



Ministry of Science
Technology and Innovation

Privacy Enhancing Technologies

META Group Report v 1.1

March 28, 2005.



METAGROUP

TABLE OF CONTENTS

1	Introduction	4
2	Management Summary	5
3	Protecting Privacy	8
3.1	WHAT IS PRIVACY?	8
3.2	HOW IS PRIVACY RELATED TO INFORMATION SECURITY?	9
3.3	WHAT ARE THE PRIVACY THREATS?	9
4	Charting the PET Landscape	11
4.1	PRIVACY PROTECTION	12
4.2	PRIVACY MANAGEMENT	13
5	Technology Features Overview	14
5.1	CRM PERSONALIZATION	15
5.2	APPLICATION DATA MANAGEMENT	15
5.3	BROWSING PSEUDONYMS	15
5.4	VIRTUAL EMAIL ADDRESSES	15
5.5	TRUSTED THIRD PARTIES	15
5.6	SURROGATE KEYS	16
5.7	ENCRYPTING EMAIL	16
5.8	ENCRYPTING TRANSACTIONS	16
5.9	ENCRYPTING DOCUMENTS	16
5.10	FILTERING EMAIL SPAM	16
5.11	FILTERING WEB CONTENT	17
5.12	BLOCKING POP-UP WINDOWS	17
5.13	SPYWARE DETECTION AND REMOVAL	17
5.14	BROWSER CLEANING TOOLS	17
5.15	ACTIVITY TRACES ERASOR	17
5.16	HARD DISK DATA ERASOR	18
5.17	PRIVACY POLICY GENERATORS	18
5.18	PRIVACY POLICY READERS/VALIDATORS	18
5.19	PRIVACY COMPLIANCE SCANNING	18
5.20	IDENTITY MANAGEMENT	18
5.21	BIOMETRICS	19
5.22	SMART CARDS	19
5.23	PERMISSION MANAGEMENT	19
5.24	MONITORING AND AUDIT TOOLS	19
5.25	FORENSICS TOOLS	19
6	Use cases	20
6.1	ANONYMOUS BUSINESS RELATIONS	20
6.2	COMMERCE CHAIN MANAGEMENT	20
6.3	PRIVACY REQUIREMENTS IN PUBLIC SERVICE	21
6.4	RADIO FREQUENCY IDENTIFICATION DEVICES (RFID)	21
6.5	FINANCIAL TRANSACTIONS	21
6.6	ANONYMOUS SHOPPING	22
6.7	POSITIONAL INFORMATION	22
6.8	HEALTH CARE SERVICES	22
7	Major PET players	24
7.1	PRIVACY PROTECTION	24
7.2	APPLICATION TOOLS	24

7.3	ANONYMIZER PRODUCTS AND SERVICES	24
7.4	ENCRYPTION TOOLS	24
7.5	FILTERS AND BLOCKERS	24
7.6	TRACK AND EVIDENCE ERASORS	25
7.7	PRIVACY MANAGEMENT.....	25
7.8	INFORMATIONAL TOOLS.....	25
7.9	ADMINISTRATIVE TOOLS	25
8	Relevant groups influencing public privacy perception	26
9	What are the problems	27
9.1	PRIVACY IN LEGACY APPLICATIONS WILL REQUIRE ADDITIONAL CHANGES	27
9.2	USER CONTROLLED PRIVACY CAN IMPACT USER RIGHTS	27
9.3	EXPLOITING DESIGN FLAWS	27
9.4	LACK OF STANDARDIZED PRIVACY SOLUTIONS	28
9.5	REDESIGN OF EXISTING SYSTEMS WILL TAKE TIME	28
9.6	CRITICAL SYSTEMS REQUIRE BACK DOOR FUNCTIONALITY	28
9.7	POOR UNDERSTANDING OF PRIVACY ISSUES	28
9.8	PRIVACY REQUIRES USER TRUST	28
9.9	CLASSIFICATION OF PRIVATE DATA REQUIRES NEW CONCEPTS.....	29
9.10	LEGISLATION NEEDS CLEAR REQUIREMENTS	29
9.11	PRIVACY IS NOT ALWAYS THE FIRST PRIORITY	29
10	Valuable initiatives	30
10.1	PLATFORM FOR PRIVACY PREFERENCES (P3P) PROJECT.....	30
10.2	PRIVACY ENHANCING TECHNOLOGY TESTING & EVALUATION PROJECT (PETTEP).....	30
10.3	ENTERPRISE PRIVACY AUTHORIZATION LANGUAGE (EPAL).....	31
10.4	PRIVACY AND IDENTITY MANAGEMENT FOR EUROPE (PRIME) PROJECT	31
11	Future perspectives	32
11.1	WHAT DRIVES MARKET DEMAND FOR PETS?	32
11.2	HOW WILL PETS BE EVOLVING OVER THE NEXT FEW YEARS?	33
11.3	WHICH CATEGORIES OF PETS WILL HAVE THE GREATEST IMPACT?	33
11.4	WHO WILL PROVIDE THE PET SOLUTIONS?.....	34
11.5	WHERE CAN INTERNATIONAL COORDINATION HELP?	34
12	Privacy Trends and Issues	35
12.1	TREND: DEMONSTRATION PROJECTS	35
12.2	TREND: ACCEPTANCE SURVEYS.....	35
12.3	TREND: PRIVACY CONSIDERATIONS IN E-GOVERNMENT SERVICES	35
12.4	TREND: REVIEW OF PUBLIC E-SERVICES INCLUDES PRIVACY	36
12.5	TREND: CORPORATE PRIVACY SOLUTIONS ARE ADVANCING	36
12.6	ISSUE: LACK OF A TRUST MODEL	36
12.7	ISSUE: SPECIFIC PROVISIONS ARE LIMITING DESIGN CHANGES	36
12.8	ISSUE: NEW TECHNOLOGIES ARE CHALLENGING OLD LEGISLATION	36
12.9	ISSUE: LACK OF STANDARDS.....	37
12.10	ISSUE: PRIVACY REQUIRES AN ARCHITECTURE	37
Appendix A: Methodology.....		38
Appendix B: References.....		40

1 INTRODUCTION

Implementing the principle of open public administration in today's eGovernment initiatives represents a significant challenge to the architects of both administrative procedures and the supporting IT systems: Protecting the privacy of the citizen, while providing rich, coherent services spanning multiple administration areas, calls for new design principles and technologies.

The term Privacy Enhancing Technologies (PETs) represents a spectrum of both new and well-known techniques to minimize the exposure of private data, for users of electronic services in the information society. However, the term does not have a widely accepted definition, and the scope of PETs is often depending on the usage scenario.

This study has been initiated by the Danish Ministry of Science, Technology and Innovation, in order to improve the ministry's background knowledge of PETs and to describe the possible scenarios of use. An important purpose of this study is to propose a high level classification of Privacy Enhancing Technologies, with a corresponding classification of the most significant products on the market and their features. The report is intended to help officials evaluate the feasibility of employing PET in the electronic communication between public administration, private enterprises and consumers. The scope of the analysis is to provide a European view, focused on the situation in Denmark, UK, Germany and common EU activities. Global trends will be included where applicable.

To explore this issue in depth, META Group has carried out research with European thought leaders with a view of understanding how the players in major information security initiatives are addressing the privacy challenge. META Group conducted a series of in-depth interviews with key persons in Europe during the summer and fall of 2004. The research yielded a wide range of views on how public and private organizations in Europe are viewing the privacy issue, and which technologies they use to provide solutions. Participants in the research were distributed across the manufacturing, finance, telecommunications, government, and utility sectors.

