Towards a Research Road Map for the Management of Privacy Risks in Information Systems

Lothar Fritsch, Habtamu Abie

Department of Applied Research in Information Technology (DART)
Norsk Regnesentral / Norwegian Computing Center
Postbox 114, Blindern, NO-0314 Oslo, Norway
Lothar.Fritsch@NR.no, Habtamu.Abie@NR.no

Abstract: Privacy risk management in information systems is a challenge to system designers and system owners. Increasing regulation requires compliance management, while publicly visible incidents damage companies' reputation in connection with their treatment of customer privacy. Additionally, increasing attacks with stolen identities and fake identification are carried out against information systems. Companies need to have a privacy management strategy and a privacy-centric technology management. However, no unified methodology for privacy risk assessment, or the selection of countermeasures, exist. This article, after presenting the historic development of data protection and privacy technology research, maps out the missing knowledge areas of privacy technology deployment, and summarizes a return-on-investment approach on privacy management. We conclude with a roadmap on privacy risk management based on preliminary results on privacy threat impact analysis from the Norwegian PETweb research project.

1 Introduction

Which privacy protection technology should be applied to a particular application? How much value is generated from investments in privacy-support in information systems? Is there a return on investment in privacy protection systems? While constitutional lawyers and privacy advocates might object the idea of framing privacy with economic boundaries, certain cost is involved in adding privacy management technology and procedures to the portfolio of any business dealing with private information. This cost is what might be important for PET research and development that is expected to lead to relevant innovations that have a practical outreach on systems deployed for application purposes. But what are the limits? There is some evidence that there can be too much technology in a security infrastructure, resulting in too high transaction cost. Three examples are chosen from the literature to illustrate this point. In the first, the question of economic sense making of cryptographic infrastructures for micropayment is raised [Odl2003a]. Odlyzko argues that for small amounts of money, strong cryptography implementing secure digital coins creates transaction costs much higher than the value of the transactions. This, according to Odlyzko, leaves an infeasible payment system. Next, Digital Rights Management (DRM) can be a victim to transaction cost. Lewis argues in [Lew2003] that forcing too expensive DRM solutions onto the market could have negative impacts on the market.

Finally, PKI and the European framework for electronic signatures are an example of a possibly too-expensive security infrastructure. In [FR2005], the authors argue that too expensive infrastructure and other market mismatches get into the way of large-scale deployment of electronic signatures in Europe. From these examples, it can be concluded that there may exist a point where no reasonable return on investment for privacy management is gained. This should be subject to further research. Some approaches are summarized in the next section. This article will focus on two topics. First, the value and associated risk of privacy breaches is analyzed. From there, we elaborate to find a decision method that will weigh such risks against investments that are necessary to reduce or remove the privacy risks.

2 Technology for protection of privacy – a brief history

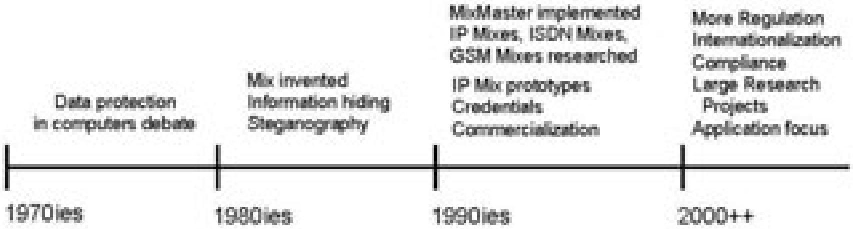

Figure 1: Brief history of Privacy-enhancing Technology.

PET as a research topic has been opened by David Chaum in 1981. In [Cha1981], he describes a method for anonymous and unobservable delivery of electronic messages called “Mix”. Chaum uses security protocols and subsequent layers of encryption to provide privacy protection by “mixing” several people’s e-mail traffic in encrypted form. The concept later was implemented in the MixMaster e-mail anonymization system [MCP+2004], which is the first practically available PET system. The appearance of technological measures for privacy protection coincides with strengthening legal regulation of the use of personal data on information systems. Starting in the 1970ies, regulatory regimes were put on computers and networks. Starting with government data processing, along the lines of computerization of communication and workflows, explicit rules like the European Data Protection Directive [Eur2002] have been put in place. With the adoption of Internet and mobile telephony in society in the past decade, the privacy challenges of information technology came to everyday life. Hence in the 1990ies, research efforts on PET increased, with Chaum’s concept being adapted to internet data traffic [PW1986] [PPW1991], [GRS1996] and call routing in ISDN [JMP+1998] or mobile telephony [FJK+1997].

Along with several publicly funded research projects [LPS+2000], [PRI2003], [FID2003], several companies turned privacy protection into a business model [Anonymizer.com, Zeroknowledgesystems.com, dossier services, XeroBank, Anti-Spyware, Virus tools]. Researchers investigated cryptography and information hiding technology to produce privacy-supporting protocols such as anonymous credentials [Cv2002]. A milestone in this development is the appearance of a "Handbook on Privacy-Enhancing Technologies" [BBO2003] written by representatives of the regulatory authorities, not by PET researchers or technicians.

