Norsk Regnesentral
NORWEGIAN COMPUTING CENTER

www.nr.no

Location Privacy by Design
- Technology & Business Incentives

Dr. Lothar Fritsch

Norsk Regnesentral
Norwegian Computing Center

Oslo

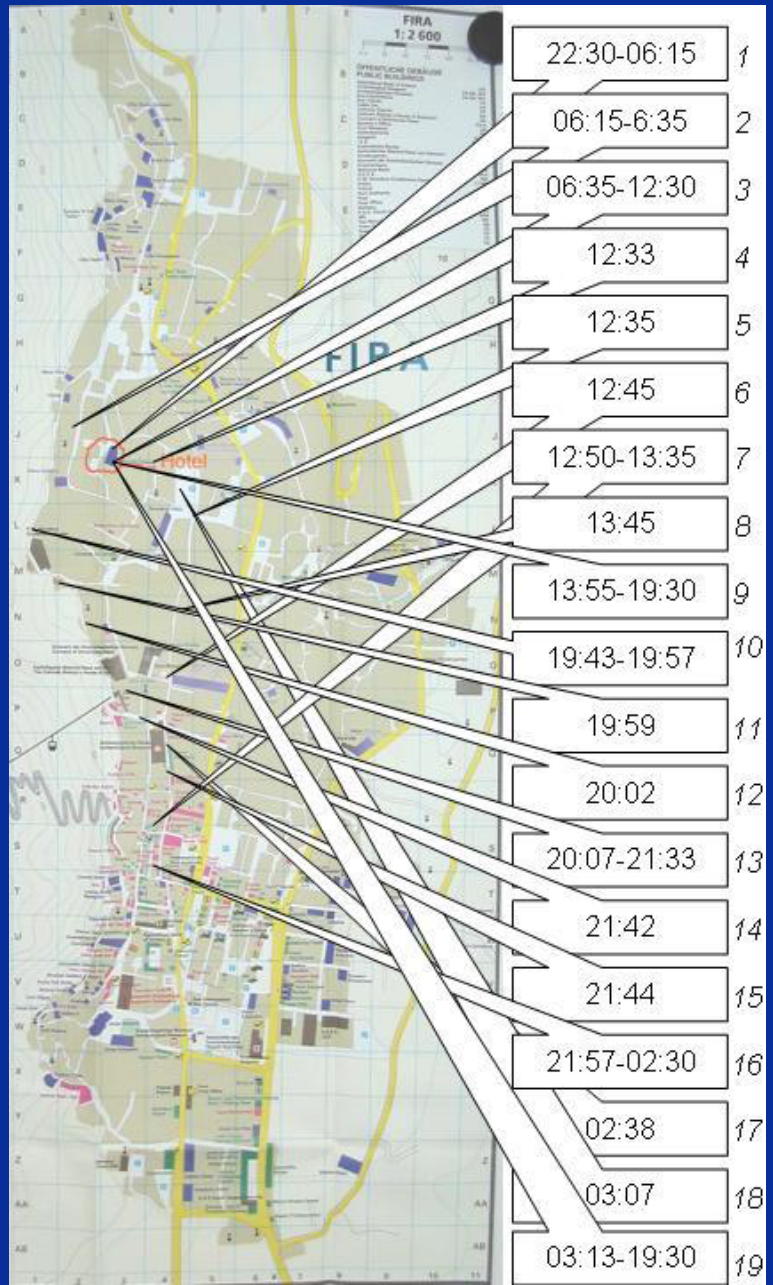
Internetdargana, Stockholm, 26-27.10.2010

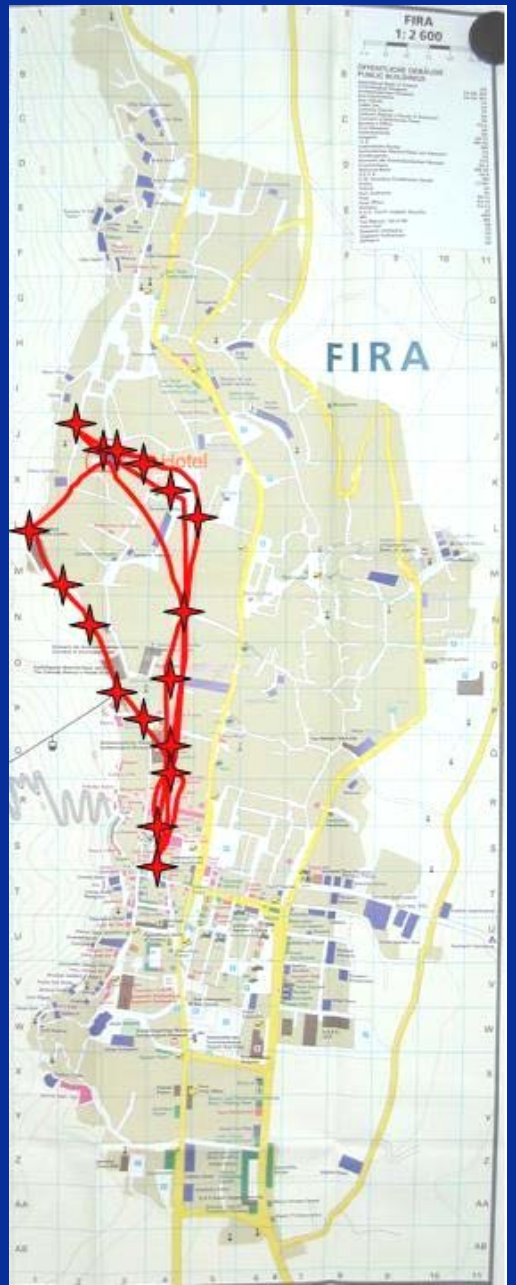
Norsk Regnesentral
NORWEGIAN COMPUTING CENTER

Contents

- Location Privacy
  - Concepts
  - Technology
- Privacy by Design
  - Planning vs. Patching
  - Design Process
- Business Incentives for Privacy
  - Customer damage is business damage
  - Businesses want privacy, too!