2 MANAGEMENT SUMMARY

For the Danish Ministry of Science, Technology and Innovation, META Group has carried out research with European thought leaders with a view of understanding how the players in major information security initiatives are addressing the privacy challenge.

Protecting privacy is focused on reducing the information collected and stored to a minimum, and deleting the information, as soon as it has served its purpose. But these principles are challenged by the individual's need for convenient electronic services, and by the need for efficiency of eBusiness or eGovernment transactions. Most of today's e-services are relying on stored data, identifying the customer, his preferences and previous record of transactions. However, combining such data will in many cases constitute an invasion of privacy. The purpose of Privacy Enhancing Technologies (PETs) is to protect the privacy of individuals, while still enabling them to interact with other parties in a modern society, using electronic communications.

The term Privacy Enhancing Technologies (PETs) represents a spectrum of both new and well-known techniques to minimize the exposure of private data, for users of electronic services in the information society. However, the term does not have a widely accepted definition, and the scope of PETs is often depending on the usage scenario.

META Group's research revealed a broad consensus regarding the need for privacy, and a general recognition of the fact, that the design of today's IT systems and networks is a serious challenge to privacy: The public IT infrastructure should be designed, or redesigned, to put the user in control of his own personal information and his private sphere. But given the extent of the infrastructure, and the considerable commercial and state interests in the collection of personal data, this will not happen overnight. In the meantime, a number of Privacy Enhancing Technologies can be used to improve the protection of privacy in selected areas and cases.

The current privacy threats fall in three major classes:

- A) Loss of confidentiality
- B) Identity theft
- C) Unsolicited messages (spam).

Privacy Enhancing Technologies can be used to improve the protection of privacy in order to minimize the threats of all three classes: Some of the privacy tools are actively involved in the information storage and transport, while others are supporting the administration of privacy. This report proposes two main categories of Privacy Enhancing Technologies: Privacy Protection and Privacy Management. The first category contains tools and technologies that are actively involved in protecting the privacy, e.g. by hiding the private information, or by eliminating the need for personal identification. The second category, Privacy Management, contains tools and technologies that support the administration of privacy rules, rather than processing the information itself.

The purpose of the Privacy Enhancing Technologies is to obtain one or more of the three main privacy aspects:

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

The report organizes the Privacy Enhancing Technologies into subcategories, and it explains how the technical features of the privacy solutions support each of the privacy aspects mentioned above.

A number of use cases illustrate common situations from the “old world”, where the protection of privacy traditionally has been an integrated part of the transaction, e.g. in recruiting agencies. When such transactions are implemented using electronic services, special care must be taken to protect the privacy of the individuals, and the use of privacy tools will be relevant. Other use cases show how the deployment of new technologies, such as Radio Frequency Identification Devices (RFID), for remote identification of products sold in a supermarket, can form a privacy threat for the consumer. Here, the new technology must have a privacy-aware design in order to gain wide acceptance.

Most of today’s Privacy Enhancing Technologies are conceptually add-on products, designed to compensate flaws in original design of IT systems and information handling procedures. But adding PETs to existing legacy applications can impact the efficiency, reliability and robustness of the service. To make existing systems “privacy-compliant”, the design principles must be revised, and central parts of the design must be reworked. The effort required to conduct such a process is considerable, and the timeframe is very large.

The overall maturity of privacy solutions is currently considered low. Standardization of privacy features and solutions is yet to come – the current PET solutions are rarely interoperable (with a few notable exceptions), because a common understanding of the concepts and requirements has not been established. However, still awaiting the formal standardization of PETs, some best practices have emerged in the area of privacy policy generation and compliance control.

Many industries already use PETs, especially when more parties have to share some data, while other data must be kept separate. The PETs used in such cases will often be embedded in custom-built solutions, rather than being added to a standard system. It is expected that tomorrow’s privacy solutions will be an integrated part of public and private administrative solutions, based on an architecture, where privacy has been an integral part of the design criteria.

Today’s public administrative systems are only including limited privacy protecting functionality, while the law requires the administrative staff to follow procedures that protect the citizen’s privacy. Unfortunately, many E-Government service developments follow this trend, by not rating privacy principles high in their basic design criteria. Privacy-aware design (of data, applications and procedures) is key to obtaining privacy, but very few examples of this have been seen.

It is expected, that companies delivering Internet shopping and other electronic services will respond to the customer’s need for privacy, by offering appropriate functionality, such as

customer anonymity, when the customer prefers it. In the future, privacy features are likely to be integrated in the IT infrastructure, as a part of the application platforms.

The most significant problem for the adoption of Privacy Enhancing Technologies is the poor understanding of privacy issues in the general public. Without this understanding, there is little demand for PETs, and no strong drivers for the evolution of privacy solutions. Many users have no perception of the value of privacy, because they have not experienced the consequences of losing it.

But awareness for privacy issues is clearly rising. A factual rise in abuse of identities (as it is currently happening in the United States, and increasingly also in Europe) is motivating citizens to more personal involvement in guarding their private data.

However, the increase in terror threats has influenced the public opinion of privacy in the opposite direction: Most people will now accept increased public control, sacrificing their privacy for the purpose of personal security. The citizens generally have high trust in the public authorities and are not expecting abuse from this side.

Market acceptance of privacy enhancing technologies is expected to be polarized in the future, driven by different consumer attitudes: The majority trusts the authorities and doesn't care about privacy in their daily life, while a small minority will be worried about their privacy, and look for privacy protection, when using electronic services.

Our research indicates, that a natural first step towards better protection of privacy would be to support and encourage the use of the *informational privacy tools* to create and implement privacy policies on public and private web sites. This could create the required broad awareness of privacy issues, and lead the way for more operational privacy solutions.

Secondly, introducing common principles for identity management – with integrated privacy features – could support the introduction of *privacy management tools* in selected areas, where the user perceives a benefit from simplified data access and control procedures.

Establishing legal requirements for PET in specific situations is difficult without a systematic approach – additional research in this field is required, before the privacy requirements can be defined precisely and consistently, so that they can form basis for legislation. Further complicating is the fact that private data easily crosses borders, whereas legislation, even within Europe, is still struggling with an easy way of handling cross-border privacy concerns.

In Europe, the EU privacy directive has been widely implemented in national legislation, regulating e.g. exchange of private data between public administrations. The directive builds on many earlier sources, such as the OECD privacy principles, but it does not provide a comprehensive conceptual framework. International cooperation in the privacy field is expected to be most useful in areas of research and development of common terminologies and concepts for classification of private data, issues and usage scenarios.

3 PROTECTING PRIVACY

3.1 WHAT IS PRIVACY?

More than a century ago, US Supreme Court Justice Louis Brandeis defined privacy as "the right to be let alone", which he said was one of the rights most cherished by Americans. But the vision of being "let alone" no longer suffices to define the concept of privacy in today's digital environment, where electronic communication is widely used in the individual's interaction with other individuals, businesses and public institutions. Today, privacy refers to the ability of the individual to protect information about him from being exposed to other parties.

Many kinds of information are generally considered private by nature, typical examples of sensitive private information are health data, financial data and records of religious or political conviction. But, depending on the context, even trivial information such as shopping patterns, phone call information or geographical position can be highly sensitive.

A key element in privacy is the possibility of linking different pieces of information. Combining information from different sources can constitute a violation of the privacy of an individual, even if the information from each source is considered harmless. This is possible, when two or more sources of information are using the same unique identifier in their records, such as a social security number. When the information sources are using the same identifier (key), there is obviously a possibility that their information can be combined, and possibly violate the privacy of an individual.