With the globalization of the economy and the IT infrastructure supporting it, in the years staring the 3rd millennium privacy management has turned into a matter of corporate governance and compliance, with legislation targeting this issue (in various directives, e.g. [Eur2002], see [Buc2004] for more legal references). Standardization bodies and interest groups such as ISO [BHR+2007], W3C[1] and IETF [Mül2004] initiate privacy technology standardization work. Global players such as IBM and HP target corporations with their privacy compliance services related to the IBM Tivoli and HP Select product lines. In this context, recent efforts on using Trusted Computing [TCG2007] to implement privacy-compliant data handling [CPB2003] show the path to the future of information privacy as a matter of compliance.

The PET research perspective was mostly on the legal foundations of privacy protection. determined by constitutional and fundamental human rights that should be protected using technology. This view is shown in an analysis of the PET vocabulary in [Koc2006]. As rights are granted to individuals, much of the research has focused on the user-side, e.g. visible in a well-quoted terminology paper [PH2007]. The legal view is propagated into contemporary frameworks like the Canadian [The2002] and Dutch [Coo2001] privacy legislation, which both define privacy audit schemes with detailed procedural definitions and responsibilities, but neglect to provide a decision support method for managers that would enable them to make feasible decisions about privacy needs based on quantifiable risks. Most of these criteria, including schemes like Datenschutz-Gütesiegel [Una2003], provide checklists with questions for the auditors. They inherently call for competent – and well-paid – external experts when they are used by a company, but are rarely based on empirical data or metrics. The PET award winning taxonomy of privacy [Sol2006] is very visibly structured along the legal view on privacy.

A recent interest in economics research picks up a different view on privacy. The cost of privacy management, the inherent value and cost of privacy for both businesses and users are modeled and studied. Varian examined the economic relevance of personal information in [Var1996]. He also presents basic transactions with personal information that are relevant. Laudon examined the market for personal information and proposed a national market for personal information in [Lau1996a] and [Lau1996b].

[1] The World Wide Web consortium, W3C, www.w3c.org

He cared for information trade with some control aspects. In addition, some of the costs of too little and too much privacy are discussed with their relevance to the information market. Some practical insight to Laudons market can be gained in Rubin & Lenard's summary of the market for personal information in: [RL2001]. The authors study players on the information market in detail, their effects on consumer privacy and the effects of privacy regulation on the United States of America information market. A transaction cost view of privacy is examined by Sholtz in [Sho2003a] and [Sho2001]. Sholtz creates an analogue between transactions cost on environmental pollution and privacy. Kahn et al develop an economic model for privacy transactions in [KMR2000]. Another economic issue is quality signaling. No work on signaling of privacy properties in relation to economics exists, but Backhouse et al show in [BHB+2004] that there can be a Lemons Market for PKI in the absence of strong quality signals. It seems very likely to be the case with expensive privacy infrastructures, but has not been researched. Much work has been done by Acquisti to find empirical foundations for the economic valuation of end-user privacy [AG2004], [Acq2002]. Steps toward business cases for PET have been undertaken in [KB2004] and [Cla2007]. Both papers suggest a view on value gained through PET deployment.

3 Toward quantifiable privacy risk

On the practical side, a methodology for privacy-risk reduction in IS design is needed. It should select the right amount of privacy protection – for a tolerable investment - to reduce the risks. For quick and efficient construction of privacy-respecting infrastructures, tools for process modeling, lifecycle management of personal data are necessary. Within the personal information treatment process, some form of "black box" abstraction for the PET basic functions is needed. This abstraction reduces a PET component to its functionality, cost of acquisition and cost of operation. A basic model has been presented as a case study for a MIX anonymization service in [FRS+2005]. Another approach to functional abstraction was done in an analysis model in [OC2002], where basic privacy functions are mapped to protection functions. However, many territories on the map of such a process-oriented, empirical approach are still unsurveyed, white spaces, particularly:

- The value of privacy in IT systems;
- The cost or damage that occurs upon privacy breaches;
- The cost-benefit distribution between companies and users (called the "dual nature" or privacy risks below);
- An abstraction of PET components into building blocks with functions, effectiveness measure and cost;
- A model of risks and their magnitude of impact;
- A model of cost versus risk versus investment;

The remainder of this section will survey the unknown territories for what is known about them, and suggest an integrated model that connects those territories.

3.1 Value of privacy

What is – being the target of privacy violations – the value of privacy for individuals? Many researchers, in particular in economics, tried to model the value. Others surveyed users or consumers about how much payment it takes to have them give up private data.

Hubermann [HAF2005] used reverse-prize auctioning to measure user's willingness to give up parts of their privacy. Different items of personal data were tested. Results show different value of attributes (age, weight, …) and differences in gender. For example, women asked for $12.49 for information about their weight, whereas men gave the information for $6.03. Spiekermann [Spi2003] surveyed users of the AN.ON anonymous web surfing service. Among the participants were 59% private users. When asked for their willingness to pay for the – now freely available – service, 40% said they won't pay. Approximately 50% were ready to pay between €2.50 and €5.00 per month for anonymous access. About 10% were ready to pay more than €5.00 per month. Acquisti's research focuses on finding the price where people rather accept money than keep their privacy. In [AG2004] and [Acq2004], some interesting effects are presented. The authors discuss phenomena they found in empirical and experimental data, such as differences in what people claim is important about their privacy versus their actual behavior. Additionally, privacy has been found to have different "buy" and "sell" prices. Trying to make sense of such detailed results, Shostack discusses in [Sho2003b] whether "people sell their privacy for a Big Mac", concluding that the trading of personal information for a Big Mac can be very rational. With unclear risk, hard to evaluate monetary value of the privacy breach, and a distant point in the future where the cost will be realized, Shostack concludes that acceptance of the Big Mac presents an immediate value versus an uncertain monetary risk. However, a convincing qualitative or quantitative valuation of "privacy in information systems" does not exist. What is missing in the field is a concept and an understanding of the short- and long-term value that is created by having privacy in information systems. We have to add unknown territory to out map:

- Who would benefit from privacy in IS? And to what amount?