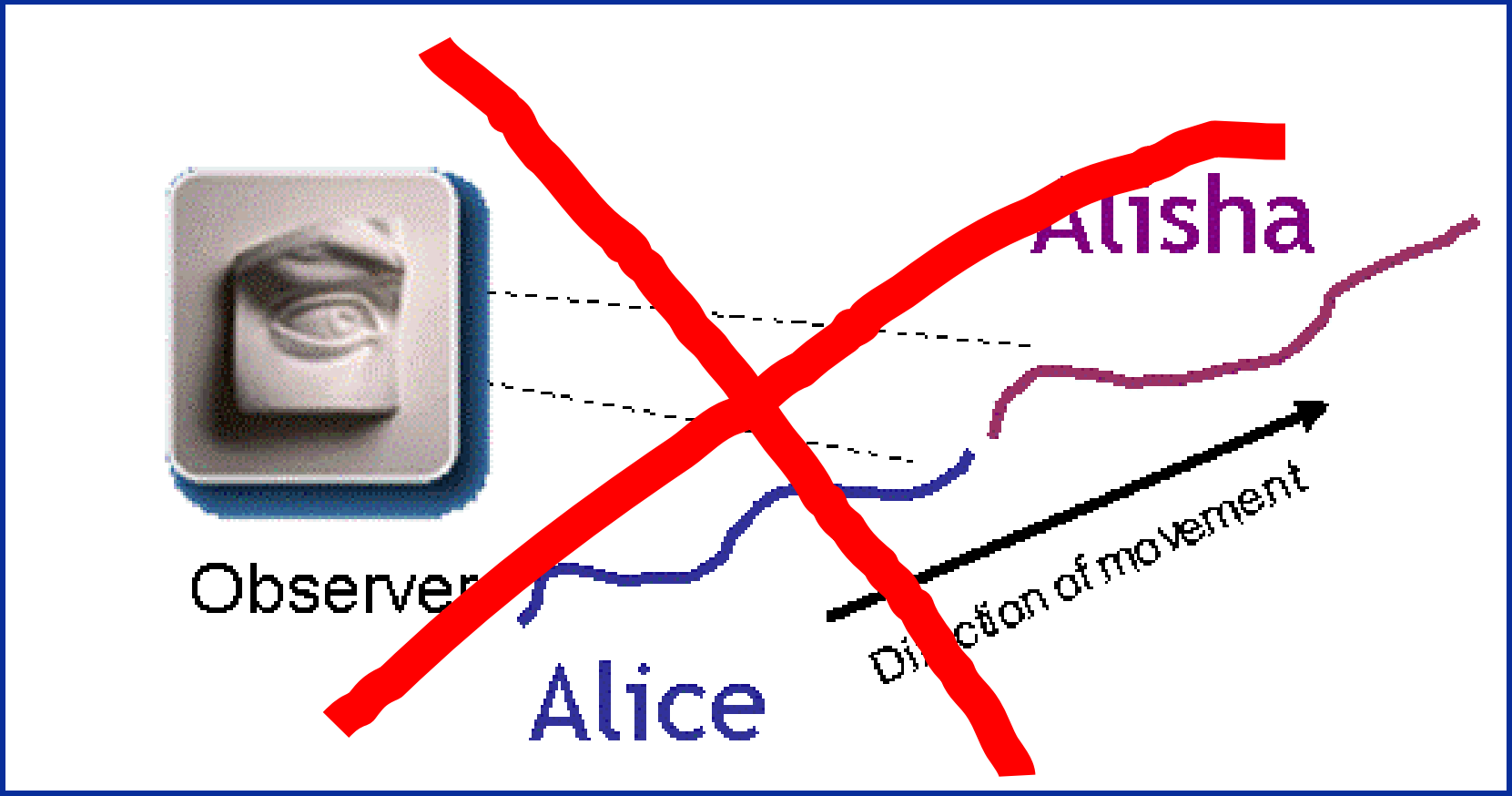

FIRA
1: 2 600
FIRA
Hotel


FIRA
1: 2 600
FIRA
Hotel
22:30-06:15 1
06:15-6:35 2
06:35-12:30 3
12:33 4
12:35 5
12:45 6
12:50-13:35 7
13:45 8
13:55-19:30 9
19:43-19:57 10
19:59 11
20:02 12
20:07-21:33 13
21:42 14
21:44 15
21:57-02:30 16
02:38 17
03:07 18
03:13-19:30 19


FIRA
1: 2 600
FIRA
Hotel

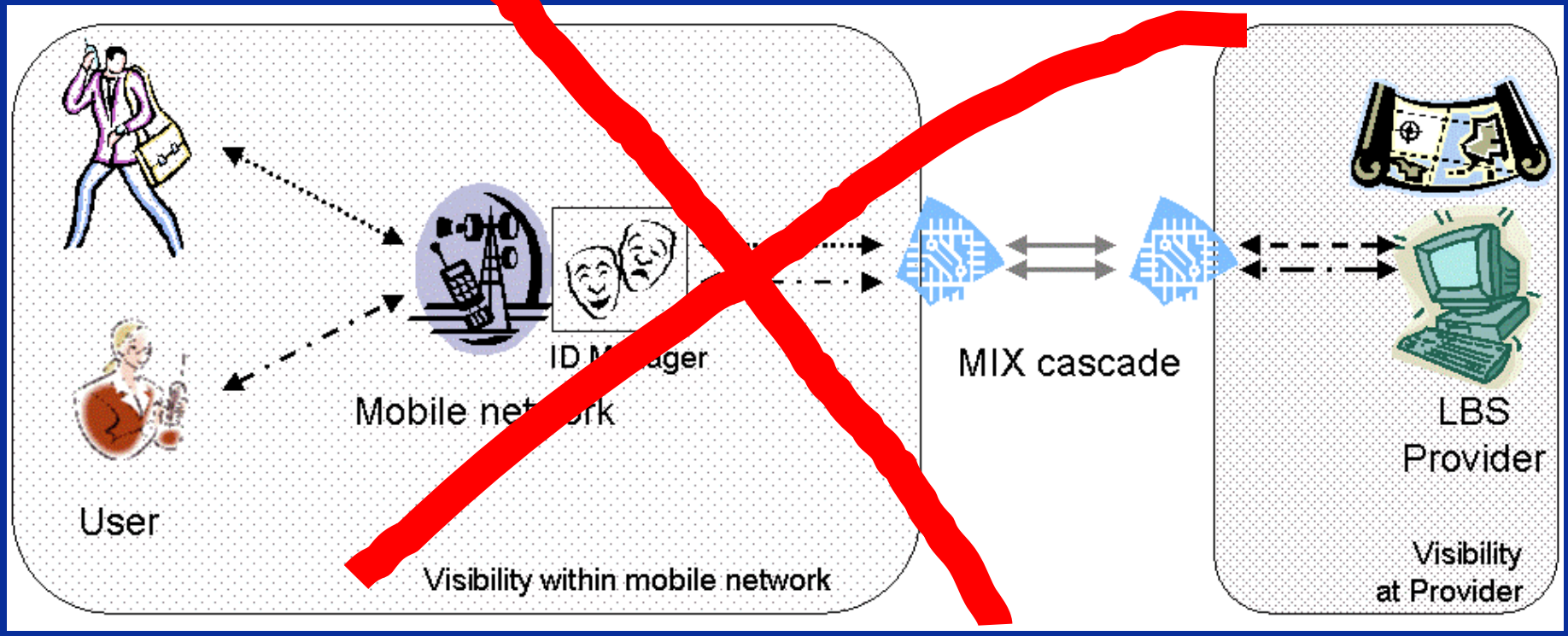
[1]

Simple change of pseudonym?



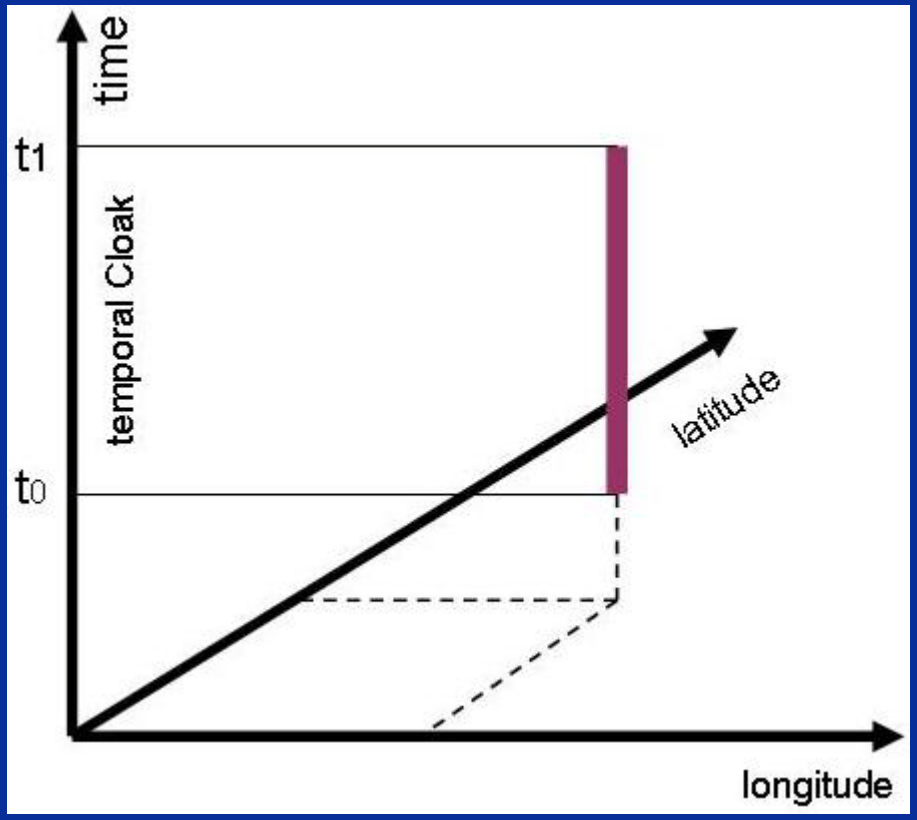
[1]

