

State of the art of Privacy-enhancing Technology (PET)

Deliverable D2.1 of the PETweb project

Report no	1013
Authors	Lothar Fritsch
Date	22-Nov-2007
ISBN	978-82-53-90523-5

About the authors



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 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.

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.

Title	State of the art of privacy-enhancing technology (PET)
Authors	Lothar Fritsch
Reviewers	Bjarte Østvold (Norsk Regnesentral) Lasse Øverlier (Høgskolen i Gjøvik)
Date	22-Nov-2007
Year	2007
ISBN	978-82-53-90523-5
Publication number	1013

Abstract

Privacy-enhancing technology (PET) is used to protect personal data in information systems. This report reviews the history of PET, presents important terms and classifications for PET and reviews existing, productive PET systems that are available for use today. Upcoming technology from research projects is referenced.

Keywords	PET, privacy-enhancing technology, data protection, information security, privacy
Target group	General public
Availability	Public
Project number	320374
Research field	ICT – Privacy & Security
Number of pages	34
© Copyright	Norsk Regnesentral

Preface

The overall goal is to enable communicating organisations to include privacy enhancing technologies (PETs) in large-scale web-based services for the general public and customers.

The motivation for this project arises from the following:

Communication services and networks have become complex and highly interconnected, and the cost of storage is approaching zero for all practical purposes. This means that there is no longer any pressing need to remove redundant or duplicate data with the result that the volume of stored data is enormous and constantly increasing. The web makes it easy to access data and easy to aggregate and correlate data from numerous different sources.

In the long run, access restriction alone cannot suffice to protect privacy and the enforcement of privacy using traditional methods of access control/PETs becomes difficult since it does not scale adequately to the increased volume of data/information.

Therefore it is necessary to investigate new approaches to privacy enhancing technologies in order to arrive at technologies that are scalable, practical and in accordance with relevant legislation.

This project was funded by the Norwegian Research Council as project nr. 180069/S10.

Contents

1	Introduction	7
1.1	History of PET	7
1.2	Taxonomy of PET.....	8
1.2.1	Privacy	8
1.2.2	Terms and Definitions	9
1.2.3	Classification of PET systems.....	10
1.3	PET in information ecosystems.....	14
1.3.1	Context of Privacy-enhancing technology	14
1.3.2	Technical standards.....	15
1.3.3	Audit and Guidelines.....	15
1.4	Current research in PET.....	17
2	Available PETs	17
2.1	Transparency tools.....	18
2.1.1	Detection tools	18
2.1.2	Policy management and enforcement	19
2.2	Opacity tools.....	20
2.2.1	Unobservability tools.....	20
2.2.2	Identity Management tools.....	27
2.3	Commercial products and services	29
2.3.1	Privacy-enhancing products.....	29
2.3.2	Privacy-enhancing services	29
2.3.3	Privacy management business software	29
3	Conclusion	30
4	Appendix	30
4.1	References	30
4.2	Index.....	34

1 Introduction

1.1 History of PET

PET as a research topic has been opened by David Chaum in 1981. In his MIX paper (Chaum 1981), 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 (Moller et al. 2004), which is the first practically available PET system.

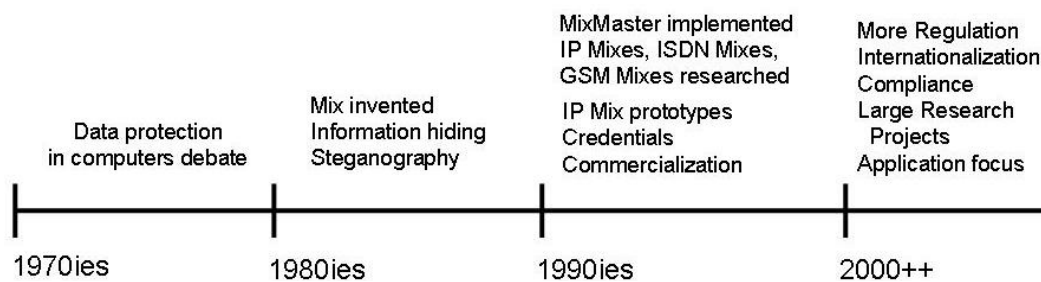


Figure 1: Brief history of Privacy-enhancing Technology.

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 (European Commission 2002) 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 (Pfitzmann and Waidner 1986), (Pfitzmann et al. 1991), (Goldschlag et al. 1996a) and call routing in ISDN (Jerichow et al. 1998) or mobile telephony (Federrath et al. 1997). Along with several publicly funded research projects (Lacoste et al. 2000), (PRIME 2003), (FIDIS 2003), 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 (Camenisch and van Herreweghen 2002). A milestone in this development is the appearance of a “Handbook on Privacy-Enhancing Technologies” (Blarkom et al. 2003) 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 starting the 3rd millennium privacy management has turned into a matter of corporate governance and compliance, with legislation targeting this issue (e.g. (European Commission 2002)). Standardization bodies and interest groups such as ISO [study period], W3C and IETF (Müller 2004) initiate privacy technology standardization work. Global players such as IBM and HP target corporations with their privacy compliance services [products, ponemon studies]. In this context, recent efforts on using Trusted Computing (TCG 2007) to implement privacy-

compliant data handling [Siani’s sticky policy paper] show the path to the future of information privacy as a matter of compliance.

1.2 Taxonomy of PET

1.2.1 Privacy

Privacy enhancing technology (PET) is about the protection of privacy in information systems. The term privacy is used in many contexts, and with many possible interpretations. In the context of PET, privacy is either viewed from a legal view – by the data protection community. Or it is viewed as a technical challenge to information security, which relates to the cryptography and computer security community. The specific challenges in information privacy are described in D. Solove’s “A Taxonomy of Privacy” (Solove 2006), which has won the 2006 PET award. Here, the four basic challenges of information privacy are found to be:

1. Information Collection
The collection of personal information by some party.
2. Information Processing
The processing of personal information by some party.
3. Information Dissemination
The distribution of personal information by some party.
4. Invasion of privacy
Intrusion of private spaces
Influencing decision

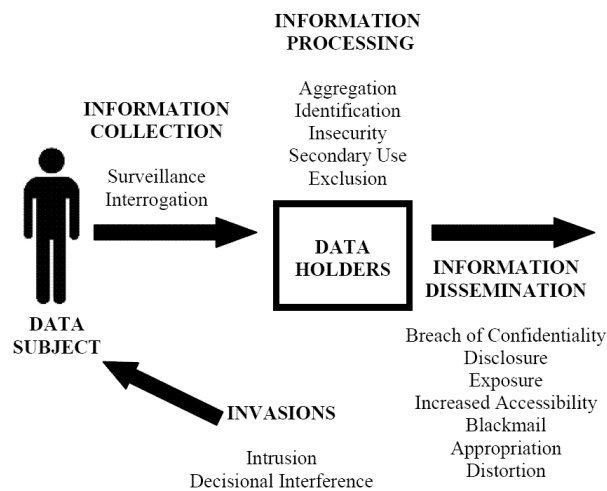


Figure 2: Taxonomy of privacy from (Solove 2006).

Solove describes the four areas in further detail, whereby he identifies particular actions that produce threats to privacy (see Figure 2).

A classification of privacy risks and the cost induced by these risks has not been done in convincing ways. 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 (Friedmann and Resnik 1999). In (Gellman 2002), 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. Noteworthy is the distinction in risks not only to the consumer, but also to businesses. Odlyzko agrees that a lack of privacy in consumer commerce settings leads to financial losses due to price discrimination (Odlyzko 2003).

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 (Gellman 2002).

1.2.2 Terms and Definitions

Terminology in the PET community is sometimes confusing. This section defines the most important terms and concepts that are used in this report. They are mostly taken from or inspired by Hansen & Pfitzmann’s long-term terminology effort (Pfitzmann and Hansen 2003), which is also a good source for the translation of the terms into many other languages beyond English.

Term	Definition
Anonymity	Anonymity means that a subject is not identifiable within a set of subjects.
Identity	A person’s identity is either the person’s self-perception, or the person’s external categorization using attributes that are observable. In the sense of PET, the identity is a set of externally observable attributes and properties that – when taken all together – allow for the identification of a subject among others. The term “partial identity” is used to point out the fact that a subject in a certain role might use – or be identified by – a subset of his personal, externally visible attributes.
Identity management	Identity management is the process of administration of various partial identities of a subject. Privacy-preserving identity management systems keeps distinct partial identities of a subject separate from each other, and thus unlinkable.
Privacy	Privacy in the sense of PET is the autonomy of a subject over his personal information. Privacy in information systems hence is the control over personal information that is being released to other parties. Additionally, transparency about what happens with the information at the other party and ways to limit actions on the information is considered a part of information privacy .

Term	Definition
Pseudonym	<p>A pseudonym is an alias name or other form of identifier that removes a subject's real name, but serves as a means of relating to that subject.</p> <p>Pseudonymity is the state of using a pseudonym as an identifier.</p> <p>Pseudonyms can model roles, transactions, persons, relationships with different degrees of anonymity.</p>
Unlinkability	Unlinkability of a pseudonym or a subject's actions refers to a situation where a n actions or appearance of a subject on a system cannot be identified to belong to any other action of this subject.
Unobservability	<p>Unobservability means that</p> <ul style="list-style-type: none"> - a data object / transfer is not observable to parties uninvolved in the transaction; - the involvement of the subjects in the aforementioned data transfer is not observable to any other parties.