For this reason, the identifier fields of personal information are often considered the most sensitive part of the information, and protected in the name of privacy. But it must be understood, that any information that is related to an individual can be used to trace personal information by linking different information sources. Linking fields could be telephone number, street address or shoe size. Not all these fields are unique identifiers, but combining several factors will often enable unique identification of an individual, and hence make it possible to combine the information.

Protecting privacy is often focused on reducing the information collected and stored to a minimum, and deleting the information, as soon as it has served its purpose. But these principles are challenged by the individual's need for convenient electronic services, offered as eBusiness or eGovernment transactions. Here, the value of the service is often depending on having a secure identification of the individual, and having access to relevant background information about him.

Whether the personal information is physically controlled by the individual – or it resides with trusted third parties, business partners or authorities – the protection will often require electronic tools that control the access to and use of the information, according to the individual's decision.

A wide spectrum of tools and technologies have been developed to enhance the privacy of electronic solutions, most of these are targeting Internet based communications and transactions. The purpose of these Privacy Enhancing Technologies (PETs), is to protect the privacy of individuals, while still enabling them to interact with other parties in a modern society, using electronic communications.

3.2 HOW IS PRIVACY RELATED TO INFORMATION SECURITY?

The concept of “Information Security” is used in many different meanings. When we express a need for security, the statement reflects one or more anticipated threats that we want to be protected against. It could be loss of information, unauthorized data changes - or exposure of secret information. Depending on the anticipated threat, we employ different measures to protect our information, such as backup copies, encryption or access control.

The requirement of privacy is the specific need for protection against loss of confidentiality for person related information. A number of general security measures are supporting privacy as well as other security needs. Loss of privacy is only one of many threats to our personal information, hence the privacy requirement must be seen in connection with other requirements to information security.

Some of the Privacy Enhancing Technologies that are included in this study can be used for other purposes than the protection of privacy. They are general tools, supporting multiple security aspects, such as confidentiality or integrity, while at the same time protecting the privacy of the information owner. However, in this report we will focus on the privacy related threats, and the technologies used to guard us against them.

3.3 WHAT ARE THE PRIVACY THREATS?

It is often argued, that loss of privacy is not representing a problem for individuals that have nothing to hide: Displaying personal details in the public space, however, can have many adverse effects: Due to the fact, that today’s electronic infrastructure makes it both easy and valuable to collect information about individuals, it must be expected that any exposed personal information can be exploited. Today, the main threats fall in three major classes: A) Loss of confidentiality, B) Identity theft , and C) Unsolicited messages (spam).

A) Loss of confidentiality – abuse of personal information.

In the same way as the individual can feel offended by physical intrusion to his home or other private areas, the intrusion into personal electronic records or the exposure of personal information is most often considered an offence or a threat to the individual.

B) Identity theft.

In many situations, such as health care services or financial transactions, a simple token of identity such as the social security number (in Denmark: CPR number) is accepted as the sole proof of identity. This is convenient for the citizen, but opens up the possibility of fraud, based on false identity. The obvious risk is financial loss caused by transactions supported by the stolen identity token, and exposure of information, to which the token gives access. But identity theft can have even worse consequences: By using crafted procedures, a simple identity token can be used to obtain other false certificates, passport, drivers license, credit cards, etc. Since last year, there are more and more instances where criminals set up fake websites of financial institutions and trick people, often via email, to reveal their confidential information. Such identity theft is often also called “phishing”. Naturally, this creates a significant threat to the targeted individual.

C) Unsolicited messages (spam).

Perhaps the most visible driver for privacy protection is the fight against unsolicited electronic messages (spam). Unlike the physical world, where addressing individuals have a significant cost (e.g. in terms of postage or work effort), most electronic media have almost no transaction cost, and is therefore ideal for mass mailing of commercial offers etc. The most used vehicle for sending spam is by far email on the Internet, but also many other communication channels are abused for this purpose, e.g. conferencing systems, weblogs, short message service (SMS) and newsgroups.

A number of different methods, technologies and products have been developed to protect the individual from these threats, by hiding the identity of the individual, controlling the access to his private information, deleting the sensitive information or blocking (filtering) unwanted messages. Many of these tools are generally called Privacy Enhancing Technologies (PETs), but currently, no widely accepted definition of PETs has been established.

The main purpose of this analysis is to propose a high level classification of Privacy Enhancing Technologies, with a corresponding classification of the most significant products on the market and their features.

4 CHARTING THE PET LANDSCAPE

It is generally recognized, that the use of information technology can create problems for the protection of privacy, because the electronic media have a different set of attributes than the documents of the traditional paper world: The information is no longer bound to one physical place, it can be copied, moved or even changed without trace. Protecting electronic information from exposure, alteration or loss has not been a major design criteria for the networks, hardware and software, that currently contain and process our personal data. Since the early days of the Internet, some features have been added to improve data protection, but the core design of the network still has a number of serious flaws, that can be exploited to gather private information, and carry out a number of fraudulent operations.

META Group's research revealed a broad consensus regarding the need for privacy, and a general recognition of the fact, that the design of today's IT systems and networks is a serious challenge to privacy: The public IT infrastructure should be designed, or redesigned, to put the user in control of his own personal information and his private sphere. But given the extent of the infrastructure, and the considerable commercial and state interests in the collection of personal data, this will not happen overnight. In the meantime, a number of Privacy Enhancing Technologies can be used to improve the protection of privacy in selected areas and cases.

Currently, no widely accepted definition of Privacy Enhancing Technologies has been established, and our research indicates that today's view of privacy related tools is much wider than the definitions stated just a decade ago. The widespread use of electronic information, and the interconnection of IT systems in public networks has created a broad range of privacy threats, and corresponding opportunities for providers of privacy related tools and services. Some of these tools are actively involved in the information storage and transport, while others are supporting the administration of privacy. The following table proposes two main categories of Privacy Enhancing Technologies, and describes a number of subclasses:

Main Category	Subclasses	Typical Features
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.

4.1 PRIVACY PROTECTION

The Privacy Enhancing Technologies are divided into two main categories: Privacy Protection and Privacy Management. The first category, Privacy Protection, contains tools and technologies that are actively involved in protecting the privacy, e.g. by hiding the private information, or by eliminating the need for personal identification. This category is divided into the following subclasses:

Pseudonymizer Tools

The best way to protect private data in electronic services is to include the privacy requirement in the basic design of the service and in the architecture of the IT systems built to support it. A wide range of general design tools can be used to develop privacy-aware services and systems, but these tools are seldom marketed as privacy tools, and they are generally not considered privacy enhancing technologies. If the privacy principles were not included in the original design of data structures and services, it is possible to use add-on products or middleware, to separate sensitive private data from the transactions. Such tools or modules are often offered in connection with e-business software, as a “privacy feature”. The provided functionality is typically replacing the name of a customer with a neutral transaction identifier. Other application building tools offer the ability to remodel existing databases, using arbitrary keys to link different tables of information, instead of unique identifiers. Using unique person identification of customers is often a privacy issue, especially if any of the transaction data is shared outside the scope of the service.

Anonymizer Products and Services

Providing anonymous access is the original core functionality of the first privacy enhancing products and services. Primarily offered on the Internet, the services allow persons to send messages and interact with electronic services without revealing their true identity. The translation between the false and true identities is typically performed by a chain of cooperating trusted parties, and protected with encryption mechanisms, so the anonymity is maintained, even if the translation tables of one of the trusted parties is compromised.

Encryption Tools

Using encryption techniques to ensure secrecy of selected information is often a central part of privacy enhancing solutions. Using encryption technology, sensitive transaction data can pass through insecure networks and servers, or identities can be hidden from other parties. As mentioned above, multiple encryptions can be combined, so the data is protected even if one or more of the keys are exposed. Although encryption techniques were invented and used long before today’s privacy issues were recognized, encryption is generally considered a privacy enhancing technology by our respondents.

