Investing in Privacy Protection with Privacy-Enhancing Technology

Nova Gorica, Slovenia, 11. 6. 2008

Lothar Fritsch

Norwegian Computing Center, Oslo

Norsk Regnesentral
NORWEGIAN COMPUTING CENTER

INFOSEK 2008 – FORUM Conference

PALSIT

enisa
European Network and Information Security Agency

ICT Research at Norwegian Computing Center

Security

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

Multimedia multichannel

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

e-Inclusion

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

Norsk Regnesentral
NORWEGIAN COMPUTING CENTER

Department f. Applied Research in ICT

INFOSEK 2008 – FORUM Conference

PALSIT

Lothar Fritsch

Research Scientist in IT Security & Privacy in Norsk Regnesentral's ICT research department DART

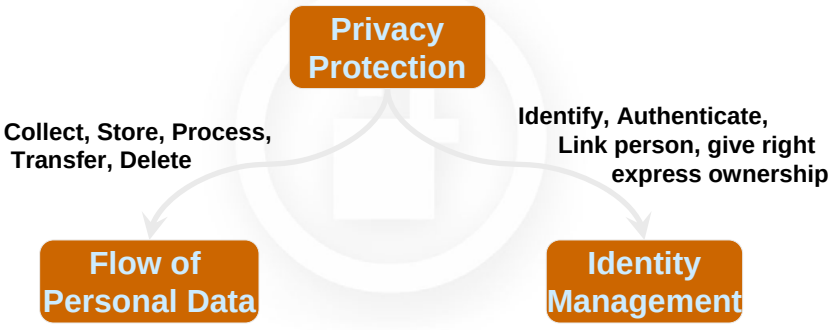
Masters degree in computer science from University of Saarland

Graduate studies at Frankfurt's Goethe University's Information Systems department

Industry experience in IT security product management

Participant in EU PET research, e.g. SEMPER, PRIME, FIDIS

Privacy Protection in IT

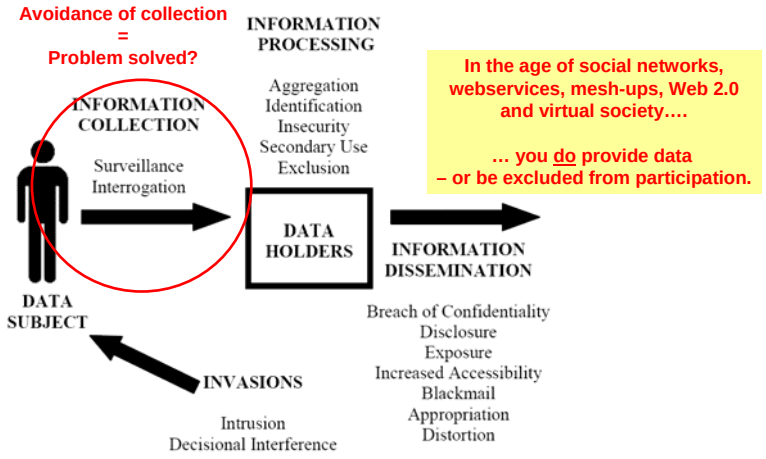


Legal view: Fundamental Principles

- 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.

J. Borking, PETweb project, NR, Oslo, Norway

Solove's privacy threat taxonomy

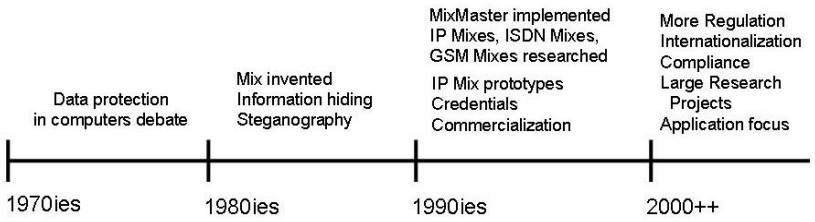


In the age of social networks, webservices, mesh-ups, Web 2.0 and virtual society....