1.2.3 Classification of PET systems

In recent research in the FIDIS project(FIDIS 2003), a functional distinction of privacy and identity protection in transparency tools and opacity tools was introduced (FIDIS 2007).

Transparency tools are intended to create insight into data processing. Their effect is a better understanding of procedures, practices and consequences of personal data processing at a data processor. Because they enhance understanding and visibility, they are called transparency tools. Opacity tools are intended to hide a user's identity or his connection to personal data that occurs at a data processor. As they hide identities, reduce visibility, or camouflage connections, they are called opacity tools.

	Transparency tool	Opacity tools
Definiton	Tools that show clearly to a person what personal data is being processed, how it is processed, and by whom it is processed.	Tools that hide a person's identity or his relationship to data as it is processed by someone else.
Non-technical example	<ul style="list-style-type: none"> • Legal rights to be informed about data processing; • Privacy audits. 	<ul style="list-style-type: none"> • Pseudonymous access to on-line services; • Election secrecy.

	Transparency tool	Opacity tools
Technical example	<ul style="list-style-type: none"> • Database audit interfaces; • Audit Agents, • Log files. 	<ul style="list-style-type: none"> • MixMaster anonymous e-mail; • TOR anonymizing web surfing; • Pseudonyms.

Table 1: Transparency and opacity tools.

This classification originally conceptualized tools as legal framework and technical practice. But its adaption to a technical classification of PET systems only is useful. The distinction is introduced in Table 1.

The distinction above can be further elaborated by the analysis of PET functionality. A study for the Danish Government (Meta Group 2005) divides privacy technologies in the two groups of “privacy protection” and “privacy management”, where the description of the technologies grouped by the two concepts goes along the transparency-opacity distinction. In Table 2, “privacy protection” lists opacity tools, while “privacy management” aims at the transparency tools.

Category	Subcategory	Description
Privacy Protection	Pseudonymizer Tools	Enabling e-business transactions without requiring private information.
	Anonymizer Products and Services	Providing browsing and email capability without revealing the user’s address and identity.
	Encryption Tools	Protecting email, documents and transactions from being read by other parties.
	Filters and Blockers	Preventing unwanted email and web content from reaching the user.
	Track and evidence erasers	Removing electronic traces of the user’s activity.
Privacy Management	Informational tools	Creating and checking Privacy Policies.
	Administrative Tools	Managing user identity and permissions.

Table 2: Privacy protection classification from (Meta Group 2005).

However, the PET community will not agree with certain aspects in Table 2, as user-centric identity management aims at a user's informational self-determination, and thus clearly is an opacity tool (Hansen and Pfitzmann 2007). Nonetheless, the Danish study proceeds with the analysis of the core protection mechanisms provided by the classified PET techniques, with a distinction of the functions in unobservability, unlinkability and anonymity. Also, the target of the mechanism is identified to be of informative, or curative nature. This once again reflects the transparency-opacity nature of PETs.

Main Category	Subclasses	Typical Features	I	1	2	3	S	
Privacy Protection	Pseudonymizer Tools	CRM personalization			X			
		Application Data Management			X			
	Anonymizer Products and Services	Browsing pseudonyms					X	
		Virtual Email addresses					X	
		Trusted third Parties				X	X	
		Surrogate Keys				X		
	Encryption Tools	Encrypting email		X				
		Encrypting transactions		X				
		Encrypting documents		X				
	Filters and Blockers	Filtering email spam						S
		Filtering web content						S
		Blocking pop-up windows						S
	Track and evidence Erasers	Spyware detection and removal		X	X	X		
		Browser cleaning tools		X	X			
		Activity traces eraser		X	X			
		Harddisk data eraser		X	X	X		
Privacy Management	Informational tools	Privacy Policy generators	I					
		Privacy Policy readers/validators	I					

Main Category	Subclasses	Typical Features	I	1	2	3	S
		Privacy Compliance scanning	I				
	Administrative Tools	Identity management				X	
		Biometrics				X	
		Smart cards		X		X	
		Permission management		X		X	
		Monitoring and Audit tools		X			S
		Forensics tools					S

Table 3: PET mechanisms classified in (Meta Group 2005).

1. Unobservability – making private information invisible or unavailable to others
 2. Unlinkability – preventing others from linking different pieces of observed information together
 3. Anonymity – preventing others from connecting observed information with a specific person
- I. Information tools
S. Secondary protection targets (countermeasures)

A closer look at the intention of, and functions provided by existing PET reveals an almost even distribution of unobservability, unlinkability and anonymity support (which suggests that non of these properties can be reached alone). Some of the tools surveyed target specific risks posed by on-line systems, such as spyware or cookies. Few of the tools are classified as “information tools” – or transparency tools. Table 3 lists the privacy-enhancing properties of the surveyed systems from (Meta Group 2005).

Roger Clarke has suggested categories for PET systems in (Clarke 2007):

- Pseudo-PETs: Privacy seals, P3P
- Counter-Technology: Counters one specific privacy threat, e.g. SSL encryption or spyware removal.
- Savage PETs: Will provide untraceable anonymity
- Gentle PETs: Balanced pseudonymity tools with accountability, identity management

However, no sharp definition of the classes and no classification of real systems is given.

1.3 PET in information ecosystems

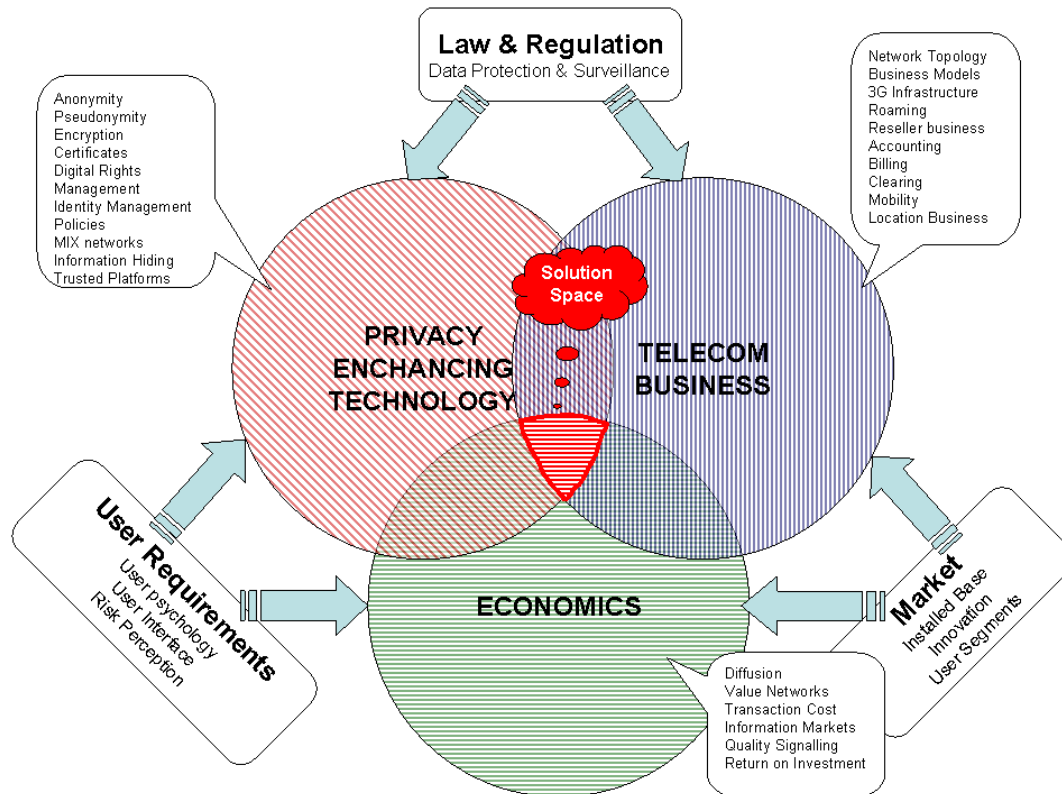


Figure 3: PETs in their information ecosystem (based on (Fritsch et al. 2006)).

Privacy in information systems is not restricted to technological matters. Information systems have a large context that is defined by all stakeholder designing, using, regulating or being influenced by the information system. A deployment of PETs and their meaning to a certain group of stakeholders, a broad analysis of the system's environment and purpose is helpful. This environment is called an "information ecosystem" in this study. At first, we will present the environment PETs are deployed into. Next, we examine the systematic approaches on how technological measures that are in favor of privacy are being handled in terms of technical standardization. Finally, certification schemes and audits are examined.