Filters and Blockers

This is a category of tools, focused on eliminating the negative effects of the loss of privacy. By deleting or blocking (filtering) unwanted messages, arriving as email, web-content or via other targeted electronic media, the filtering tools aim to protect the targeted individual against unsolicited messages (spam) of all kinds. Most people don’t consider these tools Privacy Enhancing Technologies, because they are handling the secondary effects only.

Track and evidence erasers

When communicating or using services offered through the Internet, the public telephony network or other electronic media, the user will leave traces of his activity in many places along the route of the data traffic. Some of these traces are required for administrative purposes (e.g. billing or traffic planning) while others are intended for the convenience of the user or the network provider. Both for the network and for the user equipment, a number of utilities are offered to erase history logs and traces. These utilities are generally not considered Privacy Enhancing technologies, but they can be part of a framework of products and services that support privacy.

4.2 PRIVACY MANAGEMENT

The second category, Privacy Management, contains tools and technologies that support the administration of privacy rules, rather than processing the information itself. This category is divided into the following two subclasses:

Informational tools

Raising awareness, creating policies and checking compliance are not active Privacy Enhancing Technologies, but they are often considered natural parts of a PET framework: Privacy protecting initiatives require structured policies and principles, both in the planning and implementation phase, and in the operational phase, where regular audits or reviews will document the compliance. A number of tools are offered to facilitate creation and management of privacy policies, and to verify that services, such as web sites comply with the set rules.

Administrative Tools

Both general and specific tools support Enterprise management of privacy. The general tools have a considerable functional overlap with other security functions, i.e. the management of privacy is an integral part of the enterprise security management. Specific tools for managing privacy issues are offered as add-on modules to general system management suites. These modules are considered Privacy Enhancing Technologies by some interviewees.

5 TECHNOLOGY FEATURES OVERVIEW

The purpose of most Privacy Enhancing Technologies is to obtain one or more of the three main privacy features:

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

In addition to these primary features, some tools are focused on eliminating various negative effects of losing privacy, such as unsolicited messages (spam), unwanted web content (popup windows) or even unauthorized programs (spyware, virus). We consider such tools secondary, and mark them with an S.

Another category of Privacy Tools is aimed at helping the user understand privacy issues and take privacy decisions on a well-informed basis. Such tools considered informational, they are marked with I in the table.

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					
		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

The following sections include a short introduction to the technology features of Privacy Enhancing Technologies:

5.1 CRM PERSONALIZATION

A number of tools are offered to preserve the anonymity of users of Internet based shopping and other services, some of these tools constitute an integrated part of Customer Relationship Management solutions. In it's simplest form, the CRM personalization tools enable Internet transactions between a shop and anonymous customers – more sophisticated solutions support profiling of individual customers without knowing or even storing their identity. CRM personalization is supporting the unlinkability aspect of privacy.

5.2 APPLICATION DATA MANAGEMENT

Many applications are built on a number of databases with a common, connecting key field, consisting of a unique person identifier (in Denmark: CPR-number). This design principle can make it very difficult to import and export data without compromising the privacy, because the identity of the person must follow the data to ensure consistency. In such cases, the common personal identifier can be replaced with several different key fields that link the tables without referencing the personal identity. Some tools are offered to replace the key field contents with random identifiers, and thereby enabling interoperability, and export of data, without revealing the personal identifiers. In this way, application data management is supporting the unlinkability aspect of privacy.

5.3 BROWSING PSEUDONYMS

When browsing the Internet, the user leaves traces in every place, where the traffic crosses communication equipment, servers and other active nodes. No single authority is in control of these traces, and the user cannot “switch off” the traces, because the Internet routing mechanisms are depending on the trace to deliver responses back to the user. However, some services are offering the user a false address (pseudonym), so the user can visit sites without revealing his own address. Browsing Pseudonyms is supporting the anonymity aspect of privacy.

5.4 VIRTUAL EMAIL ADDRESSES

Similar to when browsing the internet, the user leaves traffic traces in many active nodes, when an email is sent, and the possibility exist, that one or more of the nodes can keep a copy of the email, after it has been forwarded. In order to send anonymous email, not only the sending email address must be changed, also a number of technical transmission data must be fictitious. Some services are offering the use of a false email address (pseudonym) along with different degrees of anonymity, so the user can communicate via email without revealing his real identity. Virtual email addresses are supporting the anonymity aspect of privacy.

5.5 TRUSTED THIRD PARTIES

Using a Trusted Third Party (TTP) for delivering certificates and keys in a Public Key Infrastructure (PKI) services is already widely implemented. Registration Authorities (RAs), Certification Authorities (CAs), validation or time-stamping authorities, notarization, notification, anonymization and pseudonymisation are all examples of TTP services. Trusted third parties can be supporting both the unlinkability aspect and the anonymity aspect of privacy.

5.6 SURROGATE KEYS

Similar to the tools mentioned in section 5.2, a number of techniques exist to replace key fields in Data Warehouse input tables with calculated (surrogate) keys. The tools are typically used on data describing customer transactions, and the purpose is mainly to reduce the computing power required to align the incoming data with already existing databases. However, the same techniques can also prevent that data from different Data Warehouse tables can be recombined, and hence be considered a privacy enhancing technology. Used this way, a surrogate key is a technology supporting the unlinkability aspect of privacy.

5.7 ENCRYPTING EMAIL

As mentioned in section 5.4, the possibility exists, that the contents of an email can be observed by other parties, while the message is transported over the Internet, and one or more of the nodes can keep a copy of the email, after it has been forwarded. To protect the content against being exposed, the email body and/or its attachments can be encrypted, using built-in functionality in the email client or third party tools. Although this does not hide the existence of the message, encryption can prevent the exposure of sensitive email content. Encryption is a technology supporting the unobservability aspect of privacy.

5.8 ENCRYPTING TRANSACTIONS

When browsing the Internet, a “secure” protocol can be used, as an alternative to the traditional hypertext transfer protocol, HTTP. The most common secure protocol, SSL, includes encryption of the transaction content, and can also be used for authentication of the transaction parties. This technology is often used for transactions involving sensitive personal or financial information. Similar protocols are used in ATMs and Point of Sale terminals, to protect the information exchanged with the bank or clearing house. Encryption is a technology supporting the unobservability aspect of privacy.

5.9 ENCRYPTING DOCUMENTS

When storing or transmitting electronic documents with person-related information, an important issue is to assure the integrity and confidentiality of the document, or in other words: How to protect the document against unauthorized exposure, copying or alteration.

Document encryption is often used to protect privacy, especially when the document is stored or transmitted in an infrastructure that cannot guarantee the protection of the information. Encryption is a technology supporting the unobservability aspect of privacy.

5.10 FILTERING EMAIL SPAM

A large number of utilities and services are offered to protect users and organizations against unsolicited email messages (spam). These services are using several technologies, such as scanning the mail contents and address fields for known spam patterns, consulting central databases for identifying known spammers, or allowing only emails from pre-authorized users to cross the filter. However, since today’s common email protocols do not support reliable identification of the sender, such methods are not very effective. Filtering email spam is only addressing the secondary effects of loss of privacy.

5.11 FILTERING WEB CONTENT

Protecting users and organizations against unwanted web content is generally not a privacy issue, since the information is normally not targeted against individuals. However, some web applications are using knowledge about the user (e.g. domain name, IP address) to personalize the content, so the user can experience the need for filtering or blocking specific content. Web content, creating or using persistent information on the user's computer, is described in Section 5.14. Filtering web content is only addressing the secondary effects of loss of privacy.

