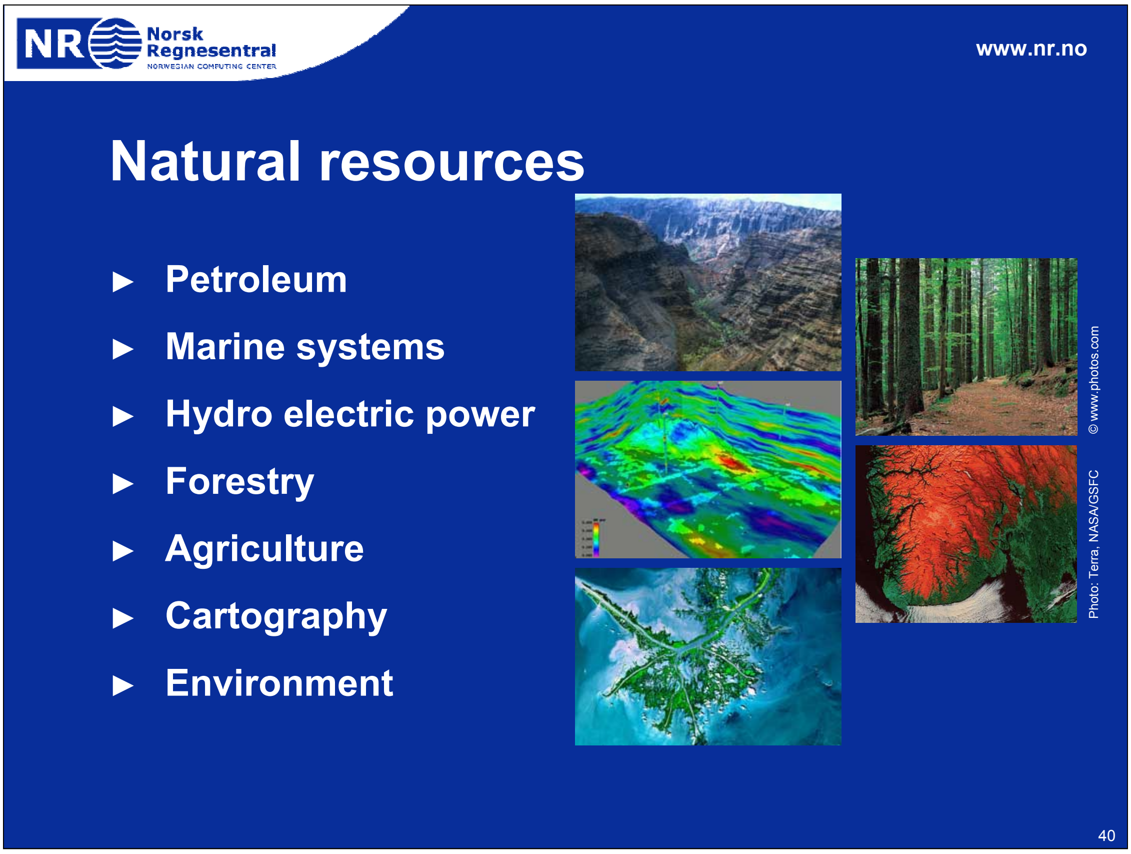
- eInclusion
  - Universal design
  - Product and services accessible by as many users as possible

Ill. Ella Okstad

Statistical-mathematical analysis and modeling

- ► Natural resources
- ► Environment
- ► Climate
- ► Remote sensing
- ► Image analysis
- ► Pattern recognition
- ► Finance and insurance

© www.photos.com



Norsk Regnesentral
NORWEGIAN COMPUTING CENTER

www.nr.no

Natural resources

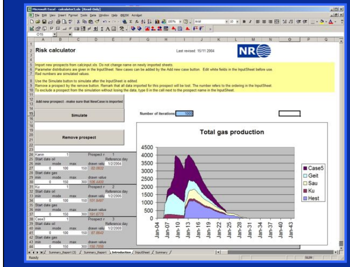
- Petroleum
- Marine systems
- Hydro electric power
- Forestry
- Agriculture
- Cartography
- Environment