1.3.1 Context of Privacy-enhancing technology

PETs are connected to many disciplines. PETs are deployed into a larger context of information systems, which in turn are governed by societies' requirements and business requirements. Few complete frameworks for PET-related contexts or approaches have been published, namely KPMG's model (KPMG Canada 2003), a security framework (Zuccato 2005), and a design process (Fritsch et al. 2006). Work on risk modelling (Hong et al. 2004) also provides insight on requirements engineering. In particular, the interdisciplinary nature calls for a model that provides a frame for knowledge in important disciplines as well as a way of integration of application-specific knowledge. In most on-line scenarios, the application specific communities can be identified as telecommunications, PET and Economics (see Figure 3). These communities are influenced by law and regulation, by the situation on the market of needs and related products, as well as by the user requirements from various disciplines respectively. They all influence the need for, and the deployment of PETs, which in Figure 3 is illustrated by the "solution space" - the union of all communities in the diagram's center. Any PET development and deployment must be made in awareness of such a context.

1.3.2 Technical standards

Very few technical standards for privacy protection exist. Those that have been specified usually lack relevance in practice. Many industrial associations have published their own hands-on standards that are intended to comply with new regulation, e.g. with the treatment of location data in mobile phone networks (e.g. the OMA/LIF privacy guidelines (Oinonen 2002)). On the level of IETF, some preparatory work has been done to standardize a large geo-spatial privacy framework called "Geopriv" (Müller 2004). The World Wide Web consortium keeps publishing specifications for privacy preferences selection and other privacy-related description languages. Their focus is web-centric, their relevance in practical application uncertain.

On the international level, there are some ISO activities, but so far the application of ISO 15408 'Common Criteria' (ISO 1999) for privacy evaluation is only under research in PRIME (Kohlweiss et al. 2004) and in a special study period at ISO/IEC/JTC1/SC27/WG3 (Brand 2005)). Current developments there are described in (Bramhall et al. 2007), however it will take some time until the ISO will actually describe a technical standard. What might come from that direction however could be an extension for the application of the Common Criteria. Protection profiles for privacy-related security properties could be expressed as illustrated for the case of MIX remailers in (Rannenbergh and Iachello 2000).

1.3.3 Audit and Guidelines

Many countries have proposed frameworks for privacy audits. Complementing commercial privacy seals aim at confirming privacy properties of e-commerce web site. The major difference in these schemes is their goal. The governmental schemes target at the implementation of the legal privacy principles (consent, purpose of data processing, transparency). The commercial seals are used for marketing purposes, and usually intend trust building with the businesses' customers.

Many of the schemes provide checklists and guidance for audits that follows closely the legal frameworks. Often, the methodologies used are intended to detect the state of a system, but not to suggest improvements of the system using PET.

A number of audit & seals schemes can be found in Table 4.

Name	Issuer	Description	Reference
Privacy Audit Manual	The Australian Privacy Commissioner	This manual outlines the policies adopted by the Privacy Commissioner for the performance of Privacy Audits, describes the Privacy Audit process and the concepts underlying it, and provides guidance as to the audit procedures that should be applied.	http://www.privacy.gov.au/publications/ippam1a.pdf

Name	Issuer	Description	Reference
Privacy Audit Framework under the new Dutch Data Protection Act (WBP)	Co-operation Group Audit Strategy	The Privacy Audit Framework was set up to carry out Privacy Audits in organisations where personal data are processed. Privacy Audits must be carried out in careful consideration: not every organisation is initially ready to undergo a Privacy Audit. A thorough analysis to assess whether a Privacy Audit has added value for an organisation must take place in advance. This is to prevent disappointing the client with regard to the Privacy Audit's results. If the aforementioned analysis shows that a Privacy Audit has insufficient added value for the organisation at that time, then the organisation must take proper measures first. The WBP Self-assessment can be used for this purpose if so desired. The auditor can help an organisation by giving advice during the improvement process.	http://www.dutchdpa.nl/downloads_audit/PrivacyAuditFramework.pdf
Datenschutz-Gütesiegel (Privacy Seal)	Independent Centre for Privacy Protection (ICPP; Unabhängiges Landeszentrum für Datenschutz)	The aim of the project is to persuasively strengthen the confidence of consumers, particularly in the Internet. This Privacy Seal certifies that the compatibility of the product with the regulations of privacy and of security was assessed in a formal process. This process is enacted in the State Data Protection Act of Schleswig-Holstein.	https://www.datenschutzzentrum.de/guetesiegel/eria/information-sheet_icpp_privacy_seal.pdf
TrustE and BBBOnline commercial seals	TrustE, BetterBusiness BureauOnline	Both companies offer privacy seals for e-commerce web sites. <u>TrustE</u> has the highest market share among the seals, listing 1,374 Web sites to <u>BBBOnline</u> 's 701. Truste has nearly a 2-to-1 edge over BBBOnline on the top 50 Web sites, and a 3-to-1 edge among Safe Harbor members.	http://www.truste.org/ http://www.bbbonline.org/

Table 4: Privacy Audit and Privacy Seals.

Concerning the commercial privacy seals, some scientific results in favor of the acceptance of privacy seals exist. In (Cranor et al. 1999), the authors state that a combination of a privacy seal and a privacy policy on a web page has a similar trustbuilding effect as a privacy audit.

1.4 Current research in PET

Current research in the area of PET focuses on several topics:

- The integration of PET into application frameworks;
- The interplay of PET and identity management systems in large, meshed-up application worlds;
- The improvement of security in the handling of personal data;
- The increasing transparency of use of personal information.

The integration of PETs into applications is researched in the PRIME project (PRIME 2003). Here, an interdisciplinary framework for the application of PET components to IT systems is developed and explored in prototypical implementations. PRIME has produced trial prototypes in three application areas. Upcoming projects are intended to research privacy and PET usage on collaboration platforms and within Web 2.0 communities. Some research focuses on the application of newer cryptographic protocols for the purpose of privacy protection, for example for hiding location information in geo-spatial, mobile applications (Kohlweiss et al. 2007).

On the identity management frontier, research came up with anonymous credentials and the IDEMIX system (Camenisch and van Herreweghen 2002) for secure, pseudonymous attestation. This approach enables unlinkability of identity and other credentials.

Concerning transparency, a recent development called “sticky policies” aims at establishing trustworthy computing environments with respect to privacy. By using a Trusted Computing platform in combination with a policy-based data processor, this research seeks to build computers that can not process personal data in any other way than expressed in a policy attached to it – hence the name “sticky policy” (Cassa Mont et al. 2003).

Some research on transparency focused on early notification of people upon their private information leaking out to the internet. With a specialized “privacy search engine”, an approach in (Deng et al. 2006) shows how to keep track of potentially compromising digital photos somebody else has made.

2 Available PETs

Since their first appearance in 1981 (Chaum 1981), many PET concepts have been turned from research into software. In this section, functioning systems are reviewed and discussed along the transparency-opacity distinction. In the end of the section, some commercial vendors of privacy tools & services are listed.

This section neglects research results that have never been put into practice. There exist numerous protocol amendments for anonymous communication on ISDN networks or mobile telephony networks (Federrath et al. 1997), but none of the systems has actually been implemented. The section presents systems in use, and commercial offerings that are related to privacy protection.

Some work on information privacy mentions cryptography as a privacy protection tool. A well-known encryption application is called “Pretty good privacy” (PGP). While such tools are useful to encrypt e-mail, this report looks at approaches that are more directly targeted toward protection of privacy within electronic transactions, data access or participation in on-line systems. Encryption of files or messages was there long before privacy protection or information hiding technology was talked about (Anderson 2001).

2.1 Transparency tools

Transparency tools are tools that provide insight into which data is there, what is done with personal data, or enforce a policy on personal data treatment.

2.1.1 Detection tools

Detection tools serve the purpose of finding out what data is there – or being alarmed when data is moving or being processed outside of the purpose it was given for. Detection mechanisms are either audits or technically sophisticated forms of intentional mistyping in names or addresses that is used by some people to find the source of unwanted mail-order offerings.

One of the detection mechanisms is that of a privacy audit. A privacy audit is a check on an information system’s data content, its data usage and its security policies. Privacy audits are traditionally performed by data protection authorities and consulting companies. An audit of an information system is either performed upon request of the system owner, or upon the complaint of a legal person with the data protection authority. An audit can be the base for the issuance of a privacy seal or privacy certificate. Examples for privacy audit schemes and certificates can be found in section 1.3.3. However, to have a meaningful audit, information systems often need an “audit trail”, which is a logfile of actions performed and data handled so the auditors can see what happens on a system.

Technical detection mechanisms are based on steganographic technology. Here, the private information is secretly marked with watermarks and fingerprints. These marks enable a person to be alarmed when personal information shows up on the web – or to take action against a specific perpetrator if personal data fingerprinted for him is leaking out. Most of the basic techniques are more known as technology for Digital Rights Management. In (Deng et al. 2006), the concept is called “Personal Rights Management” (PRM) and applied to digital cameras and a search engine. However, in practice, most of the watermarking and fingerprinting today must be done manually with a selection of tools for text or image steganography. No integration in web browsers or word processors exists. One exception is the field of digital photo and image business, where companies deploy watermarking and fingerprinting software for photographers and art studios to enable them to track the use of their intellectual property on the Web. One such vendor is Digimarc (www.digimarc.com) with its Digimarc and Digimarc Spider product line for watermarking and Web search engine services.