5.12 BLOCKING POP-UP WINDOWS

A separate class of unwanted web content is known as Pop-up windows: Using different methods, the web site presents unprompted content (most often advertisements) on the user's browser screen. Blocking this inconvenient disturbance can be useful, but this feature is not related to privacy.

5.13 SPYWARE DETECTION AND REMOVAL

Spyware is a commonly used term for software that is hidden on the user's computer, and reports information about the user's information and his actions back to the originator of the spyware. This kind of software is most often using well known virus techniques for propagation and installation on the user's computer, and is capable of reporting any information about an individual, that can be retrieved from his computer or via its access to other computers, such as banking or commercial sites. Technologies for detection and removal of spyware can be supporting all main aspects of privacy: Unobservability, unlinkability and anonymity.

5.14 BROWSER CLEANING TOOLS

A normally configured Internet browser will store significant amounts of information about its use on the computer, where it is installed. The information includes (but is not limited to) addresses of visited sites and copies of the retrieved information. In addition to this, the browser can let the web sites store any information as small files (cookies) on the computer, where they can be collected at a later date, e.g. to relieve the user from the burden of a repeated login, to remember where the user left during the previous session or to recognize updates since last visit. The stored information will reflect the history of the user's actions, and may contain both sensitive and private information. Utilities offered for cleaning the browser for this history track and the stored cookies can be supporting all main aspects of privacy: Unobservability, unlinkability and anonymity.

5.15 ACTIVITY TRACES ERASOR

Also outside the Internet browser, most computers will store information about their use, typically as log files recorded by the operation system and the applications. The stored information will reflect the history of the user's actions, and may contain both sensitive and private information. Utilities offered for deleting this history track can be supporting all main aspects of privacy: Unobservability, unlinkability and anonymity.

5.16 HARD DISK DATA ERASOR

When replacing a hard disk of a computer or when leaving it in for repair, any sensitive data on the disk is at risk, even if the rest of the computer is inoperational. Even when deleted by the computer user, such data is clearly visible to a technician, using the appropriate tools. In these situations – and many other similar cases - it is wise to assure that the data on the disk no longer can be read. A special procedure – and special utilities - is required for the user to delete the data effectively. Utilities offered for erasing hard disks effectively can be considered a privacy enhancing feature, supporting all 3 main aspects: Unobservability, unlinkability and anonymity.

5.17 PRIVACY POLICY GENERATORS

Tools for creating privacy policies are not considered active Privacy Enhancing Technologies, but they are often presented as components of a PET framework: A number of tools are offered to facilitate creation and management of privacy policies and principles, such features are considered informational tools, not directly supporting the aspects of privacy.

5.18 PRIVACY POLICY READERS/VALIDATORS

Corresponding to the tools mentioned under 5.17 , some utilities exist for users to examine a web site's privacy policy, to determine if the web site /organization is complying with the user's privacy requirements. Such readers/validators are not considered active Privacy Enhancing Technologies, but they do assist the user in taking privacy decisions. The policy readers are considered informational tools, not directly supporting the aspects of privacy.

5.19 PRIVACY COMPLIANCE SCANNING

To verify that web sites comply with the declared privacy policy for the owner organization, the sites can be scanned and the service offered can be tested using automated tools that compare the information found to the rules set out in the policy. Such a scanning can be conducted using standalone tools, or by commissioning the task to a service provider. Compliance scanning is an informational feature, not directly supporting the aspects of privacy.

5.20 IDENTITY MANAGEMENT

Reliably identifying users of electronic services is a prerequisite for providing rich functionality – and supporting the relevant security aspects. The main purpose of Identity management systems is to simplify user administration, while still protecting the privacy of the individual by leaving him in control of his own profile. Hence, tools and utilities that support identity management often form part of a privacy-enhancing framework. Once defined, the user identity can be verified using various techniques, without recording the identity itself. In this way, Identity management can support the anonymity aspect of privacy.

5.21 BIOMETRICS

As mentioned in section 5.20, the user identity can be verified in many ways, one of which can be using biometric data. The identification can be performed without recording the biometric data itself, by comparing an encrypted version of the data against a reference register. Used this way, biometrics constitute a one-way mechanism to confirm a persons identity, without linking it to his private data. Hence, when used appropriately, biometrics can support the unlinkability aspect of privacy.

5.22 SMART CARDS

Smart cards can be used for identification in a similar way to biometrics, by including encryption, either in the card or in the reader. However, it must be remembered, that the procedure can only identify the card, not the bearer. Since the card need not to hold information to identify the bearer, smart cards can support the anonymity aspect of privacy.

5.23 PERMISSION MANAGEMENT

This feature is closely connected to identity management, because a reliable identification of the user is often required to associate him with the correct credentials. However, granting a permission is often depending on the situation, combined with the role of the user, rather than his identity. In such cases, managing permissions can be performed without storing the profiles together with the identities, and permission management can support the anonymity aspect of privacy.

5.24 MONITORING AND AUDIT TOOLS

Administrative tools to monitor and audit security are well known elements of today's computing environment. The tools for monitoring privacy have a considerable functional overlap with other security functions, i.e. the management of privacy is an integral part of the enterprise security management. The privacy monitoring and audit tools can be used to support the unobservability aspect of privacy.

5.25 FORENSICS TOOLS

Tools to investigate security (or privacy) breaches are often ad hoc methods to retrieve information not normally recorded. The forensics tools are not considered operational in the management of privacy.

6 USE CASES

Every day, we encounter situations where privacy concerns have been important design criteria for the information handling procedures, independently of whether we are using electronic media or handling the information manually. A classical example is the procedure of voting: First, the voting person must be identified and checked against the electoral register, then, the vote is cast anonymously in the polling booth. If the correct voting procedure is followed, no vote can be linked to a person, while each registered voter can cast his vote only once. Similarly, a number of business and administrative procedures are designed to preserve privacy; some of these procedures are supported with privacy enhancing technologies. The following examples illustrate some typical privacy related use cases:

6.1 ANONYMOUS BUSINESS RELATIONS

A number of traditional businesses are built on the principle of being the “middle man” between two parties. Examples of such are real estate agents and recruiting agents: The agent’s business is to bring two parties together, and receiving fees from (at least) one of the parties. Hence, it is in the interest of the agent to control the parties’ information about each other, until a match is found. Traditionally, this control was achieved by the agent’s separate communication with the parties, and the parties’ trust in the agent. In the new age, where part (or all) of such a business process is carried out by IT systems, these systems must be able to support the same functionality of separating the information about the parties from their identity, and the parties must have the same trust in the technology, as they had before in the agent. The anonymous business relations are typically supported by the built-in functionality of the agent’s systems, which makes it relevant for the users of the service to check the agent’s privacy policy and to seek confirmation of the compliance of the agent’s site (see sections 5.17, 5.18 and 5.19). If the user doesn’t trust the agent or the site he is using, it could be relevant to apply user controlled tools to ensure anonymity, as described in sections 5.3, 5.4 and 5.5.