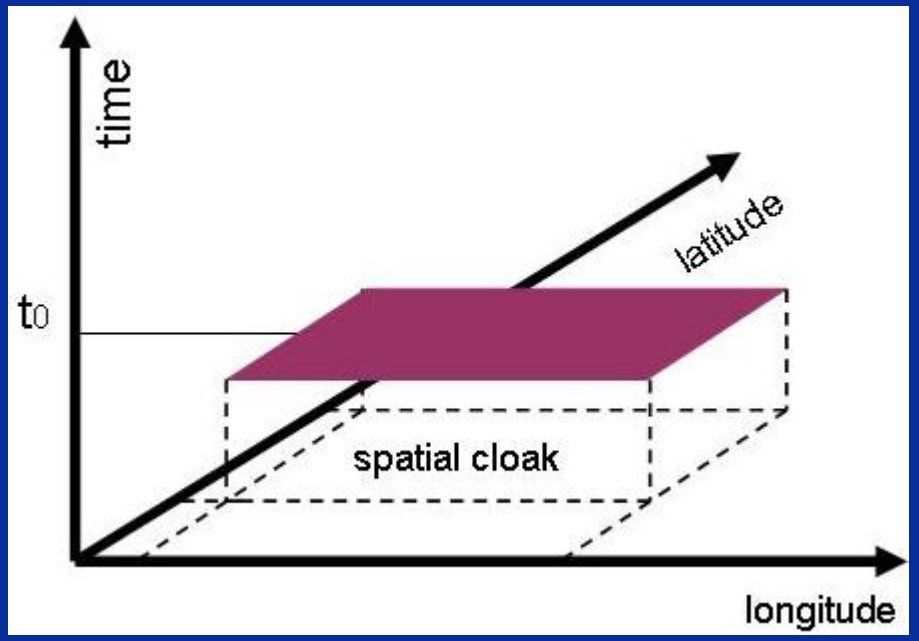
Use of Anonymizers / MIXing / TOR?



[1]

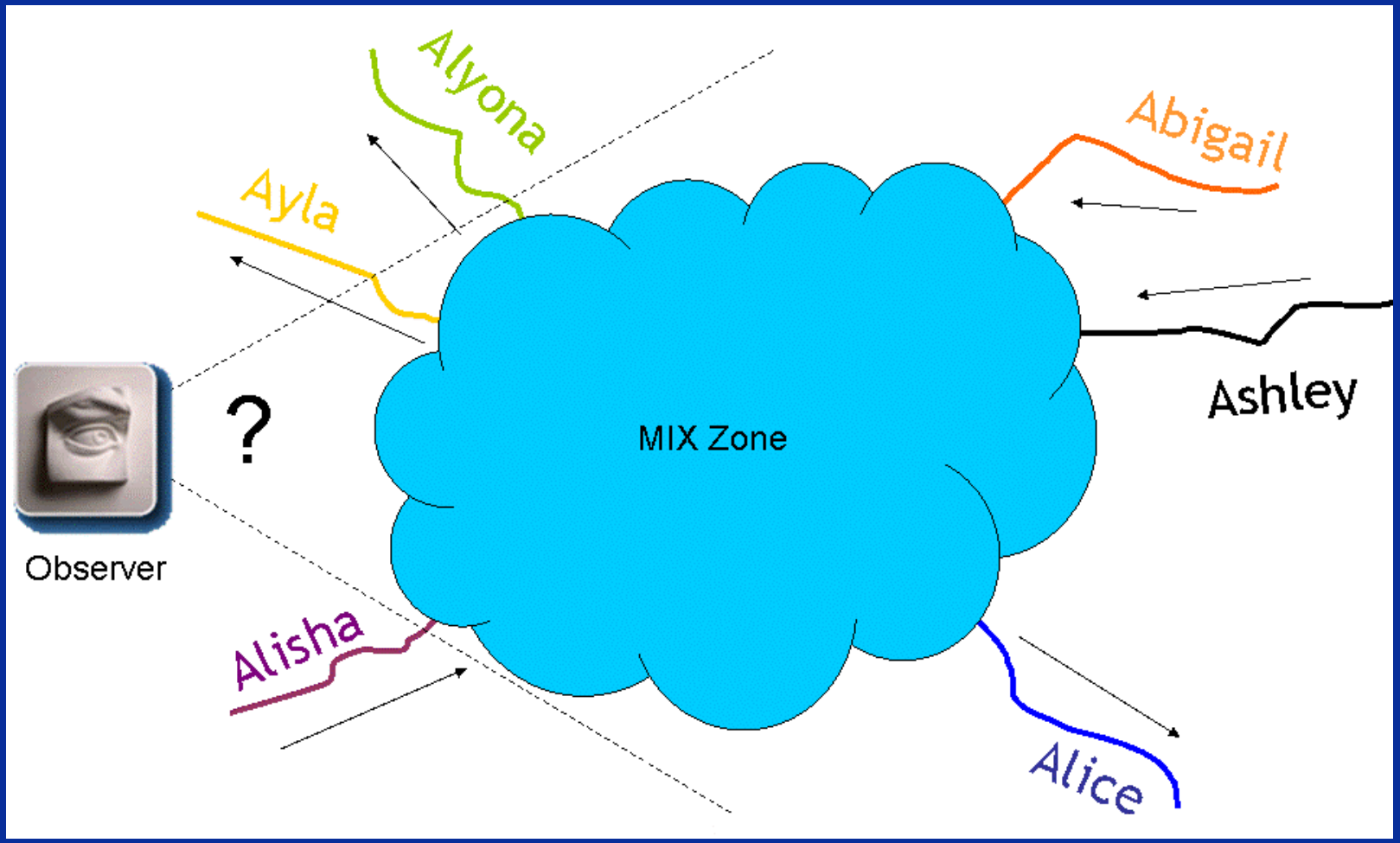
Cloaking in Time and Space





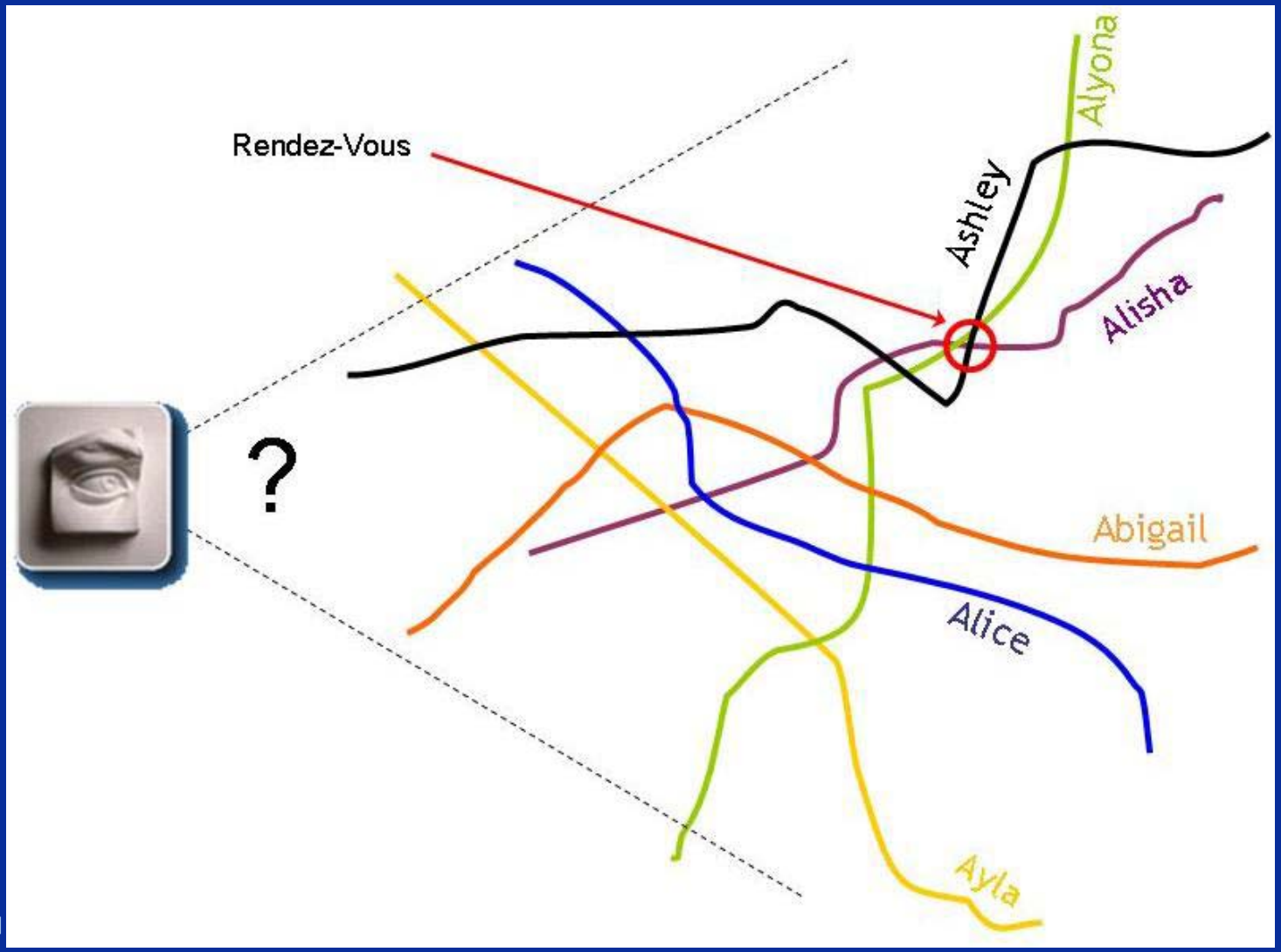
[1]