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

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

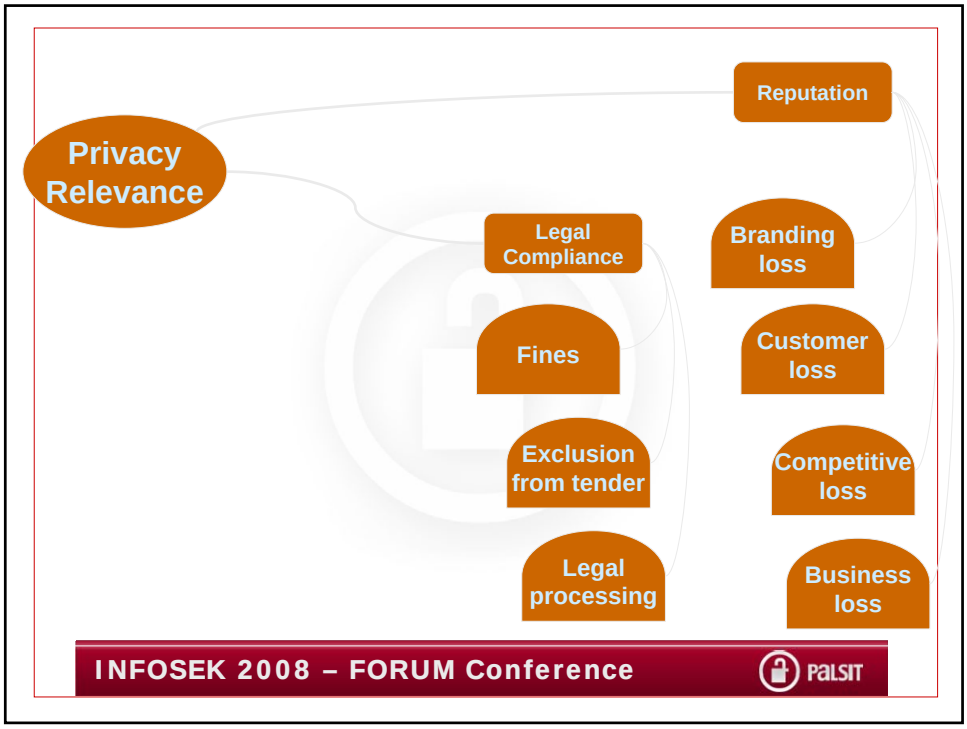
A brief history of PET

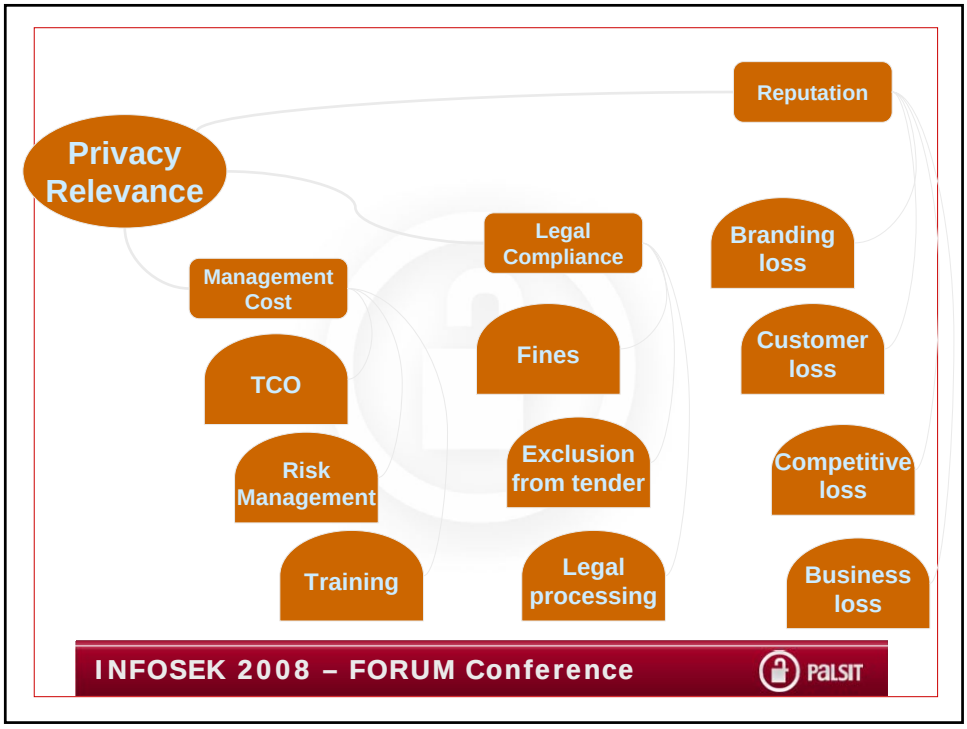


- PET development inspired by the legal perspective on basic human rights.
- PET research focused on information hiding & control
- Technology-centric approach