3.2 Unknown cost of privacy breach

In information systems (IS) security management, the question of investment in security technology usually is a question of risk management. Investment in new preventive technologies induces cost. The goal of an IS is economic efficiency for its owner while serving its purpose. To decide whether spending is justified, a risk and investment analysis is performed.

Potential damages in monetary units are assessed and set in relation to the probability of the damage occurrence. Then a decision is made whether to ignore the risk, buy insurance, invest in technology, or abandon the particular product or service. Much data has been collected by consulting and insurance companies about types of IS risks and the resulting damages to the owning business. The usual method to guess monetary damages is an analysis of past occurrences of similar problems, the damages caused by them, and the financial loss that has occurred. Additional factors like the value of transactions or the number of customers involved can be used to increase precision of the calculation. Although this method has its imperfections when it comes to precision, it is the state of the art [Bun2000]. When focusing on privacy breaches, much less history of damages is known. Two observations make it harder to implement "privacy risk management" to IS. First, unlike the IS security calculation, in the privacy domain the question of risk is not focusing exclusively on the owner of an IS and the respective damages caused to his business operation. Privacy management also involves the data subject's private data and potential damages caused to the IS users and their personal business following privacy breaches. The two entities involved complicate the generation of a simple database with cost and probability of privacy breaches, as each type of user - depending on the application - has different personal value at stake. Fundamental questions in privacy risk assessment are: How much damage is a particular privacy breach going to cause?

How long will the personal information that got out be a risk? Is the risk constant over time, does it degrade, or will it increase? How does the risk change when personal information is combined with other information? How does the entity using the personal information influence the risk? To be able to answer these questions, two kinds of classification are needed: A classification and quantification of privacy risks, and a classification of PET functions in terms of risk reduction, effectiveness, and cost is required. The latter will be discussed in section 3.4. A classification of privacy risks and the cost induced by these risks has not been done in convincing ways. Concluding this section, two of the white spaces on the map are:

- Missing empiric base of privacy damages to businesses and users
- Unclear concept of damages and cost relating to privacy breaches, in particular focusing on the lifecycle of personal information

3.3 Who is at risk? – The dual nature of privacy risk impact

Unlike the “perimeter security” paradigm that was central to information security for many years, privacy risks occur inside and outside an information system. Where the perimeter security paradigm took care that all critical information stays inside the secured systems, many open systems on the Internet trade personal information and process it as the very purpose of the system. The effects of a breach of private information security could affect the owner of the information system – but also the person the data is about. This invokes a duality of privacy risks. In technology, this insight has been transformed into the principle of “Multilateral Security” [Ran2000]. However, in the areas of risk management and investment decisions, the duality of privacy risks has not been the subject of major concern.

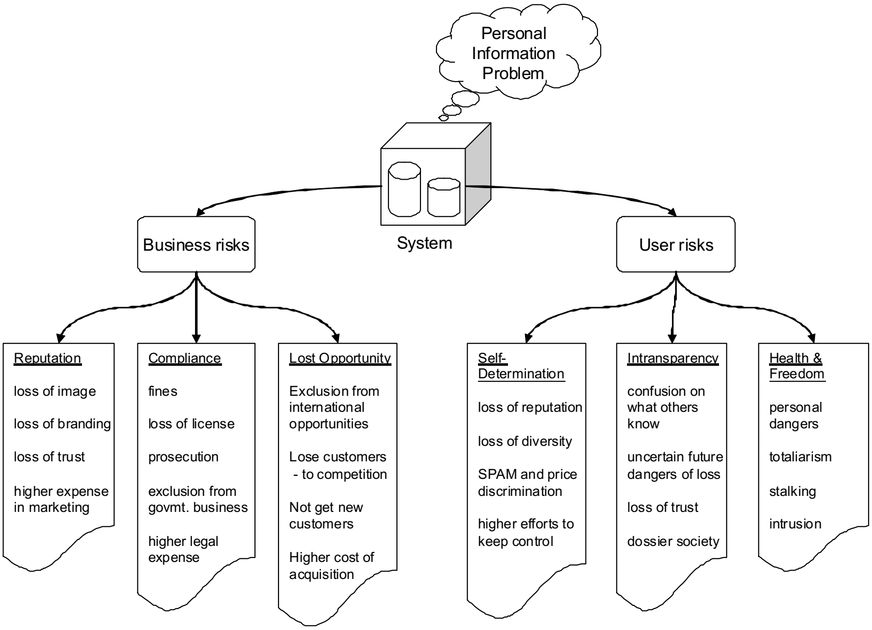

Figure 2: Duality of the impact of privacy risks.

Businesses	Consumers
Sales Losses Due to Lack of Privacy One Retailer's Loss Is Another Retailer's Opportunity Lost International Opportunities Increased Legal Costs, Investor Losses	Higher Prices Junk Mail, Telemarketing Identity Theft Internet Effects The Dossier Society

Table 1: Privacy risks from [Gel2002].