MarcSpider Standard Search Report

MarcSpider found 1146 watermarked images		
For:	MyImages Corp	Joe Smith
CreatorID:	101010	support@myimages.com
From:	1/1/2005 thru 1/31/2005	503-123-4567

Revise Filter Show/Hide Images Page 1 of 46 >>>


Site: <http://acmerecords.net>

Page: /default

	Name: ramones01copy.jpg ID: 12048475 Found: 1/5/2005 Size: 101196
---	--


Site: <http://acsspace.acsys.it>

Page: /default

	Name: marinepollution.gif ID: 12388216 Found: 1/4/2005 Size: 42166
---	---

Site: <http://afooli.blogspot.com>

Page: /default

	Name: PE-070-0117.jpg ID: 14181647 Found: 1/18/2005 Size: 29949
---	--

Site: <http://alnoorhospital.com>

Page: /home.asp


	Name: MRI%20of%20human%20head.jpg ID: 10627716 Found: 1/14/2005 Size: 15559
---	--

Figure 4: DigiMarc spider search engine results (from DigiMarc.com).

2.1.2 Policy management and enforcement

Policy management tools are twofold. First, they can be used to exchange and negotiate terms and conditions of private data use. When this is done, the next step is the enforcement of the agreement terms with feasible technical means.

2.1.2.1 Policy Management

Privacy negotiation is done between a service and a service user (Preibusch 2005). The World Wide Web Consortium has proposed the P3P specification for privacy preferences negotiation that can be performed between Web browsers and Web servers (Marchiori et al. 2002).

Basically, a set of possible policies for privacy-relevant actions on personal data is offered by a service. The client can negotiate about the offered set of policies with the service. P3P has been criticised to be a tool to dictate privacy policies (Electronic Privacy Information Center (EPIC) 2000), but in fact when the P3P results are visualized to Web surfers before they make a purchase decision, then they influence surfers to take more care of privacy (Gideon et al. 2006).

However, in some cases the P3P policies were expressing different privacy policies than the human-readable privacy statements on the Web sites (Cranor et al. 2008).

2.1.2.2 Policy Enforcement

In the last section, policy negotiations have been introduced. But what happens after a policy has been agreed upon? The user has to rely on the service to keep its promise. Only if there is a

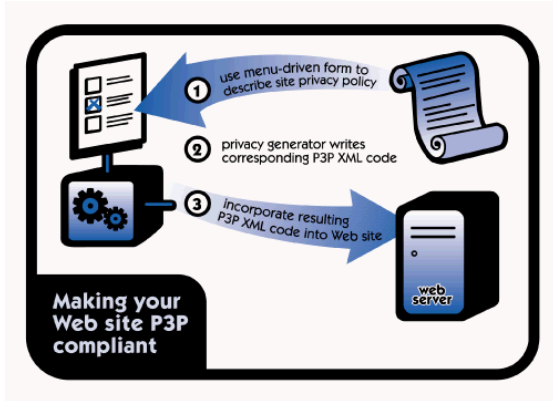


Figure 5: P3P policy generation (from W3C).

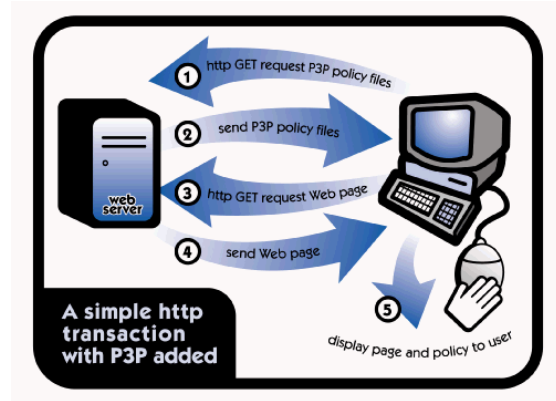


Figure 6: P3P negotiation (from W3C).

major problem with the service that gets known, an audit might check for problems with the service. To solve this problem, researchers work on the specification of systems that enforce policies. Their goal is the implementation of the whole chain of software from operating system bootup until the start of the private-information-processing application to be controlled and secure. One of the technical means that is pursued is the Trusted Computing specification (Pearson 2002). The basic idea is that a security policy is firmly attached to the data object it is intended for. Processed on computers that have secure hardware and secure operating and application software, nothing can be done to the data object that is not allowed by the attached policy. In (Cassa Mont et al. 2003), details of the necessary policy management procedures and the underlying infrastructure are described.

2.2 Opacity tools

This section presents opacity tools. Most of these tools deal with unobservable or unidentifiable access to Internet-based services. Some services try to manipulate personal data when it is sent out, e.g. the Cookie Cooker.

2.2.1 Unobservability tools

Unobservability tools are made for “invisible” access to services or data. Usually, these services are intended to protect one, two or more communicating partners from being observed by someone else. Simple encryption, e.g. of e-mail is not enough, as it is still observable who is sending e-mails to whom.

This section presents a number of working tools that were or are still available for use.

2.2.1.1 MixMaster

MixMaster is an anonymous remailer. Remailers provide protection against traffic analysis and allow sending email mail anonymously or pseudonymously. MixMaster is one of the oldest available implementations of Chaums MIX principle (Chaum 1981). Two versions of the MixMaster protocol have been made: Type I and Type II. Mixmaster is the type II remailer protocol and the most popular implementation of it (Moller et al. 2004). emailers provide protection against traffic analysis and allow sending email anonymously or pseudonymously. Mixmaster consists of both client and server installations and is designed to run on several operation systems including but not limited to BSD, Linux and Microsoft Windows. he current 2.9.x versions are stable and widely deployed. The 3.0rc releases are release candidates for the upcoming Mixmaster 3.0.

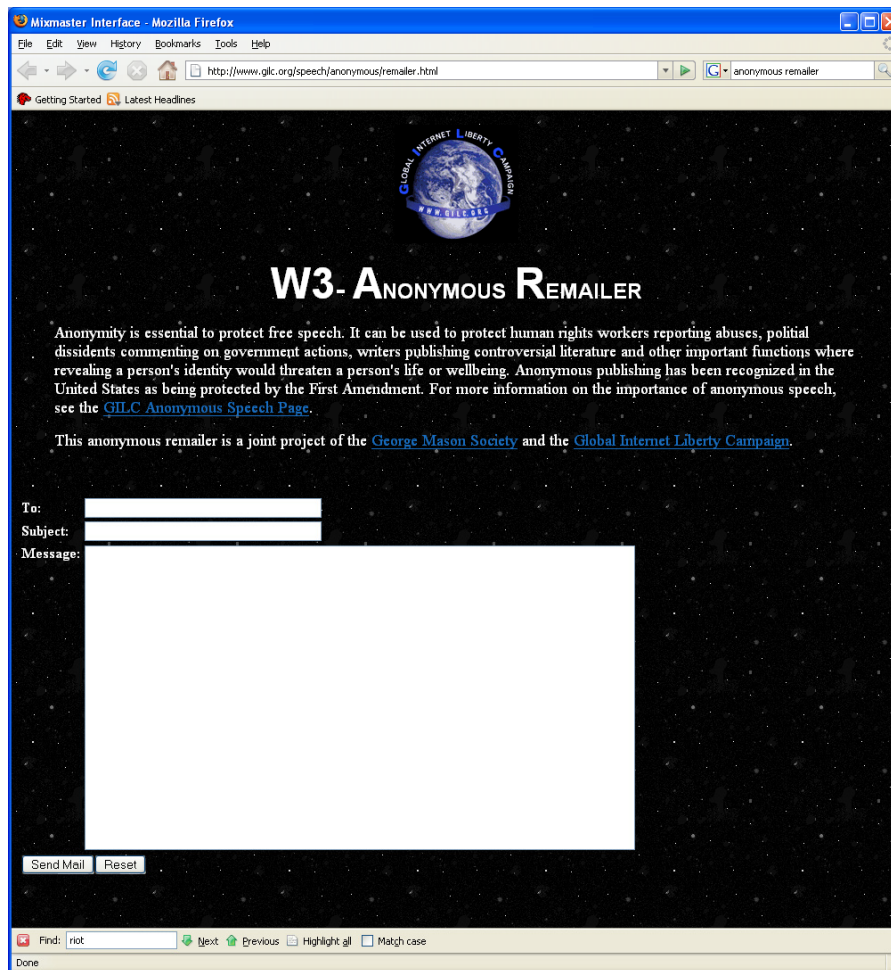


Figure 7: The W3 anonymous remailer web interface.

MixMaster can be used with PGP-encrypted e-mails with many standard e-mail programs. A few special mail clients for use with MixMasters have been programmed, and a web interface for anonymous mailing has been implemented. Most of the mail clients use the PGP cryptography software. A good overview over the clients (namely, Jack B. Nymble, John Doe, Private Idaho, Quicksilver, and Sendnym) can be found at <http://www.faqs.org/faqs/privacy/anon-server/faq/use/part6/> (12-Oct-2007). An example for a web interface is shown in Figure 7.