© www.photos.com

Photo: Terra, NASA/GSFC

Petroleum applications

- ► Modeling geology
  - ▪ Geometry – surfaces and faults
  - ▪ Properties
- ► Data integration
- ► Uncertainty and risk



Microsoft Excel - calculator3.xls [Read-Only]

Risk calculator

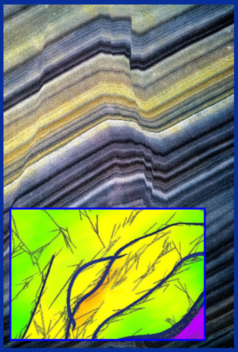
Last revised: 15/11 2004

Import new prospects from calcinput.xls. Do not change name on newly imported sheets.
Parameter distributions are given in the InputSheet. New cases can be added by the Add new case button. Edit white fields in the InputSheet before use.
Red numbers are simulated values.

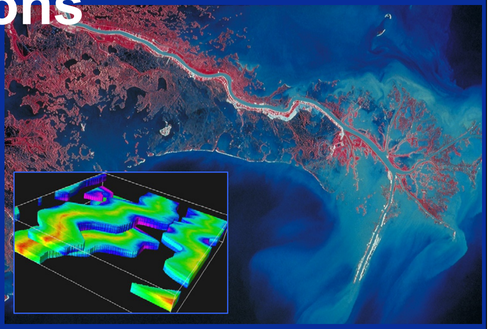
Use the Simulate button to simulate after the InputSheet is edited.
Remove a prospect by the remove button. Remark that all data imported for this prospect will be lost. The number refers to the ordering in the InputSheet.
To exclude a prospect from the simulation without losing the data, type 0 in the cell next to the prospect name in the InputSheet.

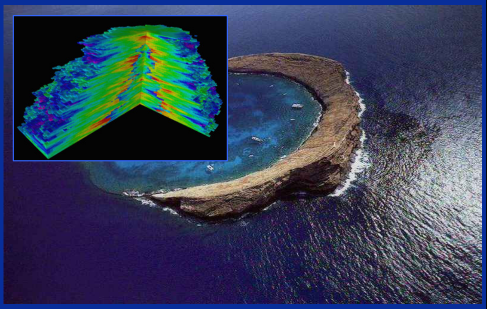
Number of iterations: 1000

Kanin	1		Prospect r	1
Start date oil				Reference day
min	mode	max	drawn valu	1/2/2004
0	100	150	82.0832	
Start date gas				
min	mode	max	drawn value	
0	150	300	106.4400	
Ku	1		Prospect r	2
Start date oil				Reference day
min	mode	max	drawn valu	1/2/2006
0	100	150	101.9497	
Start date gas				
min	mode	max	drawn value	
0	150	300	191.6775	
Case3	1		Prospect r	3
Start date oil				Reference day
min	mode	max	drawn valu	1/2/2008
0	100	150	87.8642	
Start date gas				
min	mode	max	drawn value	
0	150	300	150.7058	



© www.photos.com





Environment and marine resources

- Marine
  - Estimation with uncertainty of fish stocks and age

Counting the number of Norwegian spring-spawning herring (norsk vårgytende sild) in Vestfjorden (Photos: NR)

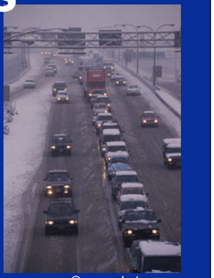
- Environment
  - Space-time models for:
    - Estimation of air pollution
    - Environmental surveillance from satellite

Statistical methods in finance and energy

- ► Finance
  - ▪ risk analysis, credit scoring
- ► Insurance
  - ▪ extreme value theory, geopricing, risk premium
- ► Energy
  - ▪ prediction of electricity, gas and oil prices