MIX zoning of users



[1]

Dummy Users as Camouflage

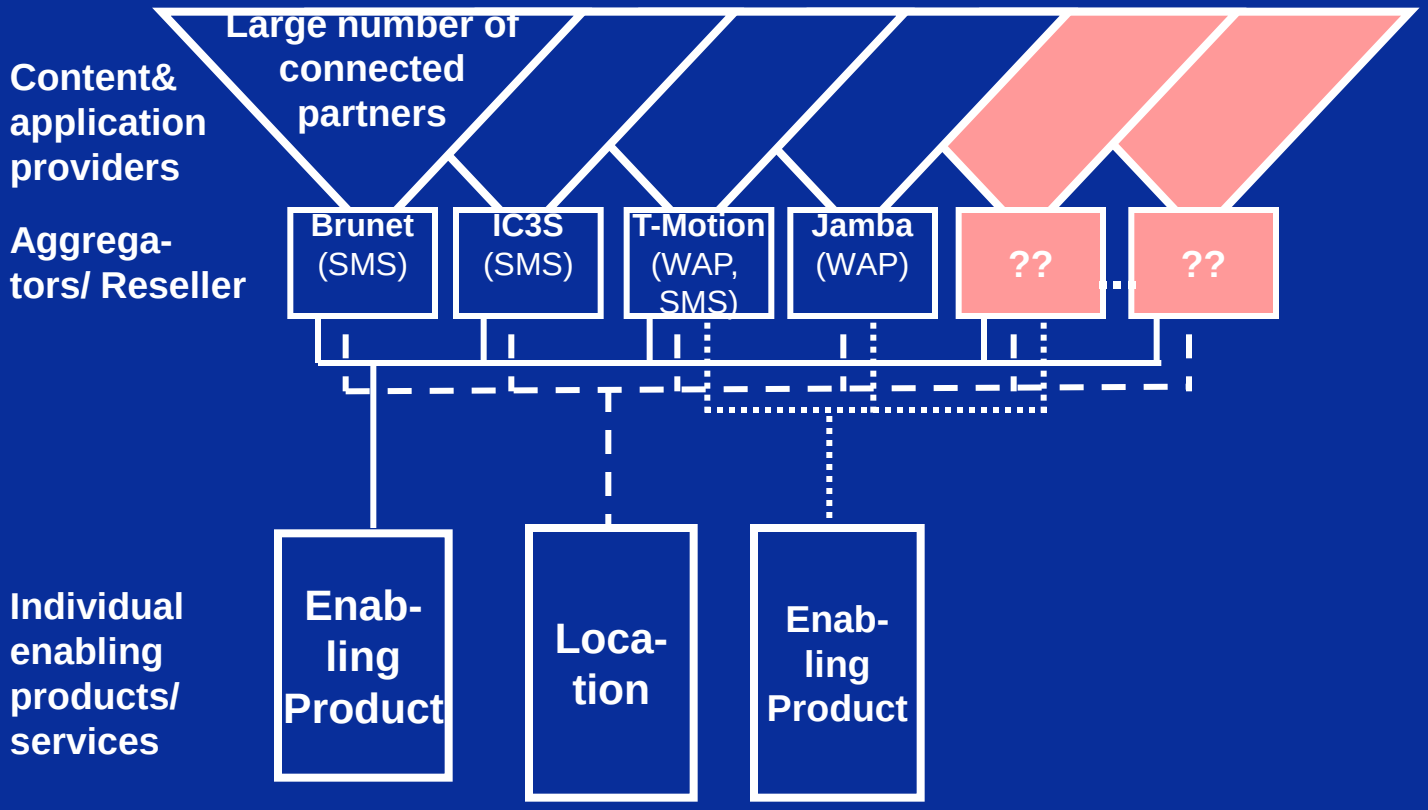


[1]

Two particular solutions

- PRIME LBS prototype for T-Mobile [2]
  - Using a 3rd-party service to separate location data from identity data
  - Creation of 3rd-party LBS supplier IDs
  - Management of user location policies at the location source
- ”Oblivious maps” – anonymous access to mapping [3]
  - Based on ”oblivious transfer” algorithm
  - Basically bundels many user’s access to a mapping service into a batch
  - Cryptographic properties ensure that the mapping server can’t profile users

PRIME: Real-World Reseller business



[7]

PRIME
Privacy and Identity Management for Europe

PRIME: Requirements

- Enable established business models on a secure, privacy-friendly architecture
- Ensure efficiency & economy of the solution
- Enable users to manage policies & their 'online' identities for each service provider and for each usage cycle
- No processing of localizations violates a user's consent
- Hide service usage patterns from observers & infrastructure providers
- Confidentiality of communication content against observers & infrastructure

Business Models & Economic Rationale

Policy Management & Consent Requirements

Privacy Solutions

[7]

PRIME
Privacy and Identity Management for Europe

PRIME: LBS privacy architecture

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

O
LS
IDM

Location Source

policy negotiation
consent

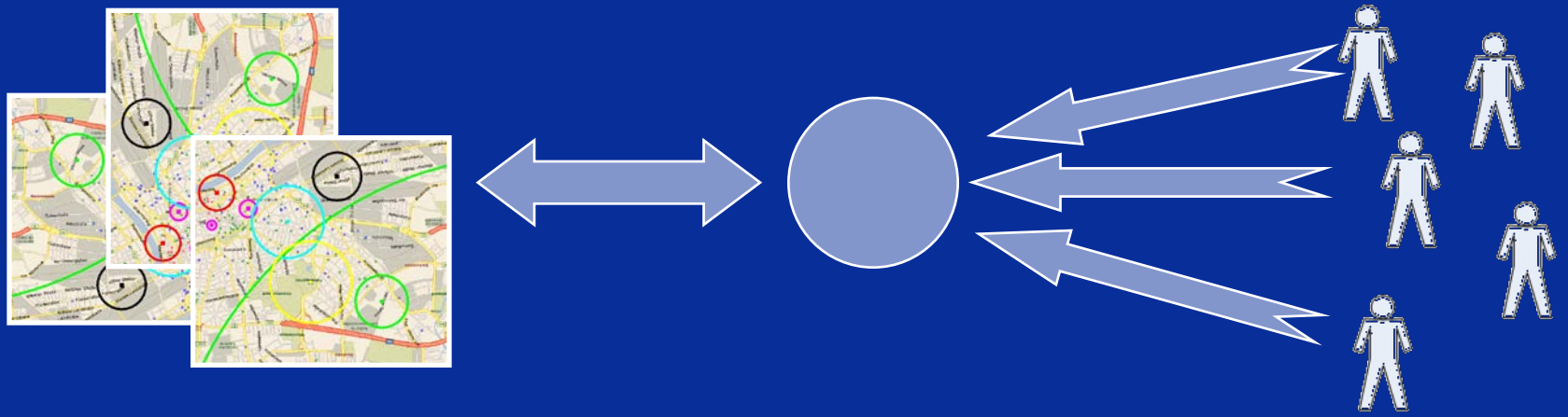
Identity Management System

PRIME
Privacy and Identity Management for Europe

[7]

Oblivious Maps

- Based on ”tiling” of the map structure
- Bundling of requests to tiles through cryptographic methods
- Mapping server always sends a batch of tiles to a number of users through an ”Oblivious transfer” protocol that hides tile receivers