Name	Address	Services
Secret 101	http://secret101.com/anonymous101/index.htm	Web access for MixMaster, pre written complaint letters (in English).
GLIC Remailer	http://www.gilc.org/speech/anonymous/remailer.html	Web access for MixMaster
Dizzum Remailer	https://ssl.dizum.com/help/remailer.html	MixMaster e-mail server

Figure 8: Example remailers.

Many MixMaster servers are operated by volunteers and activist organizations. They can disappear after a period of operation, or seized by authorities for various reasons. Figure 8 lists selected MixMaster services. However, it is advisable to use a search engine looking for “Mixmaster” or “remailer” or “remailer web interface” to find lists of servers and access pages. For reliable deployment, e.g. to encourage anti-corruption whistleblowing within a large organization, it is advisable to run an own Mixmaster service, possibly chained with other external servers to create more employee confidence. MixMaster and its documentation are available at <http://mixmaster.sourceforge.net/> (as of 12-Oct-2007).

A third version or anonymous remailers is called Mixminion (Mathewson and Dingleline 2004). This is also called a type III remailer. Mixminion is a redesign of MixMaster type II that adds anonymous return addresses and improves some of the security features (Danezis et al. 2003). Mixminion and its documentation are available at <http://mixminion.net/> (as of 22-Nov-2007).

2.2.1.2 AN.ON

The AN.ON (“Anonymität Online”) project, together with its client JAP (“Java anonymous proxy”) is a joint research and development project for unobservable internet surfing. It is carried out at the Technical University Dresden and the Independent Center for the Protection of Privacy in Kiel.

This system is an implementation of an on-line MIX system (Berthold et al. 2000). Instead of connecting directly to a webserver, users take a detour, connecting with encryption through several intermediaries, so-called Mixes. JAP uses a predetermined sequence for the mixes.

Such a sequence of linked mixes is called a Mix Cascade. Users can choose between different mix cascades. Since many users use these intermediaries at the same time, the internet

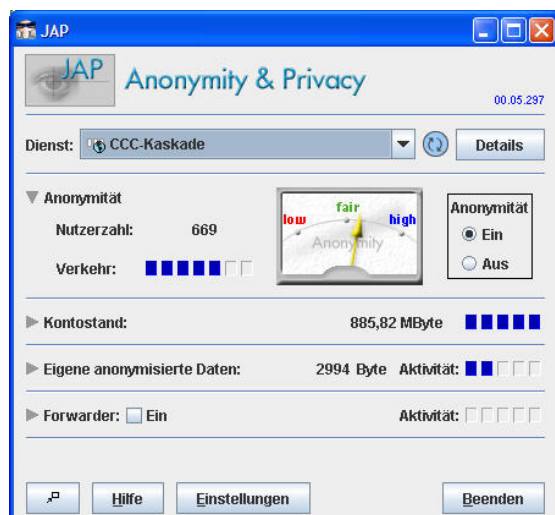


Figure 9: JAP proxy for AN.ON.

connection of any one single user is hidden among the connections of all the other users. No one, not anyone from outside, not any of the other users, not even the provider of the intermediary service can determine which connection belongs to which user. A relationship between a connection and its user could only be determined if all intermediaries worked together to sabotage the anonymization. The installation of a local Java proxy program used by web browsers establishes a connection to the AO.ON service. Several connections to servers are offered. Lately, to use a higher network bandwidth than the volunteer servers provide, commercial service can be bought and paid for. JAP encrypts all traffic that goes into the AN.ON network. However, it leaves the network unencrypted on the last step to the web server.

The project web page and programs for download are available at <http://anon.inf.tu-dresden.de/index.html> (as of 12-Oct-2007).

A company named JonDos GmbH currently offers anonymity services based on the AN.ON project. Their services include paid-for access to fast MIX cascades, and an integrated Firefox browser with pre-configured settings for using the cascades. Unlike the TOR approach below, JonDos certifies MIX operators and thus tries to establish control over who will be allowed to be part of a cascade. Jondos offers a business model for MIX node operators where they can get paid for traffic volume that is provided by their MIXes. <https://www.jondos.de/>

2.2.1.3 Onion Routing, TOR, TORPARK integration, XeroBank Browser

TOR is another approach to implement the MIX technology. TOR aims at the secure, unobservable routing of Internet connections. The project got started as "Onion Routing" (OR) by the United States Office of naval research in the 1990ies (Goldschlag et al. 1996b), (Syverson et al. 2000). The Onion Routing program is made up of projects researching, designing, building, and analyzing anonymous communications systems. The focus is on practical systems for low-latency Internet-based connections that resist traffic analysis, eavesdropping, and other attacks both by outsiders (e.g. Internet routers) and insiders (Onion Routing servers themselves). Onion Routing prevents the transport medium from knowing who is communicating with whom - the network knows only that communication is taking place. In addition, the content of the communication is hidden from eavesdroppers up to the point where the traffic leaves the Onion Routing network. More on the history of this project is written at <http://www.onion-router.net/> (12-Oct-2007).

The project was pursued non-publicly for a few years, and resurfaced in 2002 as "TOR – The Onion Router" (<http://tor.freehaven.net/>, 12-Oct-20, www.torproject.org, 22-Nov 2007). TOR has become very popular, with a large number of anonymous routers being operated by volunteers. TOR requires the installation of a local TOR client that serves as a proxy for the web browser or as an entry point to forward other types of internet connections. Setup of TOR on a PC required some IT skills, but lately, the TOR client has been built into the Firefox browser in a way that it can be started with the browser from CD-Roms or USB sticks as the TORPARK browser (see Figure 10).

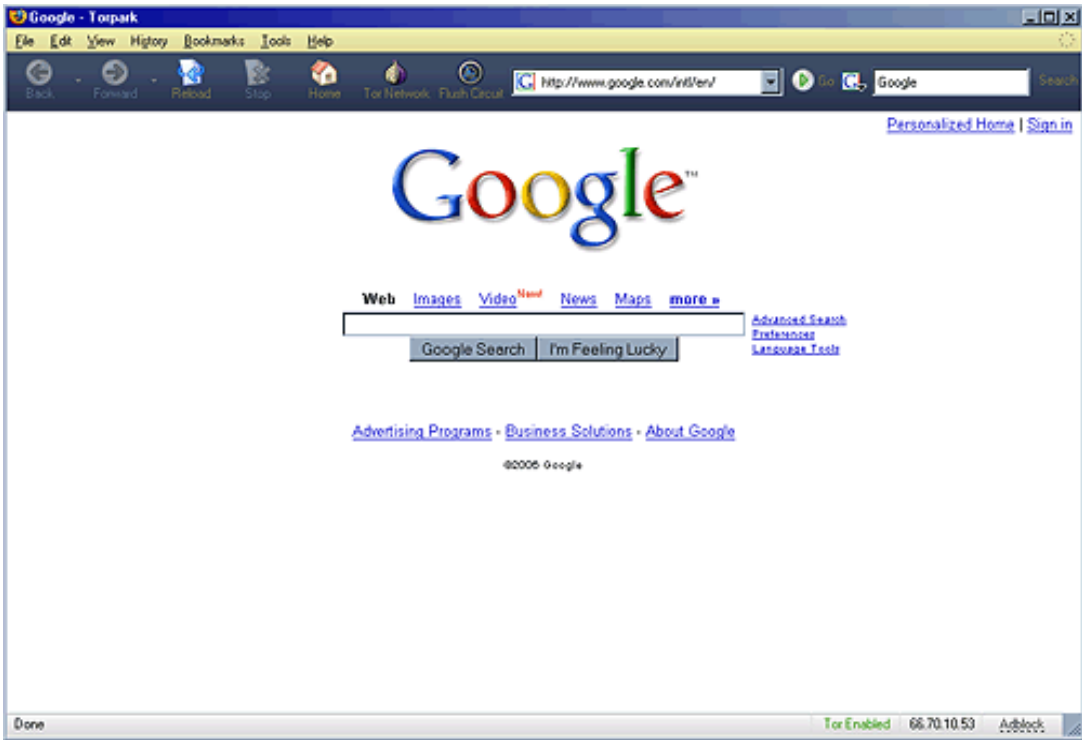


Figure 10: TORPARK browser window.

TORPARK provided a browser button to turn off anonymity, and a button to flush the TOR connection. Additionally, it has anti-advertising software installed, and enables protection from malicious content by managing scripting of browsers. TORPARK can be considered a usability milestone in the PET history, as an unskilled user can just run it and surf anonymously.

TORPARK was so successful that its creators have decided to go commercial in 2007. While TORPARK is still available for download with many shareware portals on the Web, the new development is called XeroBank or xB Browser (<http://xerobank.com/>, 12-Oct-2007). The company, XeroBank, offers private e-mail access and subscriptions for fast anonymous routing based on their own high-performance, pay-for TOR network. The xB Browser however still works with the free TOR network with the same convenience TORPARK has introduced to the PET market.

XeroBank has announced the implementation of a secure virtual machine called “xB Machine” and ready to be used on USB sticks that is intended to host privacy-sensitive applications and data (http://xerobank.com/xB_machine.html, 12-Oct-2007).