Privacy risks are not well defined in the literature. Too low quality of a particular protection technology might destroy particular applications, as Friedmann shows in [FR1999]. In [Gel2002], the business and consumer side of privacy risks and costs is examined.

The author classifies risks and provides an example with monetary figures on how much cost is imposed on the average U.S. family through privacy breaches. The suggested risks are listed in Table 1. Additionally, Solove's taxonomy presents a systematic model of user risks in [Sol2006]. But it is oriented along the legal perspective and lacks a quantification of risks.

Odlyzko agrees that a lack of privacy in consumer commerce settings leads to financial losses due to price discrimination [Odl2003b]. Many approaches exist that try to define a monetary value for personal information by the means of offering money for private information, or by requesting money in exchange for more privacy. Some examples are being discussed in paragraph 3.1.

Business side cost factors

Privacy Office: Costs associated with dedicated staff, office overhead, travel and business equipment.

Policy & Procedures: Costs associated with the creation, review, publication and dissemination of the privacy policy (and privacy notice when applicable).

Downstream Communications: Costs associated with the communication and outreach activities for the privacy program both within the company and to outside stakeholders.

Training & Awareness: Costs associated with the education of employees and other key company stakeholders about the privacy policy, program and related concepts.

Enabling Technologies: Costs associated with technologies that help mitigate privacy risk, enhance responsible information management, or protect the critical data infrastructure.

Employee Privacy: Costs associated with the protection of sensitive employee records, including heath care and OSHA claims.

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.

Audit & Control: Costs associated with the monitoring, verification and independent audit of the privacy program, including use of controlled self-assessment tools.

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

Table 2: Cost of privacy from [Pon2004].

Only few studies exist on the cost of privacy management on the business side. In 2004, the Ponemon Institute conducted a study for IBM [Pon2004]. It provides a cost factor model (see Table 2) 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.

From [Pon2004], 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. Privacy technology by itself is not a main cost driver – policies, enforcement, legal counsel and many other factors outnumber the cost of PET used. When deciding on the deployment of privacy-enhancing technologies into a business infrastructure, return-on-investment (ROI) considerations will play an important role in any investment decision – both on the business and the user sides. While ROI of information technology security investments is a much discussed topic at contemporary conferences, only few conclusive guidelines exist, e.g. [Bun2000]. Thus we add more unknown territory to the map of privacy risk management:

- What are the different assets at stake for businesses[2] and users?
- What is the difference in risks and costs for both parties in nature, latency and type?

3.4 PET effectiveness & efficiency hard to measure

For any deployment of PET into information systems, the effectiveness of the PET measure against threats is important. While in the above sections we found that risk and associated cost are not easy to quantify, the verification of effectiveness of a PET system relative to its cost is one more unknown parameter. It is a base to economic and technical decision-making that is – so far - hard to express in numbers. While PET cost of installation and operation, although non-existent, could be assessed with experiments, the efficiency of their deployment remains unknown. In the computer science field, several contributions provide information theoretic models for anonymity, identifiability or the linkability of data, e.g. Steinbrecher in [SK2003] or Diaz and Preneel in [DP2004]. Both papers build mathematical models that are rather impractical for usage in the evaluation of large-scale information systems. Another suggestion comes from an article on intrusion detection by user context modeling [MP2004], where the author tries to identify attacks by classification of untypical user behavior. Such behavioral analysis can be developed into a tool to measure effectiveness of PET. From some experiments on profiling people with publicly available data from the Internet [Dia2005], one might try to use profiling output as a measure of the quality of PET systems.

But the definition of the information that counts as a part of a profile, as well as the question of how to distinguish leaked information from intentionally published personal information make profiling a rather impractical metric. With these difficulties in measuring effectiveness of PET, how will we judge efficiency? Also, for the deployment of PET on the business side, or the acceptance of some extra effort by users adapting to PETs, there are more questions to ask: Which PET will remove or reduce a particular risk? At what cost will a particular PET remove a particular risk? How much effort (instruction, change of system usage habits, change of behavior, self-control) had to be spent on the user-side for the PET to be effective? Is there a cheaper or more convenient alternative on how to deal with a particular risk instead of PET deployment? Our research road map has to be extended by:

- Models for effectiveness, efficiency and cost of PETs in application

3.5 Privacy threats & impact analysis

In the Norwegian PETweb research project[Nor2007], we have modeled and tested a privacy threat impact analysis model. Starting with a privacy threat ontology based on CERT's security risk taxonomy [HL1998] and the impact analysis in [LR2006].

[2] For simplicity, the term "businesses" here is meant to include public administration, system owners, system operators, service providers, content providers and all other names for system controlling entities that are used.

The resulting privacy threat impact analysis model examines all system assets for threats, threat agents that can attack them, and the impact of successful attacks on the system's privacy properties (see Figure 4).