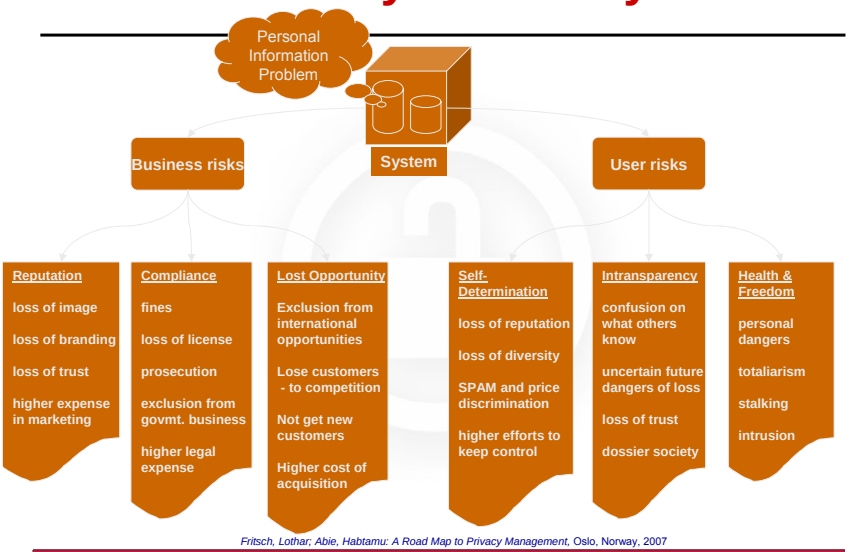
But there is a lack of deployed PETs in the ”real world”. Why?

INFOSEK 2008 – FORUM Conference PALSIT


Privacy Relevance
Reputation
Legal Compliance
Branding loss
Fines
Customer loss
Exclusion from tender
Competitive loss
Legal processing
Business loss
INFOSEK 2008 – FORUM Conference
PALSIT


Privacy Relevance
Reputation
Legal Compliance
Branding loss
Management Cost
TCO
Fines
Customer loss
Risk Management
Exclusion from tender
Competitive loss
Training
Legal processing
Business loss
INFOSEK 2008 – FORUM Conference
PALSIT

Duality of Privacy Risks

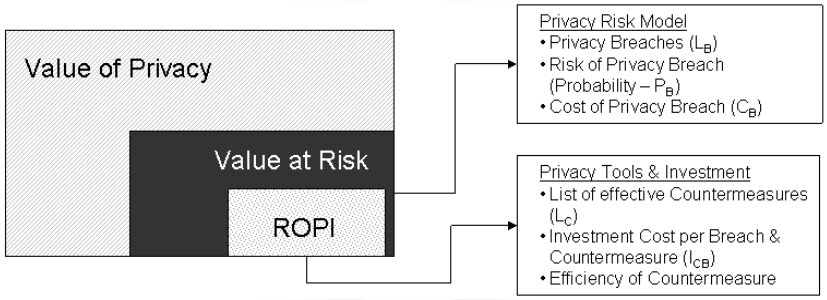


Fritsch, Lothar, Abie, Habtamu: A Road Map to Privacy Management, Oslo, Norway, 2007