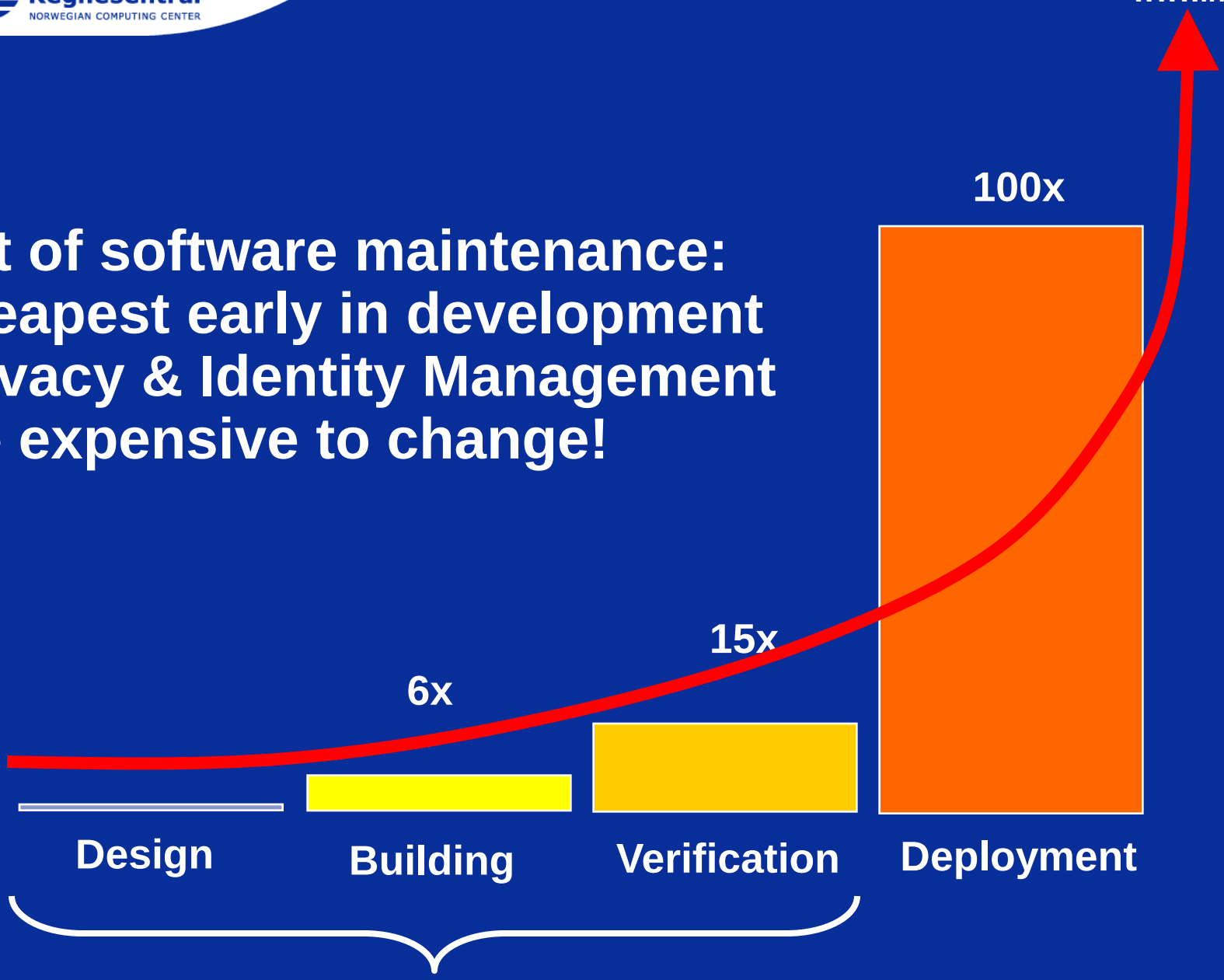
[3]

Norsk Regnesentral
NORWEGIAN COMPUTING CENTER

Contents

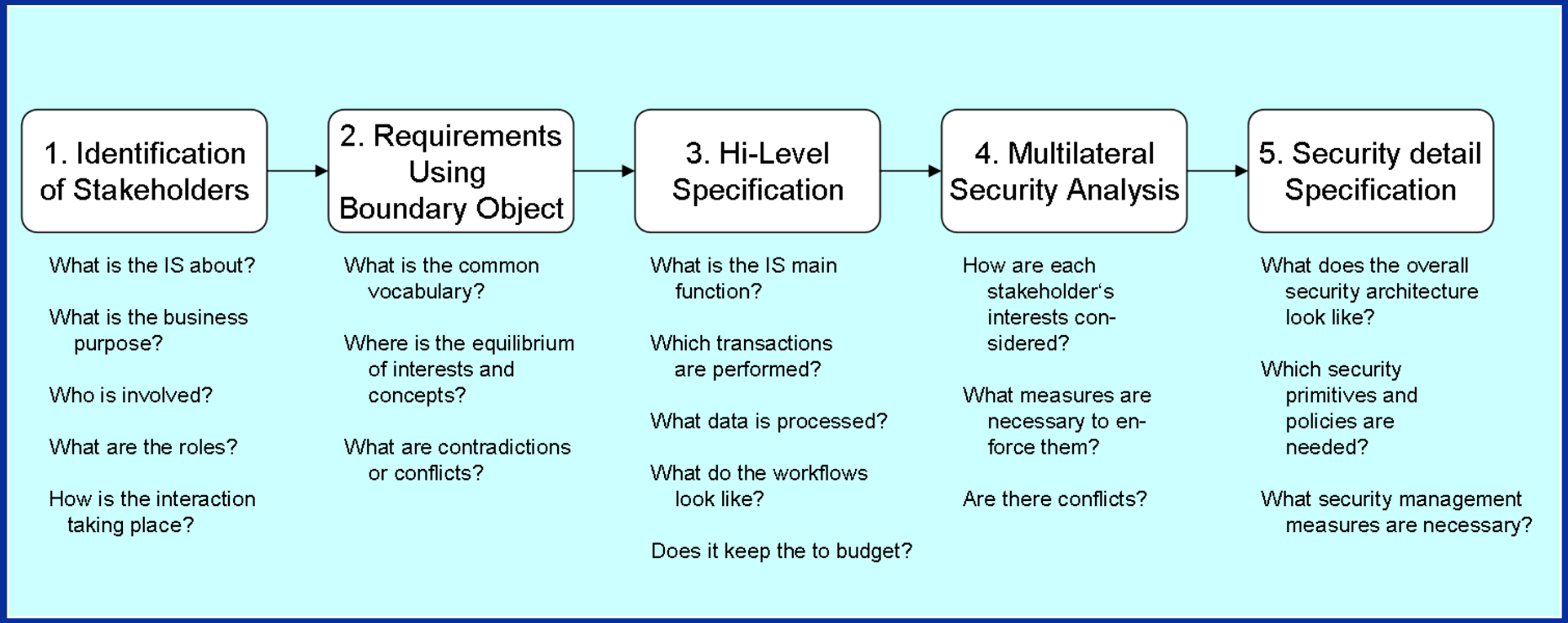
- Location Privacy
  - Concepts
  - Technology
- Privacy by Design
  - Planning vs. Patching
  - Design Process
- Business Incentives for Privacy
  - Customer damage is business damage
  - Businesses want privacy, too!

Cost of software maintenance:
- cheapest early in development
- Privacy & Identity Management are expensive to change!