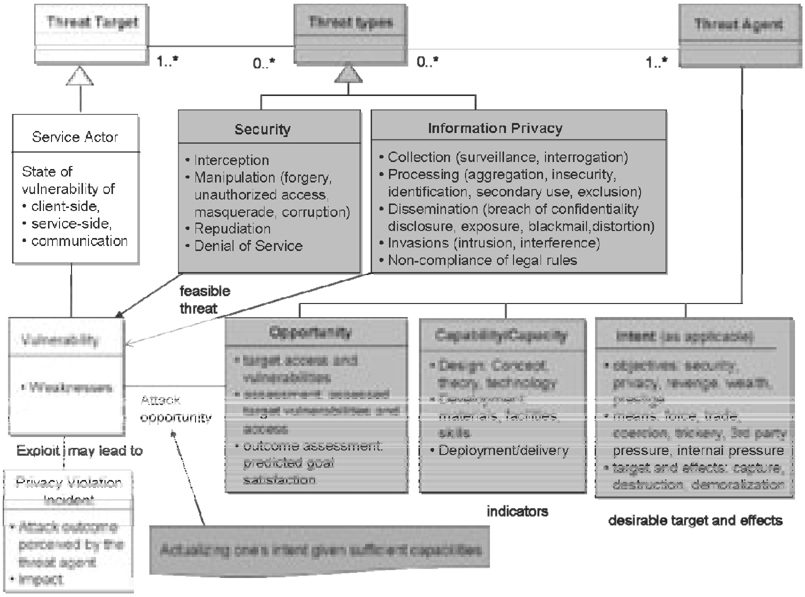
Threat Target
Threat types
Threat Agent
1..*
0..*
0..*
1..*
Service Actor
State of vulnerability of
• client-side,
• service-side,
• communication
Security
• Interception
• Manipulation (forgery, unauthorized access, masquerade, corruption)
• Repudiation
• Denial of Service
Information Privacy
• Collection (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
Attack opportunity
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
indicators
desirable target and effects
Exploit
may lead to
Privacy Violation Incident
• Attack outcome perceived by the threat agent
• Impact
Actualizing one's intent given sufficient capacities

Figure 3: PETweb privacy threat impact analysis model [Nor2007].

The practical application of the methodology was carried out with the prized Norwegian E-Government application MyPage[3] (www.norge.no). However, the applicability of the tool was limited due to high levels of uncertainty in assigning qualified values to attack properties, their privacy impact, and the overall impact. Many of the parameters had to be set with an "academic guess", because the foundations of incidents and their impact on privacy is known only on a conceptual level, but is unavailable as empiric evidence. The resulting uncertainty concerning the overall system privacy impact can only removed with empirically calibrating the analysis tool with impact figures and likelihoods. These results suggest that privacy risk analysis is another white space on our road map.

3.6 A model for privacy protection management

Based on the "Return-on-Security-Investment" (ROSI) concept in [Ber2002], an analogous model called "Return-on-Privacy-Investment" (ROPI) is derived in this section. It enhances the ROSI-like approach *Likelihood*Damage – Cost* that is presented in [HNL+2004].

[3] MyPage has won the 2007 European E-Government award, see ec.europa.eu/information_society/newsroom/cf/itemdetail.cfm?item_id=3639 as of 13-Nov-2007.

Figure 4 shows that from the total value of privacy protection, ROPI reduces financial risks through investments that avoid the risks. ROPI states the effect that a particular investment has on the privacy-relevant value of an information system. With the parameters in Figure 4, ROPI is:

$$Value\_after\_investment = Value\_of\_Privacy - (Value\_at\_Risk - ROPI)$$

where for any privacy breach L_B : $ROPI = P_B * C_B - I_{CB}$.

The following figure visualizes the aspects of ROPI. As discussed in the above sections, ROPI is based on concepts and empirical data that have yet to be scientifically explored and defined.

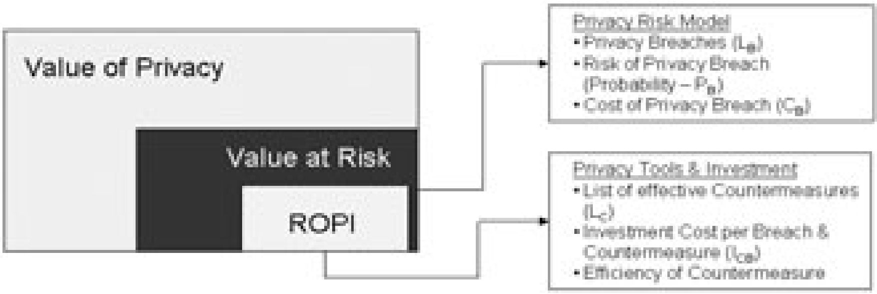
Value of Privacy
Value at Risk
ROPI
Privacy Risk Model
• Privacy Breaches (L_B)
• Risk of Privacy Breach (Probability – P_B)
• Cost of Privacy Breach (C_B)
Privacy Tools & Investment
• List of effective Countermeasures (L_C)
• Investment Cost per Breach & Countermeasure (I_CB)
• Efficiency of Countermeasure

Figure 4: Privacy protection model based on risk assessment and investment.

Figure 4 shows the ROPI model. It contains the open research areas from the roadmap as input to the calculation of various parts. From a risk management perspective, ROPI will reduce privacy risks that have been assessed as “value at risk”. An investment in PET – or insurance – then is sought after by analyzing countermeasures, their cost, and their effectiveness. Unfortunately, the components of the ROPI model are almost exclusively the white spots on our privacy risk management roadmap. The impact analysis effort in the PETweb project described in 3.5 dealt with similar difficulties in assessing quantifiable risks and their impact.