Technology view: PETs

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

Business view:
Return On Privacy Investment ROPI



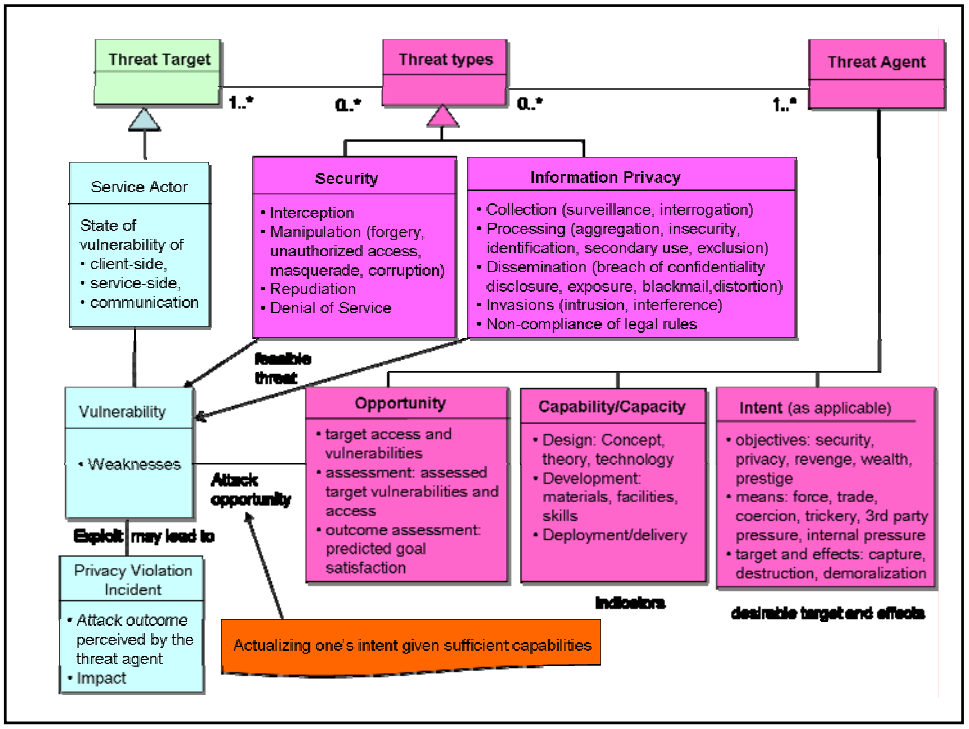
Fritsch, Lothar und Abie, Habtamu. (2008) A Road Map to the Management of Privacy Risks in Information Systems, in: Gesellschaft f. Informatik (GI) (Eds.): *Konferenzband Sicherheit 2008, Lecture Notes in Informatics LNI 128,* 2-Apr-2007, Bonn, Gesellschaft für Informatik, pp. 1-15.

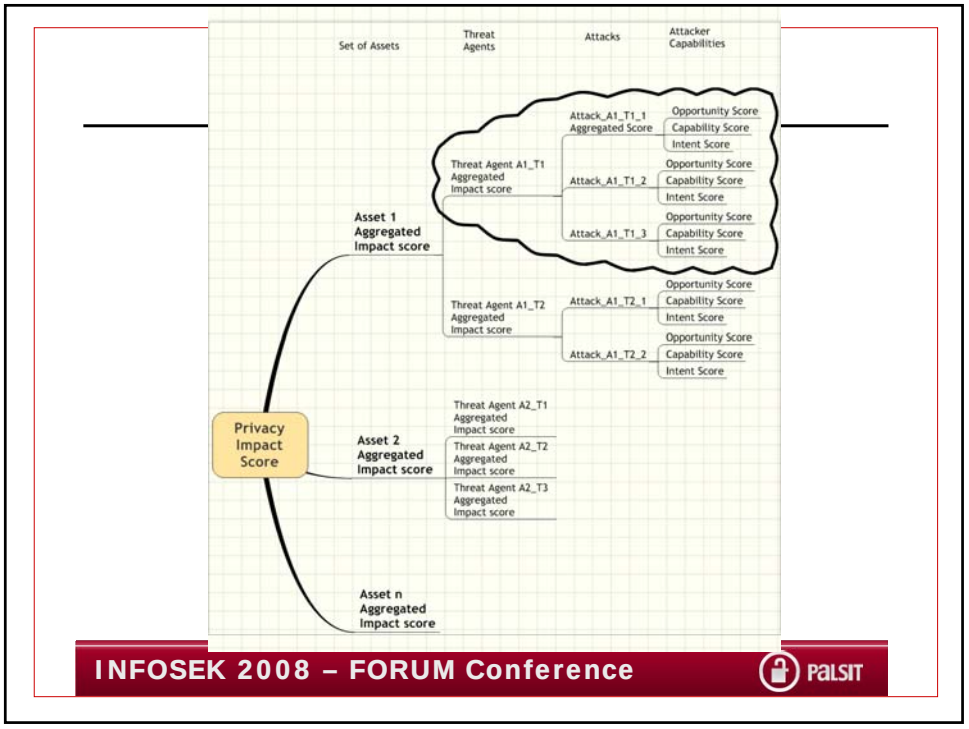
Fritsch, Lothar: Return on Privacy Investment Scheme, Oslo, Norway, 2007

Privacy Investment Decision 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

What is the system about? → Where are the problems? → What can be done? → What can we afford? → How will it be put in place?