6.2 COMMERCE CHAIN MANAGEMENT

In cases, where traditional business chains exist, connecting producer, wholesaler, retailer and consumer, it has an increasing business value to be closer to the consumer, and collect information about his interest in the products and services offered. This is seen e.g. in the travel industry, where travel agencies for purposes of logistics need to share some data about the end user with hotel chains and airline carriers, but certainly want to retain valuable information about the customer’s preferences and travel patterns. Such requirements are reflected in the design of the IT systems used by the business: They are using privacy-related technologies, but the drivers are mostly commercial. The purpose is to establish and protect the business model of the professional players, and to offer the client a personalized service. In most cases, the consumer has to provide relevant data to the agency/shop, if he or she appreciates a personal service, but the user might want to limit the use of the information to the specific instance of service, agreed with the provider. In this case, the use of privacy enhancing technologies could be appropriate, e.g. to communicate and check the privacy policy of the shop/agent (see section 5.17-5.19), or to identify the user by other means than his private information (see section 5.1, 5.20 and 5.22)

6.3 PRIVACY REQUIREMENTS IN PUBLIC SERVICE

In the recent years, the increasing use of interconnected IT systems to serve the needs of the consumer has led to growing concern about the spreading of sensitive private data, such as health data, information of political and religious attitude. Both EU directives and national legislation support the requirement of privacy, and a growing number of private and public institutions are implementing compliant policies, functionality and procedures. One example of such an implementation is the public library lending records, which according to Danish law must be deleted after 4 weeks upon book return, to prevent possible "profiling" of the users' reading. Another example is digital rights management: The IT system must document the use of software and other copyright protected material (so the copyright holder can be paid) without disclosing the identity of the user. The privacy protection in such cases is often implemented in new IT systems, or as add-on products to existing systems. However, the responsibility of privacy protection remains with the service provider, and the user must trust that the service is compliant with the legislation.

6.4 RADIO FREQUENCY IDENTIFICATION DEVICES (RFID)

In some situations, when the identity of a product can be linked to a person, the product id can be a threat to privacy, because the product can be traced. An example of this is the use of Radio Frequency Identification Devices (RFID), a technology that allows remote identification of a small computer chip that can be embedded in or attached to products of any kind. The typical usage scenario is attaching the RFID to goods sold in a supermarket, so the goods can be identified and accounted for at the exit gate. In such a case it is simple to protect the privacy of the buyer by disabling (destroying) the RFID before the exit from the store. But the producers of many goods have an interest in following their goods further, e.g. in the warranty period. To accommodate this need without compromising privacy, the RFID must be disabled at the store exit, but re-enabled by the user, if the need for warranty service occurs.

However, the scope of RFID is not limited to products. It is often used to identify pet animals, and in some recent cases, RFID chips have even been inserted under the skin of humans, volunteering to use this kind of identification. Examples of this application are the members of a beach club (for convenient access control) and some high-risk patients in hospitals (for reliable identification in emergency situations). However, in such cases, the RFID is merely used as an alternative identity token, not a privacy enhancing technology.

6.5 FINANCIAL TRANSACTIONS

In many countries, protecting the privacy of the customer is an essential part of personal banking and other financial services, and the citizen's freedom to conduct private deals and transactions with other parties is highly appreciated. However, the development of eGovernment services, combined with the fight against organized crime, has increased the general acceptance of public surveillance of the individual's financial transactions. As an example, the Danish legal requirements for employers, authorities and financial institutions to submit details of the citizen's personal economy directly to the tax authorities makes it almost impossible for a private person to conduct any substantial financial transaction without leaving tracks of information. The public has generally accepted this situation, assumedly based on a high level of trust to the authorities. However, it is possible for individuals to use

several different banks and/or financial services in parallel, without informing any of them of the other engagements.

6.6 ANONYMOUS SHOPPING

In many shopping situations, the consumer prefers not to be identified and related to the purchase. Obviously, this includes illegal drugs, stolen goods etc, but also a wide range of legal goods and services are sold to unidentified buyers: Examples are prescription drugs, books on sensitive subjects, private services, personal loans. Such transactions can be carried out person to person, using physical money or electronic cash (coin card) as payment. SSL encryption of Internet transactions (see section 5.8) is often used when transmitting credit card information, mainly to guard the parties against fraud. However, the encryption will also protect the information in-route from being read by third parties.

Alternatively, the goods can be purchased over the Internet, using privacy solutions from trusted third parties (see section 5.5) to anonymize the payment, and deliver the physical goods to a pick-up address, so the shop can do business with customers without knowing their identity. If the customer can trust the shop, anonymity can be achieved by using anonymous shopping systems (see section 5.1), and in this case, the customer wants to check the privacy policy of the shop (see section 5.17-5.19),

6.7 POSITIONAL INFORMATION

In some situations, the geographical position of an individual – or the history of positions - is considered private information. Because an increasing number of common user situations involve information technology, there are various ways of tracing the individual's position. Examples are reservations and tickets for airlines and other transport, which are linked to a credit card or other id token. Mobile phones leave clear traces of their position, and wireless LAN connected computers and PDA's can be traced by the access points they are using. In some of these cases, the privacy can be enhanced by using e.g. SIM cards in the phone that is not linked to the user's identity – or computer addresses, that can be altered by the user. However, the link can often be found by analyzing the traffic patterns (e.g. numbers called, emails sent, sites visited), even without analyzing the content, which could be encrypted: A number of encryption solutions are already in widespread use, in order to protect private data from being exposed to unauthorized parties, that have access to the medium (radio waves or public networks). Typical examples are the GSM mobile phones encryption of the transmitted payload data (including voice), and WEP encryption of wireless networks.

6.8 HEALTH CARE SERVICES

Information related to a person's health is generally classified as private, and should only be shared between a patient and the relevant health care staff. However, a safe treatment of a patient is relying on access to a full set of records, describing his medical history, condition, etc., and the ability to link this information reliably to the individual. Therefore, today's procedures and systems handling clinical health information has primarily been designed to protect the patient's health, rather than his privacy. And not surprising, most patients waive their right to privacy, when their health is at stake. Furthermore, the sharing of medical data with public and private medical insurance institutions, research organizations and pharmaceutical companies represents a wide range of challenges to privacy. The health care

service is probably the most important area for employment of privacy enhancing technologies, both as an integrated part of the enterprise architecture, and as stand-alone solutions for specific needs. Examples of such applications could be remodelling public databases (using data management tools described in section 5.2), establishing a common privacy policy for the health sector (and implementing it with tools described in section 5.17 – 5.19), or introducing alternative methods of identification of the patient (see section 5.20-5.22).

7 MAJOR PET PLAYERS

This chapter gives a reference to selected providers of privacy enhancing products and services, structured according to the principles set out in chapter 4. The list is not intended to be complete, but it includes examples of typical products and services.

There has been a high interest in privacy technologies in the early years of this century, which decreased somewhat in 2003 and early 2004. The list below includes some players that are obviously not in business anymore (marked with an asterisk *), but since they were very representative of their respective market segment, they are still listed. Since the interest in privacy is slightly picking up in late 2004 and 2005, chances are that new players will emerge, replacing those who vanished.

7.1 PRIVACY PROTECTION

7.2 APPLICATION TOOLS

E.piphany	http://www.epiphany.com/	CRM Personalization
Unica	http://www.unica.com	CRM Personalization
Outerbay	http://www.outerbay.com/	Application Data Management

7.3 ANONYMIZER PRODUCTS AND SERVICES

Synomos Enterprise (ex Zero Knowledge)	http://www.synomos.com/	Monitors privacy compliance /governance
Custodix	http://www.custodix.com/	Basic research ,TTP services.
Privacy, Inc.	http://www.privacyinc.com/	Virtual email addresses
Sapior Ltd.	http://www.sapior.com/	Pseudonym services, surrogate keys
IPrivate *	http://www.iprivate.com/	Browsing and email pseudonyms

7.4 ENCRYPTION TOOLS

PGP Encryption	http://www.pgp.com/	Encryption tools
----------------	---	------------------

7.5 FILTERS AND BLOCKERS

Acronis Privacy Expert	http://www.acronis.com/	Spyware removal Activity traces clean-up Pop-up blocker
SynergeticSoft	http://www.synergeticsoft.com/	Spam blocking tools