4 The road ahead

How will we arrive at a working privacy risk management model that is based upon empirical evidence? The challenge ahead is the surveying of the white spaces on the privacy risk management map. Particularly, research effort should be spent on:

- Modeling observable, quantifiable risks to privacy with respect to the duality of risk to businesses and users – based on a risk analysis & a risk impact model;
- Research and empirics on the impact and cost of privacy breaches;
- Modeling of PET functions to an abstraction that enables them to be used in business process modeling, including their cost function, effectiveness and efficiency;

Figure 5 shows the above research paths as the Risk Model Road, the Empirics Road and the Cost & Effect Lane.

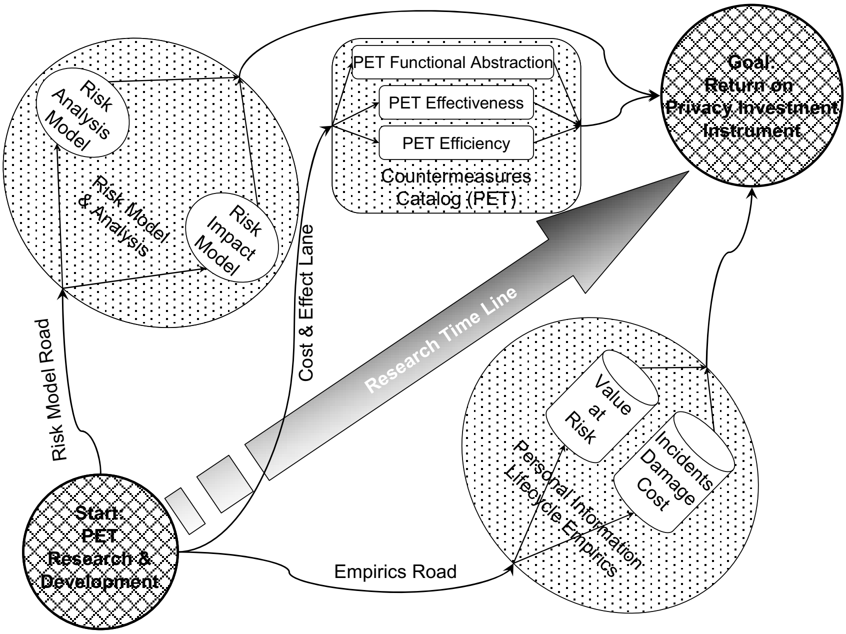

Figure 5: Roadmap to Privacy Investment Management.

The major task however seems to be a necessary "paradigm shift" in the perspective taken by research in privacy technology. The focus on the constitutional perspective, that is so prevalent in any legal discussion of privacy, seems to omit the relativity of privacy issues where it comes to application. The deployment perspective is not that of the "Privacy is an important constitutional principle" but that "How much privacy technology is needed HERE - and what will it cost?" Practitioners might tend toward calling this "Compliance Management". Some researchers might be concerned as this shift in perspective seemingly degrades the importance of privacy to an economic perspective. But this is not the case – the risk management perspective with its "How much privacy"-question can only exist upon the assumption that privacy exists and must be taken care of. What the ROPI model presented aims at is the transfer of PET technology into business practice. There, in the application, will PET research spark innovation for IT managers, auditors and users. We should therefore build the foundations for the privacy risk management – let's get on the road!

5 List of References

[AG2004] Acquisti, A. and Grossklags, J. (2004) Privacy and Rationality: Preliminary Evidence from Pilot Data,*Proceedings of the 3rd annual workshop on economics and information security (WEIS) 2004,* Minneapolis.

[Acq2002] Acquisti, A. (2002) Protecting Privacy with Economics: Economic Incentives for Preventive Technologies in Ubiquitous Computing Environments, *Workshop on Socially-informed Design of Privacy-enhancing Solutions in Ubiquitous Computing, 4th International Conference on Ubiquitous Computing (UBICOMP 2002),* Göteborg.

[Acq2004] Acquisti, A. (2004) Privacy and Security of Personal Information: Economic Incentive and Technological Solutions, in: J. Camp and R. Lewis (Eds.): *The Economics of Information Security,* Kluwer.

[BBO2003] Blarkom, G. W.; Borking, J. and Olk, J. (2003) Handbook of Privacy and Privacy-Enhancing Technologies, College bescherming persoonsgegevens, The Hague.

[BHB+2004] Backhouse, J.; Hsu, C.; Baptista, J. and Tseng, J. (2004) Spotting Lemons in the PKI Market: Engendering Trust by Signalling Quality, in: M. E. Shaw (Eds.): *Electronic Commerce and the Digital Economy,* New York.

[BHR+2007] Bramhall, P.; Hansen, M.; Rannenberg, K. and Roessler, T. (2007) User-centric identity management: New trends in standardization and regulation." *IEEE Security & Privacy* (5: pp. 64 - 67.

[Ber2002] Berinato, S. (2002) Security ROI: Finally a real return on security spending: ." *CIO Magazine* .

[Buc2004] Buchta (ed.), A. (2004) Legal Requirements - part 1 of Deliverable 1.1a of IST PRIME EU project.

[Bun2000] Bundesamt für Sicherheit in der Informationstechnik. (2000) Kosten und Nutzen der IT-Sicherheit, SecuMedia Verlag, Ingelheim.

[CPB2003] Casassa Mont, M.; Pearson, S. and Bramhall, P. (2003) Towards Accountable Management of Identity and Privacy: Sticky Policies and Enforceable Tracing Services,*Proceedings of the 14th International Workshop on Database and Expert Systems Applications (DEXA'03),* IEEE Computer Society, pp. 377.