Threat Target
Threat types
Threat Agent
1..*
0..*
0..*
1..*
Service Actor
State of vulnerability of
• client-side,
• service-side,
• communication
Security
• Interception
• Manipulation (forgery, unauthorized access, masquerade, corruption)
• Repudiation
• Denial of Service
Information Privacy
• Collection (surveillance, interrogation)
• Processing (aggregation, insecurity, identification, secondary use, exclusion)
• Dissemination (breach of confidentiality disclosure, exposure, blackmail,distortion)
• Invasions (intrusion, interference)
• Non-compliance of legal rules
feasible threat
Vulnerability
• Weaknesses
Opportunity
• target access and vulnerabilities
• assessment: assessed target vulnerabilities and access
• outcome assessment: predicted goal satisfaction
Capability/Capacity
• Design: Concept, theory, technology
• Development: materials, facilities, skills
• Deployment/delivery
Intent (as applicable)
• objectives: security, privacy, revenge, wealth, prestige
• means: force, trade, coercion, trickery, 3rd party pressure, internal pressure
• target and effects: capture, destruction, demoralization
Attack opportunity
Exploit may lead to
Privacy Violation Incident
• Attack outcome perceived by the threat agent
• Impact
Actualizing one's intent given sufficient capabilities
Indicators
desirable target and effects


Set of Assets
Threat Agents
Attacks
Attacker Capabilities
Privacy Impact Score
Asset 1 Aggregated Impact score
Asset 2 Aggregated Impact score
Asset n Aggregated Impact score
Threat Agent A1_T1 Aggregated Impact score
Threat Agent A1_T2 Aggregated Impact score
Threat Agent A2_T1 Aggregated Impact score
Threat Agent A2_T2 Aggregated Impact score
Threat Agent A2_T3 Aggregated Impact score
Attack_A1_T1_1 Aggregated Score
Attack_A1_T1_2
Attack_A1_T1_3
Attack_A1_T2_1
Attack_A1_T2_2
Opportunity Score
Capability Score
Intent Score
INFOSEK 2008 – FORUM Conference
PALSIT

	A	B	C	D	E	F	G	H	I	J	K	L	M	N
1	ber	Asset Name		Individual	Asset Weight	**Contrib. to system Rating**								
2	1	**End User (EU)**		**100**	14,00 %	**14**								
3														
4			**max-tas**	**avg-tas**	sum-tas									
5		Threat Agent type		Impact Score	Threat Weight	Threat weighted Score								
6		Hacker threats		5,00	20	100								
7		Impact scores:	max	avg	sum(avg)									
8			5,00	5,00	15,00									
9														
10		Threat Description												
11		This measures to what extent a Hacker is a threat to the User Agent and the information on it.												
12														
13			**Attacks originating from a Hacker**											
14			Social engineering				Spoofing				Eavesdropping			
15		result (floored to 5)	5,00	5,00			5,00	5,00			5,00	5,00		
16			max	avg			max	avg			max	avg		
17		- Attack Properties												
18		Automated/manual A1	1,00	1,00	handle with care!		1,00	1,00	handle with		1,00	1,00	handle	
19		Active/passive A2	1,00	1,00	0,1 - 2,0		1,00	1,00	0,1 - 2,0		1,00	1,00	0,1 - 2,0	
20		(Logical/physical)	1	1			1	1			1	1		
21		(Internal/external)	1	1			1	1			1	1		
22														
23		- Threat Agent Properties	4	2,16	54		3,2	2,24	56,1		3,2	2,24	56,1	
24			max	avg	sum		max	avg	sum		max	avg	sum	
25		**Intent**	4	2,8	14		4	3	15		4	3	15	
26		Profit orientation	1				4				4			
27		Revenge	4				2				2			
28		Vandalism	4				4				4			
29		Ego	4				2				2			
30		Curiosity	1				3				3			
31														
32		**Capabilities**	4	3,2	16		4	3,6	18		4	3,6	18	
33		Time ressources	3				4				4			
34		Education / Knowledge	4				4				4			
35		Financial resources	1				3				3			
36		Equipment	4				3				3			
37		Skills	4				4				4			
38														
39		**Opportunity**	5	3,6	18		4	3,4	17		4	3,4	17	
40		Target Access	5				4				4			
41		Target Vulnerabilities	3				3				3			
42		Assessed Target weakness	3				4				4			
43		Expected attack value / gain	3				2				2			
44		Chance of not being caught	4				4				4			
45														
46			MAX	AVG			MAX	AVG			MAX	AVG		
47		Consequence/Outcome	4,5	2,3125			4	2,3125			4	2,3125		
48			max	avg			max	avg			max	avg		
49		- Security Privacy	4	2,25			3	2			3	2		
50		Interception	1				2				2			
51		Manipulation	3				3				3			
52		Denial of service	4				1				1			
53		Repudiation	1				2				2			
54														
55		- Information Privacy	5	2,375			5	2,625			5	2,625		
56		**Information collection**												
57		Surveillance	4		fine		2				2			