2.2.1.4 Cookie Cooker



Figure 11: Cookie Cooker.

The Cookie Cooker is a tool that manages user profiles along with their set of browser-specific cookies. A cookie is a small identifier set by a web server to mark a user. Cookies are extensively used by e-commerce web sites for profiling customers.

Cookie Cooker enables users to assign distinct sets of cookies to their own “profiles”. Then the profiles can be

activated before shopping on-line. Cookie Cooker additionally offers to swap cookies with other users (to mess up the server profiles), and offers advertising blocking functions. The goal of the tool is the unlinkability of different sets of cookies, and thus unobservability.

CookieCooker's most important features about Cookies and Identities:

- Usage of different identities at one web server,
- Random choice of the identity to use,
- Restriction of cookie storage to one session,
- Exchange of cookies between users,
- Assistance for the registration with a web service.

Cookie Cooker is shareware software, available for Windows operating systems, at <http://www.cookiecooker.de/> (12-oct-2007).

2.2.1.5 Anonymous or pseudonymous payment

Many on-line transactions involve payment of one of the involved parties. Traditional payment systems are bank transfer, electronic wire transfer or credit cards. They are non-anonymous against the transaction partner and well observable and traceable by third parties (e.g. the financial institutions). Any system that involves payment that needs to be anonymous, pseudonymous or protect identities of users therefore needs means for the secure transfer of payments. This section will present to ways of reaching this.



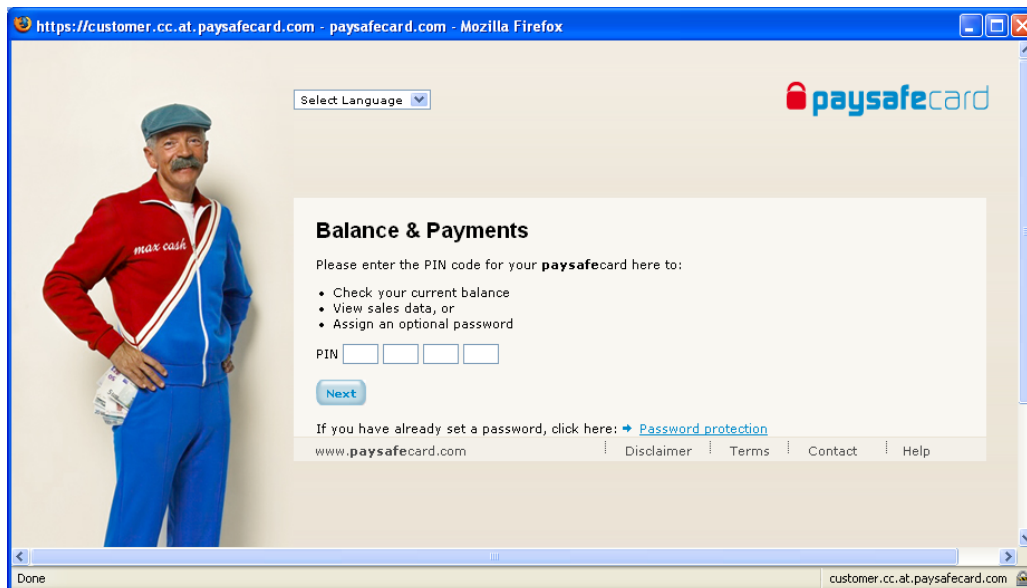
Figure 12: The paysafe card.

2.2.1.5.1 Electronic cash

In 1998, the principle of anonymous electronic cash was published (Chaum et al. 1990). In this application of a cryptographic technique called “blind signatures”, a “bank” issues cryptographic coins that are issued anonymously. Anonymous, electronic cash was designed to have all anonymity-supporting properties that real cash has. Some extra properties have been designed, which can be read about in (Schmidt et al. 1999). Soon after anonymous e-cash was invented, strong concerns about its possible misuse surfaced. In (van Solms and Naccache 1992), a perfect blackmailing scheme with electronically exchanged, anonymous currency was discussed. Many of real cash’s problems such as money laundry and illegal funds transfers were realized to worsen with anonymity. Some solutions to these problems were found in research (Sander and Ta-Shma Amnon 1999). E-Cash inventor David Chaum (Chaum et al. 1990) started the company DigiCash in 1994. Until its bankruptcy in 1998, the company tried to deploy electronic cash to the growing e-commerce market. Since the intensified “War on Terror” and tighter controls on money laundry in international financial transactions, not many banks seem overly interested in electronic cash anymore.

2.2.1.5.2 Prepaid solutions

Simple alternatives to the full-featured e-cash system with wallet software and server software are pre-paid cash cards. Many systems exist, e.g. the PaySafeCard (www.paysafecard.com). This is a simple pre-paid cardboard card with a unique code. E-shops can connect to the paysafe clearing server for collection of money. The owner of the card enters the card number for



payment, and money is taken off the card account. Upon using up the pre-paid money (cards come with a fixed amount of value), the card is replaced by a new one. Cards are bought at kiosks, super markets and newsstands. There is a version of the paysafe card that is given only to adults for the purpose of age control concerning adult entertainment and on-line gambling.

Many other vendors for pre-paid solutions are operative. Approaches range from smart cards with cash wallets up to on-line third party approaches with credit card clearing organizations. Approaches differ significantly in the degree of anonymity and the requirements on hard- and software. A recent overview can be found in (Stolte 2005).

2.2.1.6 Eternity service

British cryptographer Ross Anderson proposed the “Eternity Service” (Anderson 1996). Its goal is the reliable, distributed storage of information. Additionally, the ownership of the information is hidden to avoid sabotage to parts of the service. The concept envisioned unobservable communications with globally distributed servers that store parts of a data set that are cryptographically protected. The parts are to be stored in a decentralized fashion, and with high redundancy. By a signal the owner of the data triggers, the servers release their data shares for the owner to collect and decrypt.

Two projects currently work at implementations of such a redundant, anonymized, unobservable archive. Both are – not surprisingly – called “Eternity Service”. As of 12-Oct-2007, they can be found on these web pages:

<http://www.cypherspace.org/adam/eternity/>

<http://kocour.ms.mff.cuni.cz/~petricek/papers/eternity//>

An interesting, yet scientifically unproven observation of the author is that current peer-2-peer file sharing tools such as BitTorrent and eDonkey2000 reach a high level of file distribution and traffic obfuscation. Soon, by adding some cryptography, they might implement a large base for an eternity service.

2.2.2 Identity Management tools

User identities are an important aspect of information systems. User identities are the base for access control decisions. They are needed to express ownership of data. Identities can be part of policies, e.g. data processing policies attached to personal data. However, the full person identity with parameters such as real name, social security number, address or date of birth is not needed for all interactions and operations. According to the data protection principle of data minimization, identity management should rely on transmission and processing of the minimum amount of identification data that is required for a particular purpose. For example, an age control system that limits access to adult persons does not need to know a person's name, address or date of birth if there is another way to assert this property.

Such systems exist in practice. This section introduces two of them.

2.2.2.1 IDEMIX

The IBM "Identity Mixer" is a system for strong anonymous or pseudonymous credentials (Camenisch and van Herreweghen 2002). IDEMIX is a library of cryptographic protocols and data formats that are the result of IBM research work on various useful security protocols. Its purpose is the attestation of personal properties (aka identity information) using zero-knowledge protocols. These protocols have the property of keeping the identity secret, but accomplishing the attestation of the desired property. Many degrees of anonymity can be reached, e.g. could anonymous credentials be used to assert that a person has a drivers license and is over 25 years old whilst neither revealing the identity, the driverslicense number nor the birth date to the car rental company while querying for a price quote.

IDEMIX has been used in large research projects such as PRIME (PRIME 2003) and within the Eclipse Higgins ID management framework (an open source development project).

2.2.2.2 Liberty Alliance identity federations

The Liberty Alliance (Liberty Alliance 2007) was formed in 2001 by approximately 30 organizations to establish open standards, guidelines and best practices for federated identity management. The group was formed as an answer to Microsoft's plans to provide centralized user

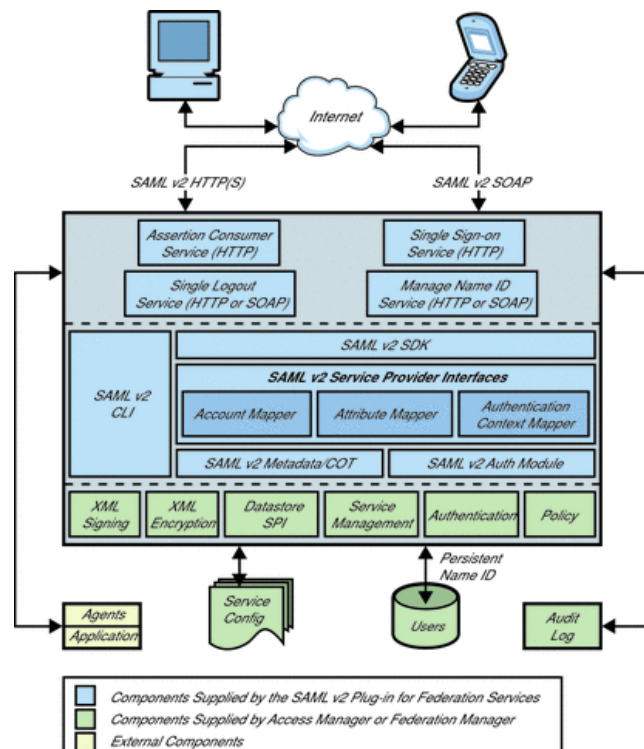


Figure 14: Sun's implementation of Liberty Identity Management using the SAML language.

management with the now discontinued passport service.