Privacy Manager	http://www.anonymizer.com/	Spam blocking tools
Computer Associates / Pest Patrol	http://www.ca.com/products/pestpatrol/	Anti-Spyware solution

7.6 TRACK AND EVIDENCE ERASORS

Ibas ExpertEraser	http://www.ibas.no/datasletting	Harddisk data eraser
PrivacyEraser	http://www.privacyeraser.com/	Browser cleaning tools

7.7 PRIVACY MANAGEMENT

7.8 INFORMATIONAL TOOLS

AT&T Privacy Bird	http://privacybird.com/	Reads P3P Policies
OECD Privacy Policy Generator	http://www.oecd.org/	Policy Generator Tool
W3C Policy Validator	http://www.w3.org/P3P/implementations http://www.w3.org/P3P/validator.html	Online validator service
Watchfire	http://www.watchfire.com/	Scans privacy compliance of web sites
Privacy Council	http://www.privacycouncil.com/	Scans privacy compliance of web sites
Coast	http://www.coast.com/	Monitors privacy compliance of web sites
Idcide *	http://www.idcide.com/	Monitors privacy compliance of web sites

7.9 ADMINISTRATIVE TOOLS

PrivacyRight	http://www.privacyright.com/	Permission management and audit software
IBM Tivoli Privacy Manager	http://www-306.ibm.com/software/tivoli/products/privacy-mgr-e-bus/	Privacy management
Access Data	http://www.accessdata.com/	Forensics/Password recovery

8 RELEVANT GROUPS INFLUENCING PUBLIC PRIVACY PERCEPTION

In Denmark, like most other European countries, the public awareness of privacy issues is still very low, mostly due to the fact that common knowledge of the issues is at a very low level. However, a number of organizations are working to inform the public about privacy matters and influence the public opinion towards demanding e-services that respect the privacy of the citizen. The participants of our research have identified the groups and organizations listed in this section:

- European Commission, namely Directorate General “Internal Market” (EU DG IM)
- Article 29 Working Party at EU DG IM
- Organization for Economic Co-operation and Development (OECD)
- National (and e.g. in Germany and Switzerland also Regional) Data Protection Agencies
- EGovernment authorities (in Denmark: Digital Task Force, Ministry of Science)
- Human rights organizations (e.g. the Danish Human Rights Institute)
- Privacy user groups
- Internet based forums on privacy
- Private institutions, researching and developing concepts
- Research community (universities, public institutions, e.g. *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein*)
- Trade associations, representing industry sectors
- Commercial institutions, e.g. banking, insurance, Telco’s
- Private companies, selling PETs and consulting services
- Security working groups, e.g. IFIP Tech Committee 11
- User groups on sensitive data, e.g. health data

9 WHAT ARE THE PROBLEMS

9.1 PRIVACY IN LEGACY APPLICATIONS WILL REQUIRE ADDITIONAL CHANGES

Most of today's Privacy Enhancing Technologies are conceptually designed to repair flaws in original design of IT systems and information handling procedures. The PETs are conceptually add-on products to improve the privacy aspect of information systems that were built without this requirement. Hence, using PETs in a legacy environment will in most cases be a work-around solution, rather than an integrated component. As an example, adding PET to a legacy system (e.g. by replacing CPR-numbers with neutral identifiers) can have several negative side effects:

- a) It can reduce the overall efficiency of the system, when e.g. database searches have to be performed with multiple criteria, rather than using one unique key (the personal ID).
- b) It can lead to less reliable data, when the unique keys are no longer visible, because flaws in the data consistency are less likely to be discovered – by the user or by maintenance tools.
- c) It can increase the vulnerability of the system against fraud and abuse, because the possibilities of cross-checking one database against others has been limited.

This implies that adding PETs to existing legacy applications will often require additional changes of the system, to maintain the efficiency, reliability and robustness of the service. Such changes are generally not covered by the services of PET suppliers, and they will often require detailed knowledge of the application.

9.2 USER CONTROLLED PRIVACY CAN IMPACT USER RIGHTS

The “classical” PET tools and services (anonymizers, pseudonymizers etc.) are designed to assist the user in protecting his true identity from exposure. When using such tools in the interaction with services that assume that a true identity is presented, the user may be violating the business assumptions of the service provider. In other words, if the service has not been designed for anonymous users, the service provider could be unwilling or unable to fulfil his subsequent obligations towards the user, e.g. in case of warranty claims.

9.3 EXPLOITING DESIGN FLAWS

Some PET implementations are exploiting holes in the design of existing applications to add a level of privacy, for instance by inserting fictive data into fields designed to hold unique identification, where the appropriate check of the content has been omitted in the receiving system. In other cases, the PET tools are tampering with e.g. email message headers, exploiting design flaws in the protocol. Such methods are similar to the techniques used by hackers, spammers and virus programmers; they are ethically unacceptable, and they can seriously reduce the reliability and compatibility of the IT solutions.

9.4 LACK OF STANDARDIZED PRIVACY SOLUTIONS

Standardization of privacy features and solutions is yet to come – the current PET solutions are rarely interoperable (with the notable exception of P3P and EPAL, see below), because a common understanding of the concepts and requirements has not been established. Hence, most of today's Privacy Enhancing Technologies must be considered immature.

9.5 REDESIGN OF EXISTING SYSTEMS WILL TAKE TIME

Legacy systems are built on the assumption that secure identification of the user is required to provide almost any service. The principles behind the design (architecture principles) have typically not taken privacy requirements into account, but were focused on achieving simplicity and efficiency. To make existing systems "privacy-aware" or even "privacy-compliant", the design principles must be revised, and central parts of the design must be reworked. The effort required to conduct such a process is considerable, and the timeframe is very large.

9.6 CRITICAL SYSTEMS REQUIRE BACK DOOR FUNCTIONALITY

Many privacy solutions aim at putting the user in control of her/his own data. However, if the user is temporarily or permanently unwilling or incapable of taking the appropriate decisions, both sensible defaults and emergency "back-doors" must be available. This raises the question: Who should guard the back doors – and who should have the authority to take decisions on behalf of the user in emergency situations?

9.7 POOR UNDERSTANDING OF PRIVACY ISSUES

The most significant problem for the adoption of Privacy Enhancing Technologies is the poor understanding of privacy issues in the general public. Without this understanding, there is no demand for PETs, and no real drivers for the evolution of privacy solutions. Many users have no perception of the value of privacy, because they have not experienced the consequences of losing it. As an example, many persons willingly give up secret passwords for a small bonus or gift.

In Denmark – and many other European countries – the citizens have a high trust in the authorities, and see little need for controlling the government's access to their private data. However, there is a growing awareness of guarding private information when dealing with private companies, and still more citizens will expect to be informed of how their private information can be used by a company, delivering services and products.

9.8 PRIVACY REQUIRES USER TRUST

Before the user can use PETs, he must establish trust in the technology, and/or the service. This means that the users must also trust the party that offers the technology. Such a trust is hard to establish, for a user that does not know the technology, and who does not have a clear understanding of the privacy risks. The lack of conceptual knowledge can seriously hamper the adoption of any new technology, as we have seen before, e.g. with the introduction of the Danish Citizen's Card (*Borgerkort*).

9.9 CLASSIFICATION OF PRIVATE DATA REQUIRES NEW CONCEPTS

It is important to recognize, that “data in context” can be sensitive, even if the same data out of context is not. This means that the privacy value (or threat) of a given data instance cannot be defined by classification of the data alone – it must be related to the situation.