Drawbacks

Lack of quantified data (cost & occurence of incidents, effectivity & cost of PET)

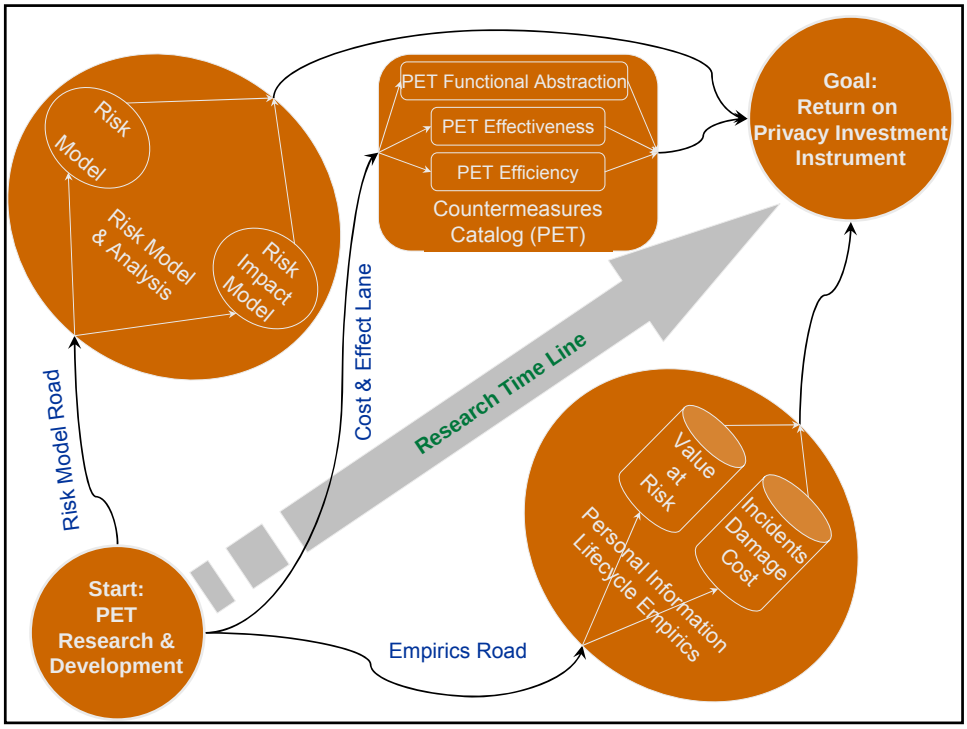
Lack of long-term privacy risk model (duality!)

Much "expert guessing" necessary

- Good for expert's hourly rates
- Bad for scientific accuracy

Good for scientists:

- More research necessary



Summary

- Privacy management is part of IT management
- Privacy-enhancing technology is available
- Some of the business implications are not well researched

References

The PETweb project: http://petweb.nr.no

State of the Art of Privacy-enhancing Technology: http://publ.nr.no/4589

Contact & Project Interests

Application and Management of Privacy-Enhancing Technology (PET)

Location-based Services, Location-sensitive Applications, and their Privacy Properties

Multimedia Security, Rights Management, and Media Handling

Sensor Networks and Security

Security Analysis & Verification

Security Usability & E-Inclusion