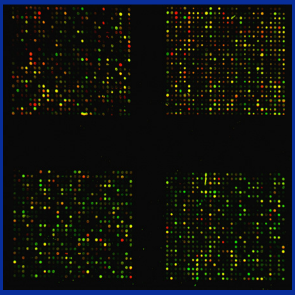
© www.photos.com

General statistical applications



© www.photos.com

- General statistical modeling and analysis
  Examples:
  - optimal distribution of newspapers
  - modeling of traffic
  - analysis of data from Internet questionnaires
  - prognosis for World



- Statistical methods in bioinformatics

Microarray data are used for measuring gene expression, i.e. how active the different genes in a cell are. The role of thousands of genes are studies simultaneously. Experiment by Anne Forus

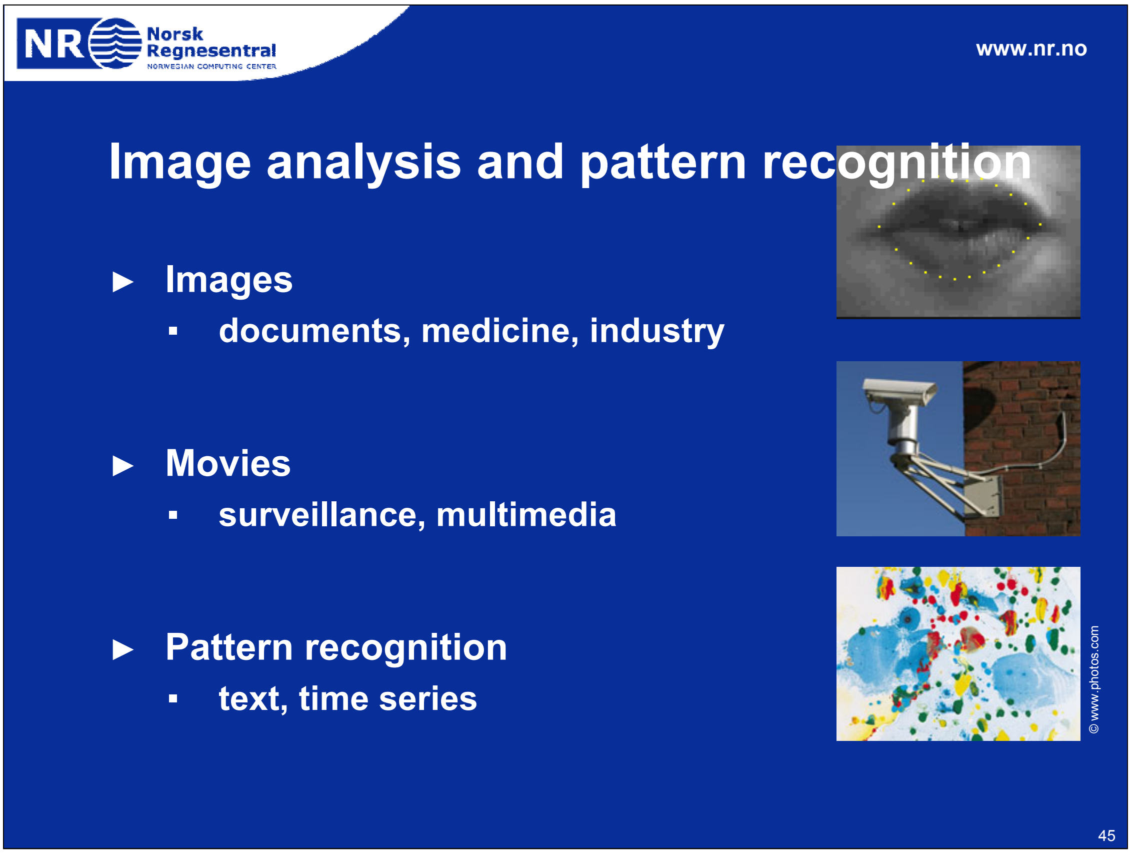


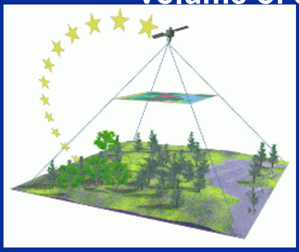
Image analysis and pattern recognition

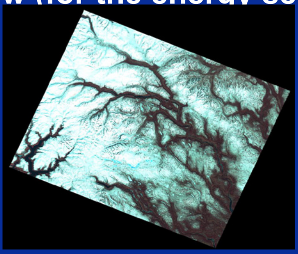
- ► Images
  - ▪ documents, medicine, industry
- ► Movies
  - ▪ surveillance, multimedia
- ► Pattern recognition
  - ▪ text, time series

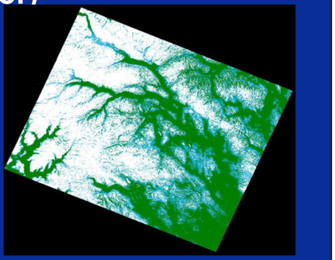
© www.photos.com

Remote sensing

- Analysis of images from satellites and airplanes
  - Environment
    - oil spill, forest surveillance
  - Snow
    - volume of snow (for the energy sector)







Statistics for innovation

- ► One of 14 Norwegian Centres for Research-based Innovation
- ► Funding 10 MNOK/y 2007-2014
- ► Academic partners: UiO, NTNU
- ► Application areas and partners:
  - ▪ Petroleum: Statoil
  - ▪ Finance: DnBNOR, Gjensidige, Hydro
  - ▪ Marine: IMR
  - ▪ Health: Biomolex, PubGene, Riks-Rad.hosp.,Sencel, Smerud