[Cha1981] Chaum, D. (1981) Untraceable electronic mail, return addresses, and digital pseudonyms, *Communications of the ACM* (4:2), pp. 84-88.

[Cla2007] Clarke, R. (2007) Business Cases for Privacy-Enhancing Technologies, in: R. Subramanian (Eds.): *To appear in: Computer Security, Privacy and Politics: Current Issues, Challenges and Solutions,* 12-Jun-2007, Hershey, USA, IDEA Group Publishing.

[Coo2001] Cooperation Group Audit Strategy (2001) Privacy Audit Framework under the new Dutch Data Protection Act (WBP), College bescherming persoonsgegevens,Netherlands, Den Haag.

[Cv2002] Camenisch, J. and van Herreweghen, E. (2002) Design and Implementation of the Idemix Anonymous Credential System: Research Report RZ 3419, IBM Research Division,IBM Zürich Research Lab, Zürich.

[DP2004] Diaz, C. and Preneel, B. (2004) Anonymous communication, in: Swedish Institute of computer science (Eds.),*WHOLES - A Multiple View of Individual Privacy in a Networked World,* Stockholm.

[Dia2005] Diaz, C.(2005) Profiling Game,1st FIDIS Doctoral Consortium, IST FIDIS Project, Riezlern, Austria.

[Eur2002] European Comission (2002) Directive 2002/58/EC of the European Parliament and of the council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

[FID2003] FIDIS (2003) Future of Identity in the Information Society: The IST FIDIS Network of Excellence, *www.fidis.net,* accessed 6.11.2006.

[FJK+1997] Federrath, H.; Jerichow, A.; Kesdogan, D.; Pfitzmann, A. and Spaniol, O. (1997) Mobilkommunikation ohne Bewegungsprofile, in: A. P. G. Müller (Eds.): *Mehrseitige Sicherheit in der Kommunikationstechnik,* Addison-Wesley-Longman, pp. 169-180.

[FR1999] Friedmann, E. J. and Resnik, P. (1999) The social cost of cheap pseudonyms, *Journal of Economics and Management Strategy* (10:2), pp. 173-199.

[FR2005] Fritsch, L. and Rossnagel, H. (2005) Die Krise des Signaturmarktes, in: H. Ferderrath (Eds.): *Sicherheit 2005,* Bonn, Köllen Druck+Verlag GmbH, pp. 315-327.

[FRS+2005] Fritsch, L.; Roßnagel, H.; Schwenke, M. and Stadler, T. (2005) Die Pflicht zum Angebot anonym nutzbarer Dienste: Eine technische und rechtliche Zumutbarkeitsbetrachtung." *Datenschutz und Datensicherheit (DuD)* (29:10), pp. 592-596.

[GRS1996] Goldschlag, D. M.; Reed, M. G. and Syverson, P. F. (1996) Hiding Routing Information, in: R. Anderson (Eds.): *Information Hiding,* Berlin, Springer, pp. 137-150.

[Gel2002] Gellman, R. (2002) Privacy, Consumers and Cost: How The Lack of Privacy Costs Consumers and Why Business Studies of Privacy Costs are Biased and Incomplete .

[HAF2005] Hubermann, B. A.; Adar, E. and Fine, L. R. (2005) Valuating Privacy, *IEEE Security & Privacy* (5:3), pp. 22-25.

[HL1998] Howard, J. and Longstaff, T. (1998) A Common Language for Computer Security Incidents: Report SAND98-8667, Sandia National Laboratories,Sandia Corporation, Albuquerque, New Mexico, USA.

[HNL+2004] Hong, J.; Ng, J.; Lederer, S. and Landay, J. (2004) Privacy risk models for designing privacy-sensitive ubiquitous computing systems, in: D. Benyon; P. Moody; D. Gruen and I. McAra-McWilliam (Eds.): *Proceedings of the 2004 conference on Designing interactive systems: processes, practices, methods, and techniques,* August 1, 2004, New York, ACM Press, pp. 91-100.

[JMP+1998] Jerichow, A.; Müller, J.; Pfitzmann, A. P. B. and Waidner, M. (1998) Real-Time Mixes: A Bandwidth-Efficient Anonymity Protocol: Special Issue on "Copyright and privacy protection"." *IEEE Journal on Selected Areas in Communications* (16:4), pp. 495-509.

[KB2004] KPMG; Borking, and Borking, J. (2004) Privacy-enhancing technologies: Whitepaper for decision-makers, Dutch Ministry of the Interior and Kindom Relations,The Netherlands, The Hague.

[KMR2000] Kahn, C.; McAndrews, J. and Roberds, W.(2000) A Theory of Transactions Privacy,Financial Institutions Center, The Wharton School, University of Pennsylvania, Atlanta.

[Koc2006] Koch, C. (2006) Taxonomie von Location Based Services, Frankfurt am Main.

[LPS+2000] Lacoste, G.; Pfitzmann, B.; Steiner, M. and Waidner, M. (2000) SEMPER - Secure Electronic Marketplace for Europe, Springer, Berlin.

[LR2006] Little, E. and Rogova, G. (2006) An ontological analysis of threat and vulnerability,*Proceedings of the 9th international conference on information fusion (ICIF'2006),* July 2006, Florence, Italy, IEEE Computer Society, pp. 1-8.