Liberty Alliance’s focus is on the question of how to manage user’s identities in a world where every person uses dozens of web services with different identities. The solution provides a set of specifications and tools that aim at interoperability in managing user identities. Many use cases exist, from forming “circles of trust”, where user identities are shared among business partners up to providing partial identity information such as a persons age or postal code to an external business partner.

While Liberty Alliance is not an explicit privacy technology, it can be deployed and configured to implement the principle of data minimization.

Liberty Alliance is a successful venture, as it has been adopted by major system integration firms and their suppliers. Its specification is open, and Liberty installations keep showing up in more and more services. However, whether a particular implementation serves the purpose of privacy-enhancement or the purpose of a more profitable user management has to be checked for every single instance.

2.2.2.3 Reachability management

Reachability management tools take care of the “invasion of privacy” threat. These tools provide measures about excluding unwanted information or communication. Invasions quite frequently happen with unsolicited advertising, SPAM mails, unwanted incoming phone calls or other forms of being reachable in electronic communication. Reachability management usaly combines the control over incoming communication on a communication channel with some form of identity management (or, in telephony terms, caller ID management).

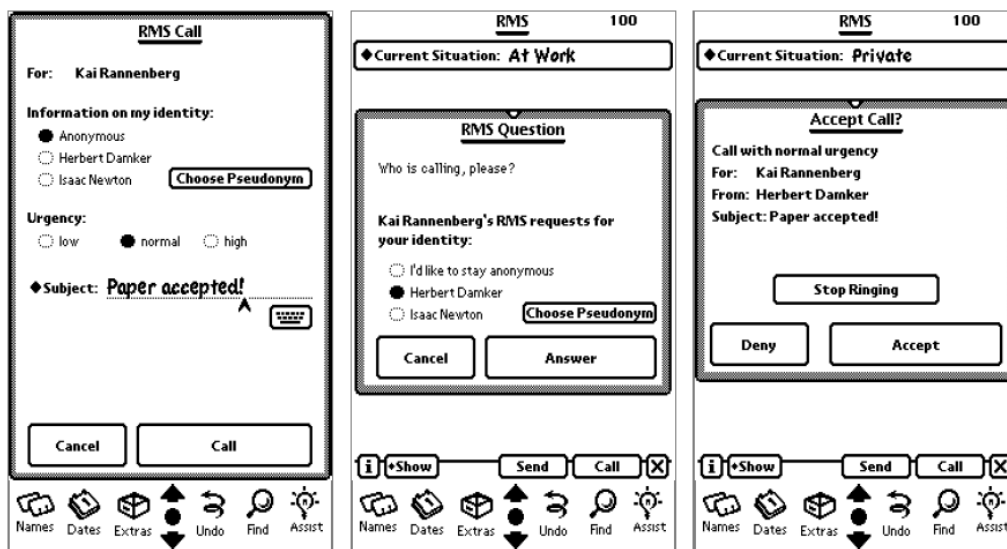


Figure 15: Reachability manager from (Reichenbach et al. 1997).

An early prototype was implemented for mobile telephones and PDAs (Reichenbach et al. 1997). Here, a software agent would inspect incoming calls, their credentials and the called person’s current reachability policy before forwarding the call to the phone. Cryptographic tokens could replace caller identity, and “emergency calls” could break the barrier by offering e-cash deposits to assure their importance.

Recent efforts aim at the problem of unwanted incoming calls. This problem is annoying on landlines, but has the potential to turn into large nuisance with nearly zero-cost IP telephony. Unwanted calls (called SPIT – Spam over Internet Telephony) are being fought off by the SPIT-AL prototype which is under research in Kiel (TNG 2007).

In practice, however, most technologies ranging from mobile phones and groupware clients on a PC up to the in-fashion social networks of the Web 2.0, reachability management is reduced to simple blacklists (banning a user) or whitelists (“link” a user or accept a user on a friends list). Much could be learned from the above projects.

2.3 Commercial products and services

Many vendors or service companies have tried to establish themselves with privacy protection. Some deliver privacy-enhancing products such as tools to counter a particular privacy threat, others offer privacy-enhanced services. A third group of vendors focuses on privacy management issues that are focusing on compliance and corporate governance. This section is mainly based on a survey by Meta Group (Meta Group 2005) with a few enhancements.

2.3.1 Privacy-enhancing products

Here, a few tools like the WebWasher and SpyBot have started a trend. These tools search for spyware, block it, and suppress advertising on web pages. These functions – as of 2007 – have been integrated by major web browsers, anti-virus-software vendors and Microsoft (in the Malicious Software Protection system). Some authors also consider encryption tools and secure deletion tools as privacy tools. All products in this category are separate software tools that have to be installed and used on a user machine.

2.3.2 Privacy-enhancing services

A path of services that started with Anonymizer.com and rapidly developed in a large number of small businesses that offer re-routed, anonymous or encrypted access to the Web, the internet or e-mail. Some even offer anonymous home page hosting or blogging against cash sent in by postal mail. While one of the efforts from the PET community (ZeroKnowledge systems) failed, the technically less sophisticated vendors are still there. While Anonymizer.com sells anonymity as a product, many other vendors such as your-freedom.net (www.your-freedom.net/) target users who want to obscure what they do on the Internet (e.g. accessing games, messaging or auctions from the workplace, using encrypted tunnels to get past firewalls and filters).

With the spread of blogging, services take shape that will search the Web for information about a person and deliver a paid-for dossier. Some services promise to remove the information against a fee, but do not offer details on how to reach this against long-term search engine indexes.

2.3.3 Privacy management business software

Some of the large software and computer vendors have started to implement privacy management in their business software. On this end of the scale, privacy management usually is compliance management, where a corporation must know and manage private information on computers within some legal regulation.

IBM offers the Tivoli Privacy Manager (<http://www-306.ibm.com/software/tivoli/products/privacy-mgr-e-bus/>), a policy enforcement mechanism for business data bases and systems that helps corporate privacy officers to manage information privacy in a company.

Hewlett-Packard implements privacy and identity management in its "HP Openview Select" family of business software. The HP approach follows a data lifecycle management that focuses on privacy (<http://www.hpl.hp.com/personal/mcm/Projects/PrivacyAwareIdentityLifecycleManagement/PrivacyAwareIdentityLifecyclemanagement.htm>).

Several systems for privacy audit support have been implemented.

3 Conclusion

This study shows the availability of privacy-enhancing technology. Particularly, tools for unobservability and identity protection have reached a high level of maturity. Some concepts, such as trusted platforms, anonymous credentials or DRM technology application for information tracking have not entered the market yet. However, for the purpose of managing personal data in information systems, many working building blocks are available. They should be taken advantage of.

4 Appendix

4.1 References

- Anderson, R. (2001) Security Engineering, Wiley, New York.
- Anderson, R. J. (1996) The Eternity Service, *Pragocrypt 1996*, Prag, pp. 11.
- Berthold, O.; Federrath, H. and Köpsell, S. (2000) Web MIXes: A system for anonymous and unobservable Internet access, *In the Proceedings of Designing Privacy Enhancing Technologies: Workshop on Design Issues in Anonymity and Unobservability, July 2000*, pp. 115-129.
- Blarkom, G. W.; Borking, J. and Olk, J. (2003) Handbook of Privacy and Privacy-Enhancing Technologies, College bescherming persoonsgegevens, The Hague.
- Bramhall, P.; Hansen, M.; Rannenber, K. and Roessler, T. (2007) User-centric identity management, : New trends in standardization and regulation." *IEEE Security & Privacy* (5): pp. 64 - 67.
- Brand, S. (2005) ISO/IEC/JTC1/SC27/WG3 COMMITTEE MEETING, http://www.incits.org/tc_home/CS1/2005docs/cs1050163.htm, accessed 16.Nov. 2006.
- 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.
- Cassa 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.