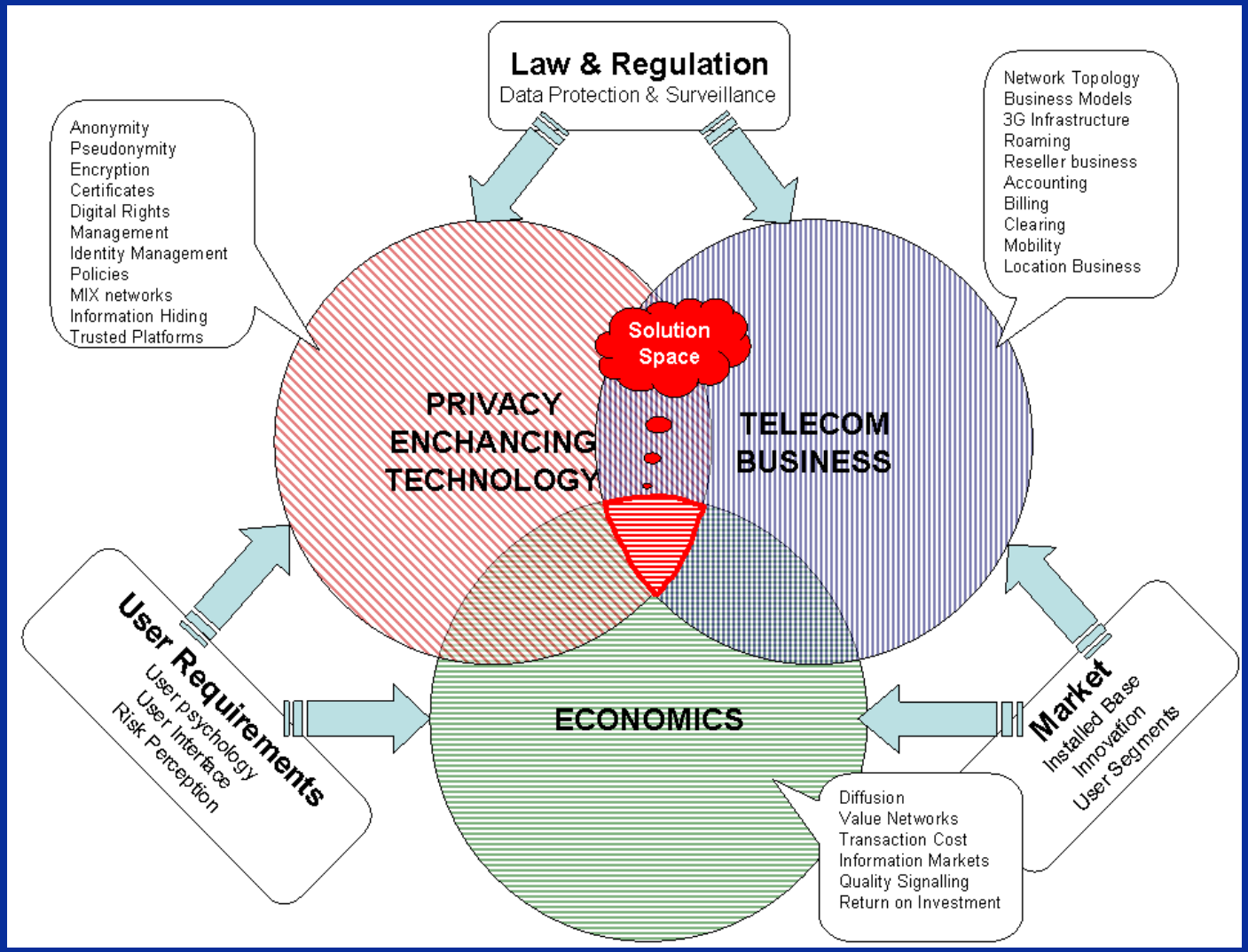
Privacy by Design provides cheaper results

Privacy by Design



[4]

Find a stakeholder consensus!



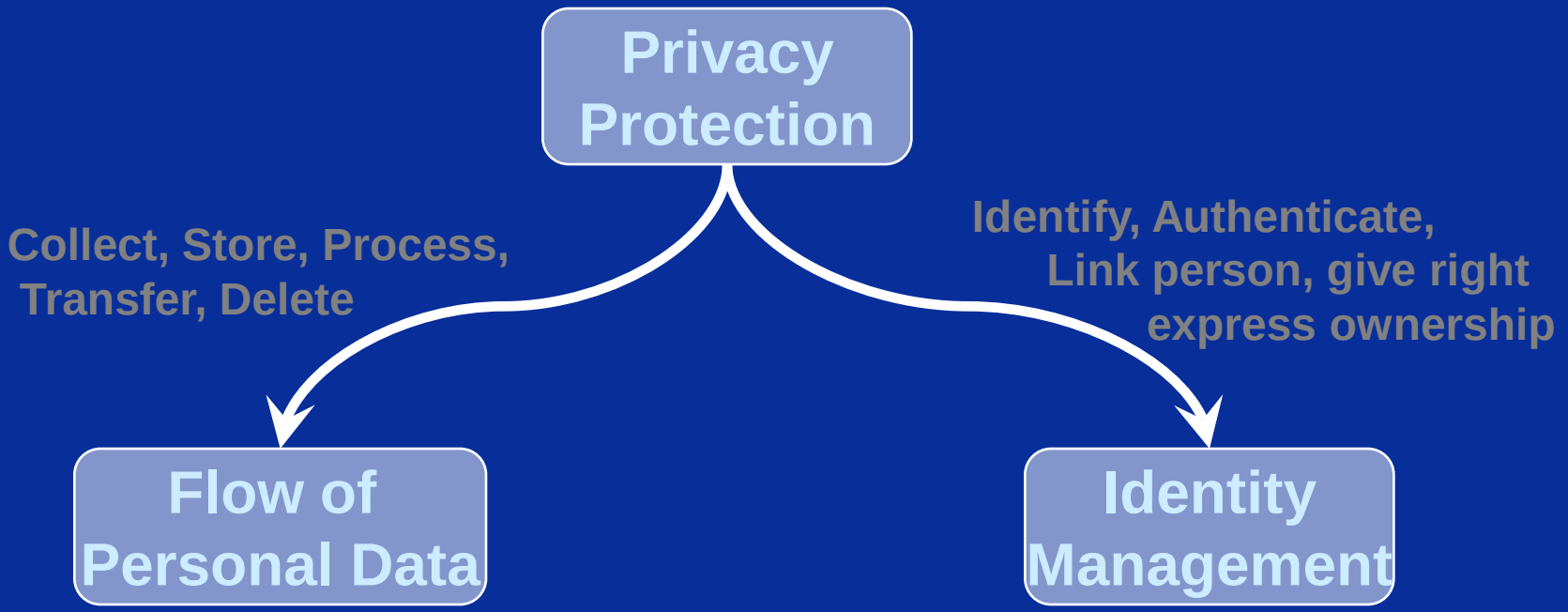
[4]