[Lau1996a] Laudon, K. C. (1996) Markets and Privacy, *Communications of the ACM* (39:9), pp. 92-104. (a)

[Lau1996b] Laudon, K. C. (1996) Extensions to the theory of Markets and Privacy, Stern School of Business,New York University, New York. (b)

[Lew2003] Lewis, S. R. (2003) How much is stronger DRM worth? *2nd Annual Workshop 'Economics and Information Security'; University of Maryland, May 2003,* .

[MCP+2004] Möller, U.; Cottrell, L.; Palfrader, P. and Sassaman, L. (2004) Mixmaster Protocol Version 2, *http://www.ietf.org/internet-drafts/draft-sassaman-mixmaster-03.txt,* accessed 15-Jan-2008.

[MP2004] Mazhelis, O. and Puuronen, S. (2004) Combining One-Class Classifiers for Mobile-User Substitution Detection,*Proceedings of 6th International Conference on Enterprise Information Systems (ICEIS'04),* Porto, pp. 130-137.

[Mül2004] Müller, M. (2004) Standards for Geographic Location and Privacy: IETF's Geopriv, *Datenschutz und Datensicherheit (DuD)* (28:5), pp. 297-303.

[Nor2007] Norsk Regnesentral (2007) The PETweb research project: Privacy-enhancing technologies (PETs) in large-scale web-based services for the general public and customers, *http://petweb.nr.no/petweb/index.php/Main_Page,* accessed 13-Nov-2007.

[OC2002] Osorio, C. A. and Camp, L. J. (2002) Dimensions for the analysis of conflicts between business and technological models in privacy-enhancing solutions for electronic commerce, *Inet 2002,* .

[Odl2003a] Odlyzko, A. (2003) The case against micropayment, in: R. Wright (Eds.): *Proceeding of Finanical Cryptography 2003 (FC03),* Springer, pp. 77-83. (a)

[Odl2003b] Odlyzko, A. (2003) Privacy, Economics, and Price Discrimination on the Internet: Extended Abstract. (b)

[PH2007] Pfitzmann, A. and Hansen, M.(2007) Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management – A Consolidated Proposal for Terminology:v0.29, Dresden.

[PPW1991] Pfitzmann, A.; Priftzmann, B. and Waidner, M. (1991) ISDN-mixes: Untraceable communication with very small bandwidth overhead,*In the Proceedings of the GI/ITG Conference on Communication in Distributed Systems, February 1991,* pp. 451-463.

[PRI2003] PRIME (2003) Privacy and Identity Management for Europe: The IST PRIME Project, *www.prime-project.eu,* accessed 6.11.2006.

[PW1986] Pfitzmann, A. and Waidner, M. (1986) Networks Without User Observability – Design Options,*Advances in Cryptology - EUROCRYPT '85: Proceedings of a Workshop on the Theory and Application of Cryptographic Techniques,* Berlin, Springer, pp. 245.

[Pon2004] Ponemon Institute (2004) The Cost of Privacy Study,The Ponemon Institute, Tucson, Arizona.

[RL2001] Rubin, P. H. and Lenard, T. M. (2001) Privacy and the commercial use of personal information,Progress & Freedom Foundation, Washington, D.C.

[Ran2000] Rannenberg, K. (2000) Multilateral Security - A concept and examples for balanced security,*Proceedings of the 9th ACM New Security Paradigms Workshop,* September 19-21, 2000, Cork, Ireland, ACM Press, pp. 151-162.

[SK2003] Steinbrecher, S. and Köpsell, S. (2003) Modelling Unlinkability, in: Roger Dingledine (Eds.): *Proceedings of Privacy Enhancing Technologies workshop (PET 2003),* Springer Verlag.

[Sho2001] Sholtz, P. (2001) Transaction Costs and the Social Costs of Online Privacy, *First Monday* (6:5).

[Sho2003a] Sholtz, P. (2003) Economics of Personal Information Exchange, *First Monday* (9:5). (a)

[Sho2003b] Shostack, A. (2003) 'People Won't Pay For Privacy,' Reconsidered, *2nd Annual Workshop 'Economics and Information Security'; University of Maryland, May 2003,* . (b)

[Sol2006] Solove, D. (2006) A taxonomy of privacy: GWU Law School Public Law Research Paper No.129." *University of Pennsylvania Law Review* (154:3), pp. 477.

[Spi2003] Spiekermann, S. (2003) Die Konsumenten der Anonymität: Wer nutzt Anonymisierungsdienste?." *Datenschutz und Datensicherheit (DuD)* (27:3), pp. 150-154.

[TCG2007] TCG (2007) The Trusted Computing Group, *http://www.trustedcomputinggroup.org,* accessed 16-Jun-2007.

[The2002] The Treasury Board of Canada (2002) Privacy Impact Assessment Guidelines Version 2.0: A Framework to Manage Privacy Risks, *http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/paipg-pefrld_e.asp,* accessed 15-Jan-2008.

[Una2003] Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (2003) Datenschutz-Gütesiegel, *http://www.datenschutzzentrum.de/guetesiegel/index.htm. (accessed 1-Dec-2007)*

[Var1996] Varian, H. (1996) Economic aspects of personal privacy, In: *Privacy and Self-Regulation in the Information Age,* Dec. 6, 1996, Washington, U. S. Department of Commerce.