- Chaum, D. (1981) Untraceable electronic mail, return addresses, and digital pseudonyms, *Communications of the ACM* (4:2), pp. 84-88.
- Chaum, D.; Fiat, A. and Naor, M. (1990) Untraceable electronic cash, in: S. Goldwasser (Eds.): *Proceedings of the 8th Annual International Cryptology Conference on Advances in Cryptology 1988*, Berlin, Springer, pp. 319-327.
- 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,.
- Cranor, L. F.; Reagle, J. and Ackermann, M. S. (1999) Beyond Concern: Understanding Net User's Attitudes About On-line Privacy: AT&T Labs-Research Technical Report TR 99.4.3.
- Cranor, L.; Egelman, S.; Sheng, S.; MacDonald, A. and Chowdhury, A. (2008) (forthcoming) P3P Deployment on Websites, *Electronic Commerce Research and Applications* (7: pp. unknown.
- Danezis, G.; Dingledine, R. and Mathewson, N. (2003) Mixminion: Design of a Type III Anonymous Remailer Protocol, in: IEEE Computer Society (Eds.), *IEEE Symposium on Security and Privacy*, Oakland, California, USA, IEEE Computer Society, pp. 2-15.
- Deng, M.; Fritsch, L. and Kursawe, K. (2006) Personal Rights Management,,: Taming camera-phones for individual privacy management, in: G. Danezis and P. Golle (Eds.): *Privacy Enhancing Technologies - Proceedings of the 6th workshop on privacy-enhancing technologies PET2006*, 29.Jun.2006, Berlin, Springer.
- Electronic Privacy Information Center (EPIC)(2000) Pretty Poor Privacy: An Assessment of P3P and Internet Privacy,Electronic Privacy Information Center (EPIC).
- European Commission (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).
- FIDIS (2003) Future of Identity in the Information Society,,: The IST FIDIS Network of Excellence, www.fidis.net, accessed 6.11.2006.
- FIDIS(2007) FIDIS Deliverable D7.5: Profiling the European Citizen,,:Cross-Disciplinary Perspectives, European Union IST FIDIS Project.
- 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.
- Friedmann, E. J. and Resnik, P. (1999) The social cost of cheap pseudonyms, *Journal of Economics and Management Strategy* (10:2), pp. 173-199.
- Fritsch, L.; Scherner, T. and Rannenber, K. (2006) Von Anforderungen zur verteilten, Privatsphären-respektierenden Infrastruktur, *Praxis in der Informationsverarbeitung und Kommunikation (PIK)* (29:1), pp. 37-42.
- 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 .

- Gideon, J.; Egelman, S.; Cranor, L. and Acquisti, A. (2006) Power Strips, Prophylactics, and Privacy, Oh My! *Symposium On Usable Privacy and Security (SOUPS 2006)*, Pittsburgh.
- Goldschlag, D. M.; Reed, M. G. and Syverson, P. F. (1996a) Hiding Routing Information, in: R. Anderson (Eds.): *Information Hiding*, Berlin, Springer, pp. 137-150.
- Goldschlag, D. M.; M. G. R. and Syverson, P. F. (1996b) Hiding Routing Information, *In the Proceedings of Information Hiding: First International Workshop, May 1996*, pp. 137-150.
- Hansen, M. and Pfitzmann, A. (2007) Anonymity, Unobservability, and Pseudonymity - A Proposal for Terminology, v0.29, Dresden.
- 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.
- ISO (1999) ISO 15408 The Common Criteria for Information Security Evaluation.
- 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.
- KPMG Canada (2003) A Retailer's guide to Privacy Risk Management, KPMG LLP, Canada.
- Kohlweiss, M.; Fritsch, L.; Radmacher, M.; Hansen, M. and Krasemann, H. (2004) Overview of existing assurance methods: PRIME Delivery D5.1.a, EU IST PRIME Project.
- Kohlweiss, M.; Gedrojc, B.; Fritsch, L. and Preneel, B. (2007) Efficient Oblivious Augmented Maps: Location-Based Services with a Payment Broker, *Proceedings of the 7th workshop on Privacy-enhancing technology*, Ottawa, Canada.
- Lacoste, G.; Pfitzmann, B.; Steiner, M. and Waidner, M. (2000) SEMPER - Secure Electronic Marketplace for Europe, Springer, Berlin.
- Liberty Alliance (2007) The Liberty Alliance project, [=96 - Buchholz 2003 Liberty Alliance Pro. =], accessed 16-Oct-2007.
- Marchiori, M.; Cranor, L.; Langheinrich, M.; Presler-Marshall, M. and Reagle, J. (2002) The Platform for Privacy Preferences 1.0 (P3P1.0) Specification W3C, The World Wide Web Consortium.
- Mathewson, N. and Dingledine, R. (2004) Mixminion: Strong Anonymity for Financial Cryptography, in: A. Juels (Eds.): *8th International Conference on Financial Cryptography (FC04)*, 21-Sep-2004, Berlin, Springer, pp. 227-232.
- Meta Group (2005) Privacy Enhancing Technologies Ministry of Science, Technology and Innovation, Ministeriet for Videnskab, Teknologi og Udvikling, København, Denmark.
- Moller, 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 29-Dec-2004.
- Müller, M. (2004) Standards for Geographic Location and Privacy: IETF's Geopriv, *Datenschutz und Datensicherheit (DuD)* (28:5), pp. 297-303.
- Odlyzko, A. (2003) Privacy, Economics, and Price Discrimination on the Internet: Extended Abstract.

- Oinonen, K.(2002) TR101 - LIF Privacy Guidelines.
- PRIME (2003) Privacy and Identity Management for Europe, : The IST PRIME Project, www.prime-project.eu, accessed 6.11.2006.
- Pearson, S. (2002) Trusted Computing Platforms. TCPA Technology in Context, Prentice Hall International.
- Pfitzmann, A. and Hansen, M.(2003) Anonymity, Unobservability, and Pseudonymity - A Proposal for Terminology, :v0.21.
- 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.
- Pfitzmann, A.; Pritfzmann, 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.
- Preibusch, S. (2005) Implementing privacy negotiation techniques in e-commerce, *E-Commerce Technology, Proceedings of the Seventh IEEE International Conference on E-Commerce (CEC'2005)*, 19-22 July 2005, IEEE Computer Society, pp. 387-390.
- Rannenber, K. and Iachello, G. (2000) Protection Profiles for remailer Mixes -- Do the New Evaluation Criteria Help? *Proceedings of the 16th ACSAC*, IEEE Press, pp. 107-118.
- Reichenbach, M.; Damker, H.; Federrath, H. and Rannenber, K. (1997) Individual Management of Personal Reachability in Mobile Communication, in: L. Yngström and J. Carlsen (Eds.): *Information Security in Research and Business ; Proceedings of the IFIP TC11 13th international conference on Information Security (SEC'97)*, May 1997, London, Chapman & Hall, pp. 164-174.
- Sander, T. and Ta-Shma Amnon, (1999) On anonymous electronic cash and crime, *ISW'99*, pp. 5.
- Schmidt, J.; Schunter, M. and Weber, A. (1999) Can Cash be Digitalised? in: G. Müller and K. Rannenber (Eds.): *Multilateral Security in Communications, Vol. 3: Technology, Infrastructure, Economy*, München, Addison-Wesley Longman, pp. 301-320.
- 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.
- Stolte, B. (2005) Location-based Services: Sicheres e-payment von ortsbasierten Diensten, Frankfurt am Main.
- Syverson, P.; T., G.; Reed, M. and Landwehr, C. (2000) Towards an Analysis of Onion Routing Security, *In the Proceedings of Designing Privacy Enhancing Technologies: Workshop on Design Issues in Anonymity and Unobservability, July 2000*, pp. 96-114.
- TCG (2007) The Trusted Computing Group, <http://www.trustedcomputinggroup.org>, accessed 16-Jun-2007.
- TNG (2007) Project SPIT-AL filter, <http://www.spit-abwehr.de/>, accessed 16-Oct-2007.
- Zuccato, A. (2005) Holistic Information Security Management Framework, Karlstadt University Universitetsstrycjeriet, Karlstadt.
- van Solms, S. and Naccache, D. (1992) On blind signatures and perfect crimes, *Computers and Security* (11:6), pp. 581-583.

4.2 Index

- AN.ON Mix, 22
- anonymous payment, 25
- audit, 18
- challenges of information privacy, 8
- checklists, 15
- classification, 11
- Cookie Cooker, 24
- data protection authorities, 18
- Datenschutz-Gütesiegel, 16
- detection tools, 18
- e-cash, 26
- electronic cash, 25
- Eternity Service, 26
- fingerprints, 18
- IDEMIX, 27
- IDEMIX anonymous credential system, 17
- identity management, 17, 27
- integration of PET, 17
- Liberty Alliance, 27
- Mix, 7
- Mix Cascade, 22
- MixMaster anonymous remailer, 21
- Onion Routing, 23
- opacity, 10, 20
- opacity tools, 10
- P3P, 19
- payment, 25
- PET, 8
- PET award, 8
- PET functionality, 11
- PET terminology, 9
- policy management, 19
- policy enforcement, 20
- pre-paid cash cards, 26
- privacy audit, 15, 18
- Privacy Audit Framework, 16
- privacy breaches, 9
- privacy certificate, 18
- privacy cost, 8
- Privacy enhancing technology, 8
- privacy preferences negotiation, 19
- privacy risks, 8
- privacy seal, 18
- privacy seals, 15, 17
- Reachability management, 28
- research, 17
- stakeholders, 14
- standards, 15
- steganography, 18
- sticky policies, 17
- taxonomy of privacy, 8
- TOR Mix, 23
- TORPARK browser, 24
- transparency, 10, 17
- transparency tools, 10
- Trusted Computing, 17, 20
- Unobservability, 20
- watermarking, 18
- watermarks, 18
- XeroBank Browser, 24