- ► Long term research, innovation focus, PhD, international collaboration

Privacy protection

- Strategic institute program 2002-2005
- 8 MNOK
  - Main topics
    - enabling organizations to protect the privacy of their customers
    - using personal information legally
    - development of a framework for enforcement of privacy policies
- Academic collaboration
    - AFIN, Faculty of Law, Univ. of Oslo

© www.photos.com

Norges forskningsråd

Service channeling (channel S)

- Strategic institute program 2000-2004
- 9 MNOK
  - Five main topics
  - Service and information architectures
  - Mobile solutions
  - User interface
  - Interoperability
  - Electronic commerce
- Multi-client R&D

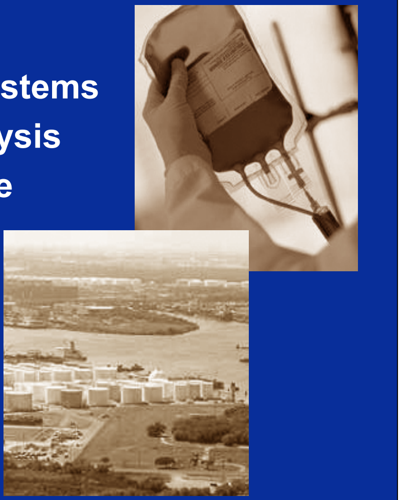
StAR - Statistical Analysis of Risk

- Strategic institute program 2003-2007
- 16 MNOK
- Areas of risk
  - Finance and insurance
  - Environment and ecology
  - Disease and health
  - Industrial risk
- Multi-client R&D
- Self-financed R&D

NR Norges forskningsråd

StAR - Statistical Analysis of Risk

- Statistical methodologies
  - Highly structured stochastic systems
  - Survival and event history analysis
  - Modern time series and extreme events
  - Partially specified models
  - Model validation



TuMod - Turbidite Modeling

© Open University
Image courtesy of the Open University

- Sponsors: NFR, ConocoPhillips, Hydro
- Partners: UiB (CIPR) and Complex Flow Design
- Main idea:
- Major challenges:
  - Realistic geometry