Norsk Regnesentral
NORWEGIAN COMPUTING CENTER

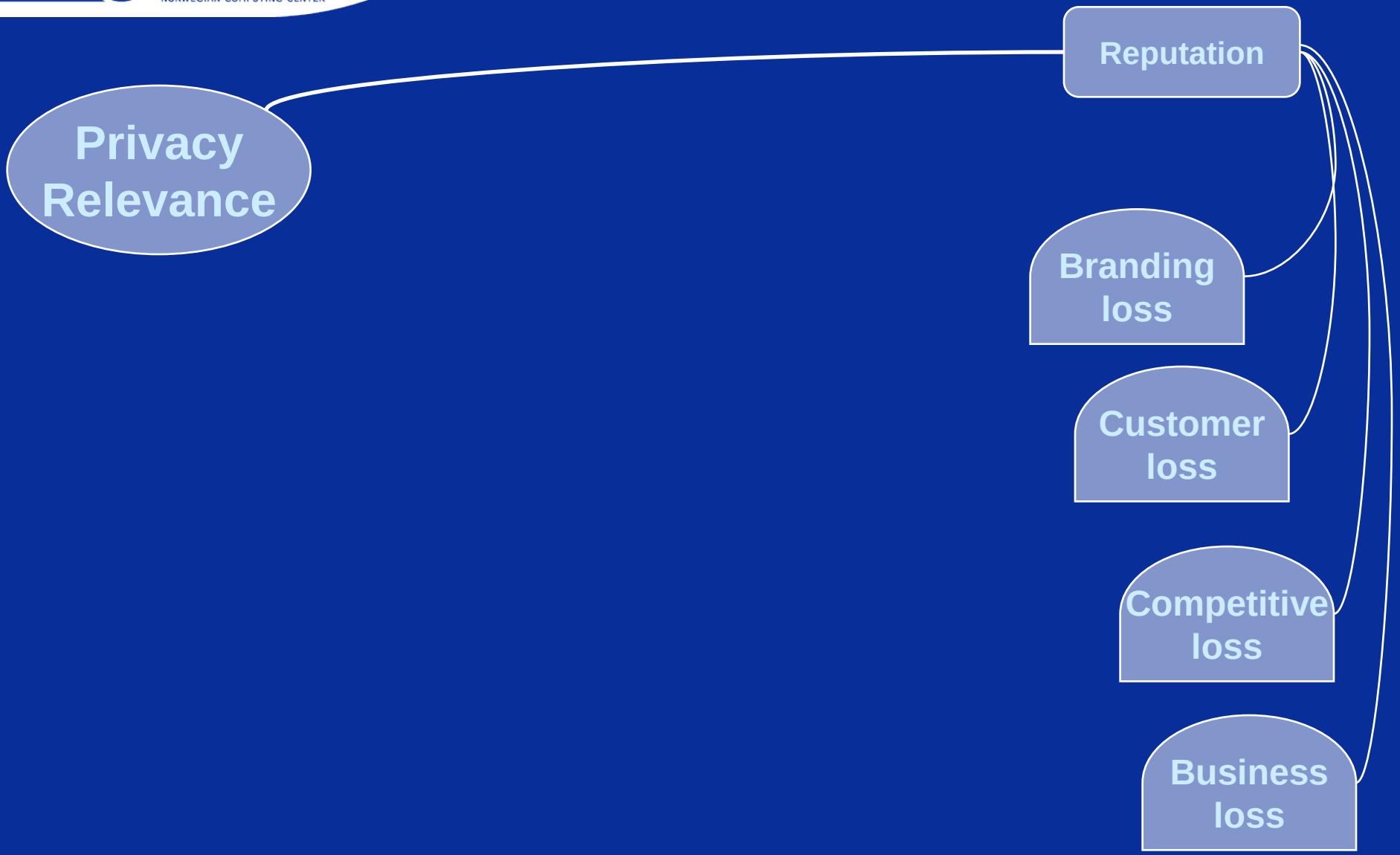
Contents

- Location Privacy
  - Concepts
  - Technology
- Privacy by Design
  - Planning vs. Patching
  - Design Process
- Business Incentives for Privacy
  - Customer damage is business damage
  - Businesses want privacy, too!

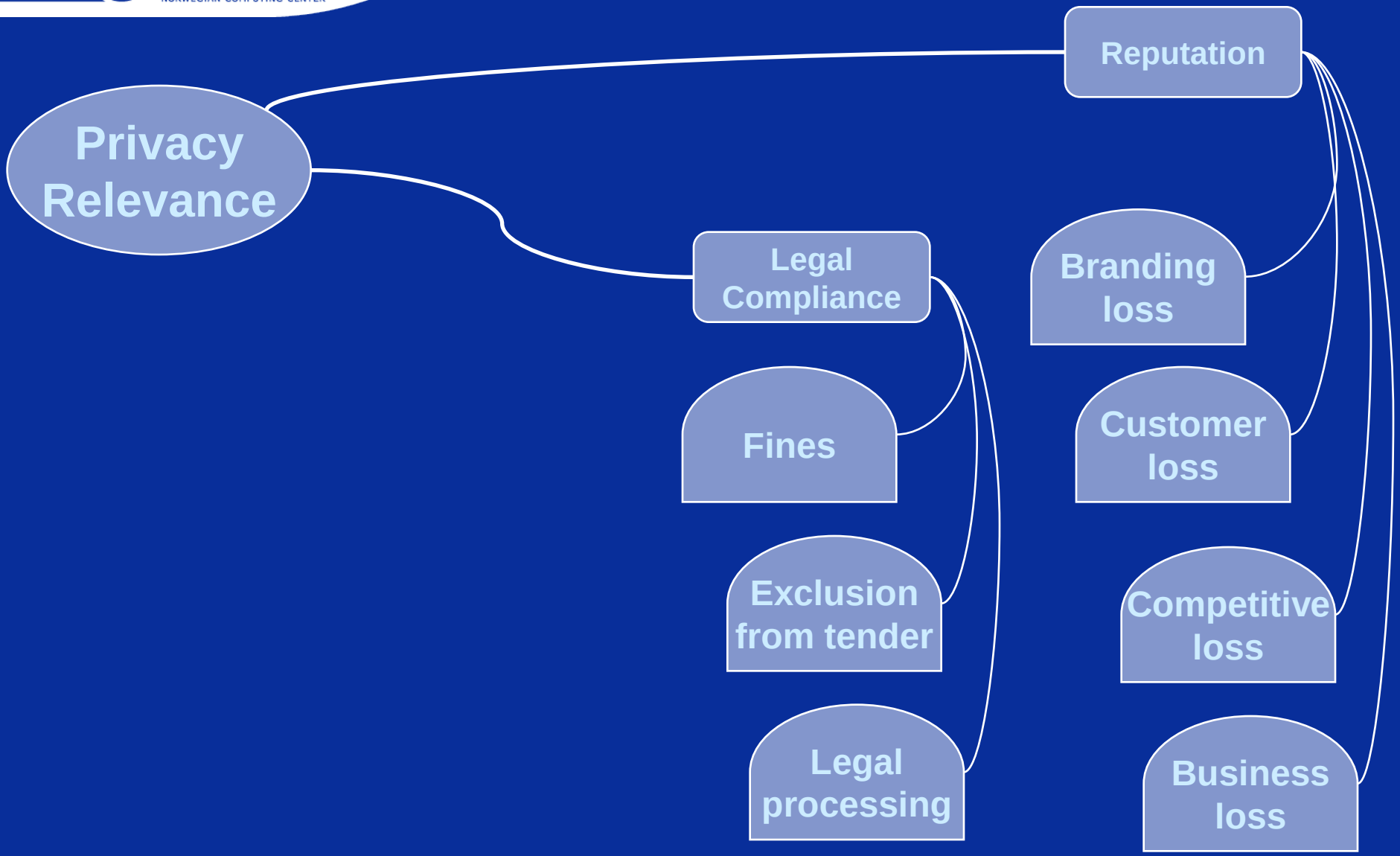
Privacy Protection in IT



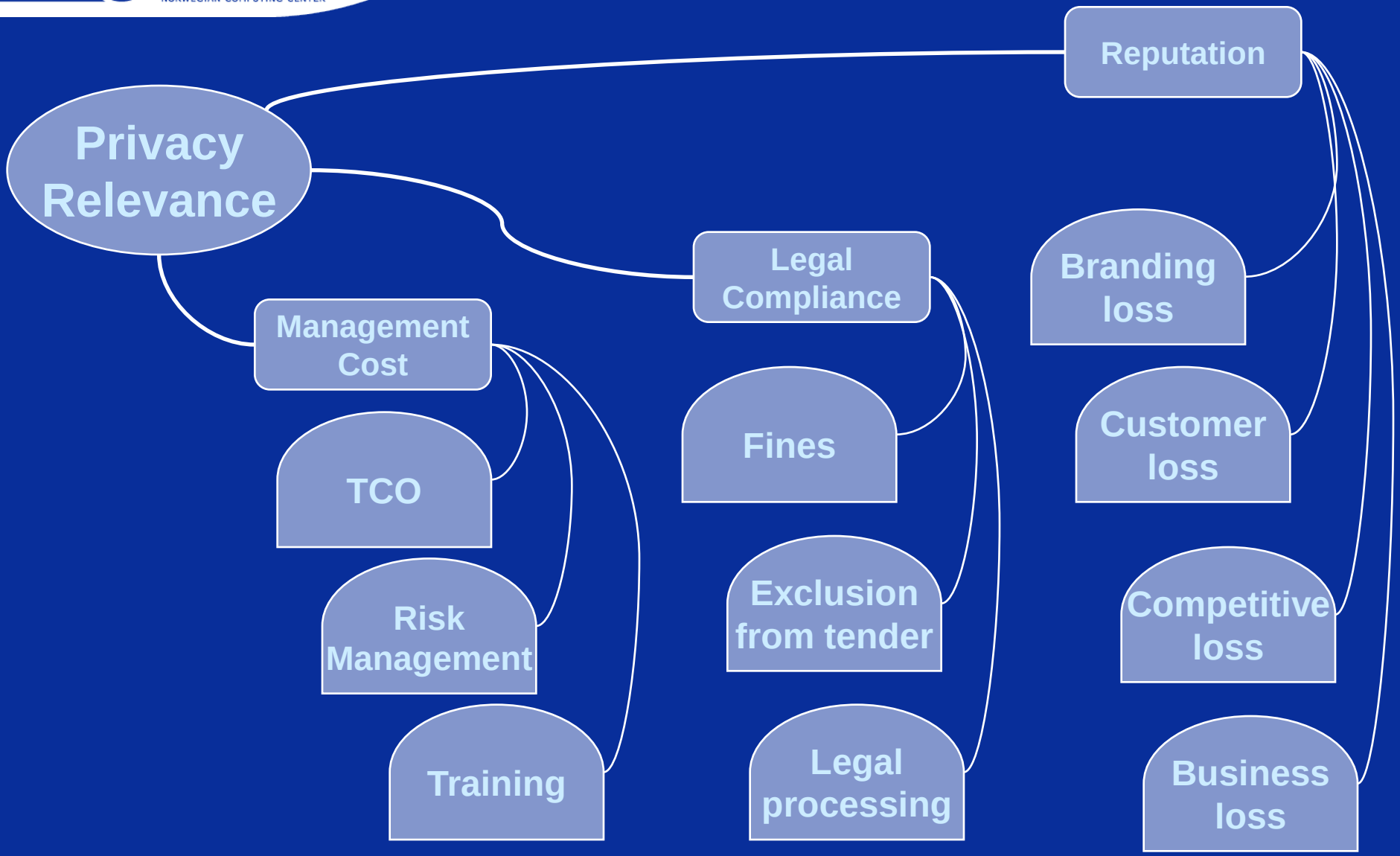
[6]


Reputation
Privacy Relevance
Branding loss
Customer loss
Competitive loss
Business loss

[6]

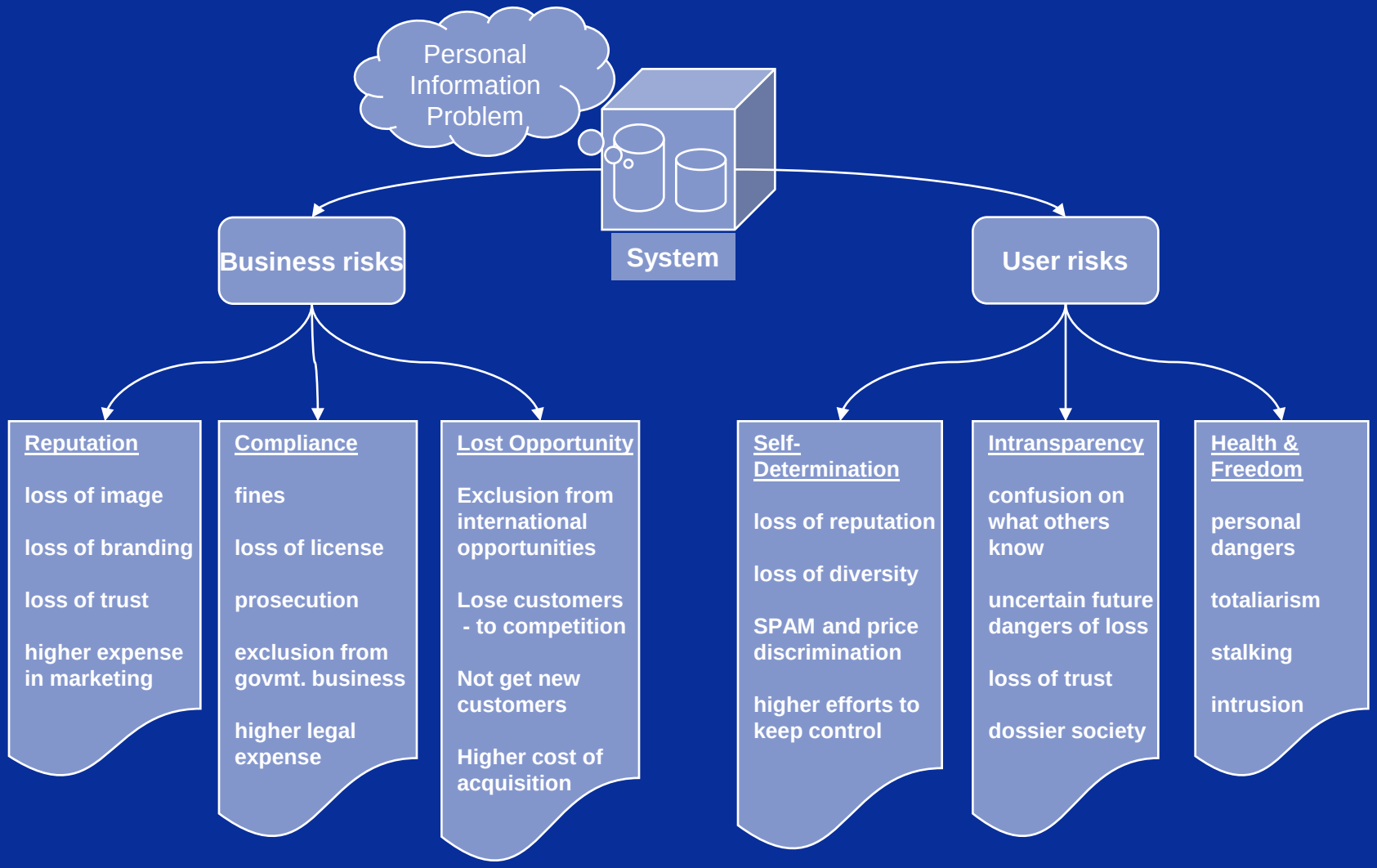

Reputation
Privacy Relevance
Legal Compliance
Branding loss
Fines
Customer loss
Exclusion from tender
Competitive loss
Legal processing
Business loss

[6]


Reputation
Privacy Relevance
Legal Compliance
Branding loss
Management Cost
Fines
Customer loss
TCO
Exclusion from tender
Competitive loss
Risk Management
Legal processing
Business loss
Training

[6]

Duality of Privacy Risks



[6]

Businesses need privacy, too.

- Or… bad things might happen anytime soon…

The Boycott Pho

Web community

3G data connection

Supermarket cart

[5]

RFID future uses – the two-edged sword [5]

Imagine a world where…

- A vendor's trash (packages, products) will be tracked around the globe, even 20 years after production, until it turns up on a polluted site in Africa – and on some NGO's agenda;
- The city trash removal facilities read RFIDs on package waste to bill the producers for the trash processed;
- Corporate tax & toll is adjusted based on scanners at borders, ware houses and waste dumps.
- Does the "kill" function kill TID tag serial numbers?

Privacy by Design Instruments

System Environment Analysis Instrument	Privacy Impact Analysis Instrument	Counter-measures Instrument	Total Cost of Ownership Instrument	Design & Deployment Instrument
Legal frame Technical frame User requirements Business Models	Threats to privacy Threat impact model Impact analysis	Catalog of protection PET catalog Insurance coverage Hope & Pray	Model of cost, Effectiveness and efficiency of privacy protection Abstraction of PET into function, price and QoS	Business process model Life cycle Best practices Assurance

Further reading

[1] 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.

[2] Zibuschka, Jan; Fritsch, Lothar; Radmacher, Mike; Scherner, Tobias und Rannenberg, Kai (2007) Privacy-Friendly LBS: A Prototype-supported Case Study, 13th Americas Conference on Information Systems (AMCIS), Keystone, Colorado, USA,.

[3] Kohlweiss, Markulf; Gedrojc, Bartek; Fritsch, Lothar und Preneel, Bart. (2007) Efficient Oblivious Augmented Maps: Location-Based Services with a Payment Broker, in: N. Borisov und P. Golle (Eds.): Privacy Enhancing Technologies, 7th International Symposium, PET 2007 (LNCS 4776), Berlin, Springer, pp. 77-94.

[4] Fritsch, Lothar (2007) Privacy-Respecting Location-Based Service Infrastructures: A Socio-Technical Approach to Requirements Engineering, Journal of Theoretical and Applied E-Commerce research (2:3), pp. 1-17.

[5] Fritsch, Lothar. (2009) Business risks from naive use of RFID in tracking, tracing and logistics, in: VDE Verlag GmbH (Eds.): RFID SysTech 2009 - ITG Fachbericht 216, 16.Jun. 2009, Berlin, pp. ch. 7.

[6] 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-2008, Bonn, Gesellschaft für Informatik, pp. 1-15

[7] Jan Camenisch, Lothar Fritsch, Markulf Kohlweiss, Mike Radmacher, and Dieter Sommer: LBS Application Prototype, “Requirements and Concepts”, PRIME internal presentation, 2005

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