9.10 LEGISLATION NEEDS CLEAR REQUIREMENTS

Establishing legal requirements for PET in specific situations is difficult without a systematic approach – additional research in this field is required, before the privacy requirements can be defined precisely and consistently, so that they that can form basis for legislation. Further complicating is the fact that private data easily crosses borders, whereas legislation, even within Europe, is still struggling with an easy way of handling cross-border privacy concerns.

9.11 PRIVACY IS NOT ALWAYS THE FIRST PRIORITY

In a number of situations, the average user will accept loss of control over his private data – or even loss of privacy. Examples of this could be a patient opening his medical records to a doctor, when he is about to receive life saving treatment on a hospital. Or accepting video surveillance, personal search or other violations of privacy in order to minimize the risk of terror attacks. Hence, the requirements for privacy must always be balanced against other vital needs.

10 VALUABLE INITIATIVES

10.1 PLATFORM FOR PRIVACY PREFERENCES (P3P) PROJECT

<http://www.w3.org/P3P/>

P3P is a specification developed by the World Wide Web Consortium (W3C). That specification, when implemented in Web sites and browsers, brings a measure of ease and regularity to Web users wishing to decide when and under what circumstances to disclose personal information.

On a P3P enabled Web site, a company's privacy policy is translated into a machine-readable format (Extensible Markup Language, XML). On the user side, a P3P client can automatically fetch and read P3P privacy policies on Web sites. A user's browser equipped for P3P can check a Web site's privacy policy and inform the user of that site's information practices. The browser could then automatically compare the statement to the privacy preferences of the user, self-regulatory guidelines, or a variety of legal standards from around the world. P3P client software can be built into a Web browser, plug-ins, or other software.

Such an implementation does not offer privacy protection, but it can greatly advance transparency and be used to support efforts to improve privacy protection. However, for P3P to be widely adopted, consumer interest will have to increase, so service providers can see an incentive to invest the effort.

10.2 PRIVACY ENHANCING TECHNOLOGY TESTING & EVALUATION PROJECT (PETTEP)

<http://www.ipc.on.ca/>

Formed by the Ontario Office of the Information & Privacy Commissioner, the Privacy Enhancing Technology Testing & Evaluation Project (PETTEP) is a global team of privacy and data protection experts from government and private sector organizations, committed to developing internationally accepted testing and evaluation criteria for the privacy protecting functions of information systems.

The group is collecting and structuring Fair Information Practices (FIPs) and mapping them to the Common Criteria (CC) framework. The effort is focused on creating a framework for formal evaluation, but could also be high-level principles for the design of privacy solutions.

The group is proposing that ISO establishes a Standards Committee for Privacy, and is aiming to develop a common definition for Privacy and a common set of FIPs as input into multipart ISO standard.

The reports from the group are publicly available, and the national privacy work in the countries is worth noting – illustrating both the advantage of a consistent framework and the difficulties with aligning it with local legislation.

10.3 ENTERPRISE PRIVACY AUTHORIZATION LANGUAGE (EPAL)

<http://www.zurich.ibm.com/csc/>

Developed by the IBM Privacy Research Institute, EPAL is a formal language for defining enterprise privacy practices. Enterprises promise a certain level of privacy to its customers using privacy statements or the Platform for Privacy Preferences (P3P). The EPAL language can then be used to formalize these promises. By automated enforcement of these enterprise-specific privacy practices, enterprises are enabled to comply with the promises made.

A privacy policy describes the privacy practices as well as the opt-in and opt-out choices of an individual. Policies are then associated with all data collected by an enterprise. This "sticky policy paradigm" mandates that policy sticks to the data, travels with it, and can be used to decide how the data can be used. By separating application- and enterprise-dependent deployment information from the actual policies, E-P3P policies can be used to control the flow and usage of data inside and among enterprises.

10.4 PRIVACY AND IDENTITY MANAGEMENT FOR EUROPE (PRIME) PROJECT

<http://www.prime-project.eu.org/>

During the research phase of this study, the PRIME project was launched. PRIME is a European RTD Integrated Project under the FP6/IST Programme, addressing research issues of digital identity management and privacy in the information society. The project will last for four years, and is planning to develop concepts and products in the field of identity management. Although the scope of PRIME is only a subset of all privacy enhancing technologies, we expect that the project will be addressing some of the issues described in chapter 12 of this report.

11 FUTURE PERSPECTIVES

11.1 WHAT DRIVES MARKET DEMAND FOR PETS?

Our interviewees see different drivers for the development and adoption of Privacy Enhancing Technologies:

Users of PET:

- Public awareness of privacy is perhaps the most important driver for PETs.
- Many commercial organizations see an important competitive value in PETs: It gives credibility and trust, when you can offer good privacy solutions to your clients.
- The general user's irritation over spam and other intrusions of the private sphere will increasingly motivate him to use privacy enhancing tools and techniques.
- Companies using Customer Relations Management (CRM) systems experience that data quality is much better for companies with privacy policy than for those who just collect any customer data.
- Phishing attacks and privacy theft is a driving force for the general demand for PETs; mostly because the ultimate driver is always the danger of losing money...
- Some users think that certification could help select the right PET, others suggest some public regulation to define when and where the use of PET is appropriate, or even required.

Producers of PET:

- Most suppliers of privacy solutions and services recognize that the lack of public understanding of the privacy issues and values is an important barrier for their success.
- Suppliers are waiting for regulation by public authorities, so regulatory compliance will become an important driver for the adoption of PETs.
- Privacy Impact Assessments are gaining popularity – in some cases it is even demanded by governments as part of generic risk assessments – this could also lead to a larger demand for PETs.

Authorities:

- Privacy Seals of approval (e.g. TRUSTe, BBBonline) is recognized as a major driver, because it makes the user decision easier, and in some cases it can be influencing public purchase decisions.
- E government initiatives could be a driving force for privacy solutions, if the authorities choose to include privacy functions as an option or a requirement.

11.2 HOW WILL PETS BE EVOLVING OVER THE NEXT FEW YEARS?

The following statements represent a summary of our research responses:

Awareness of the privacy issues is clearly rising. But only a factual rise in abuse of identities will motivate citizens to accept increased public control, or more personal involvement in guarding their private data. Market acceptance will be polarized, driven by different consumer attitudes: The majority doesn't care about privacy in their daily life, while a small minority will be worried, and demand/use PET.

The recent increase in terror threats has changed the general opinion of privacy: Most people will now accept increased control, sacrificing their privacy for the purpose of personal security. As an example, video surveillance is becoming common in Denmark, although a special permission is required to set up a camera in any public place. Very few permissions are given, but the responsible Danish authority (*Datatilsynet*) receives only few complaints from the public.

The citizens generally have high trust in the public authorities and are not expecting abuse from this side. Today's public administrative systems are not including much privacy protecting functionality, but the law requires the administrative staff to follow procedures that protect the citizen's privacy. Unfortunately, most E-Government initiatives follow this trend, by not including privacy principles in their basic design criteria. Privacy-aware design (of data, applications and procedures) is key to obtaining privacy, but very few examples of such solutions have been seen.

Many industries already use PETs, especially when more parties have to share some data, while other data must be kept separate. An example of this is when pharmaceutical companies are conducting clinical testing or joint research projects. The PETs used in such cases will often be embedded in custom-built solutions, rather than being added to a standard system. It is expected that tomorrow's privacy solutions will be an integrated part of public and private administrative solutions, based on an architecture, where privacy has been an integral part of the design criteria.

11.3 WHICH CATEGORIES OF PETS WILL HAVE THE GREATEST IMPACT?

Our research indicates, that a natural first step towards better protection of privacy would be to support and encourage the use of the *informational privacy tools* to create and implement privacy policies on public and private web sites. This could create the required broad awareness of privacy issues, and lead the way for more operational privacy solutions.

Secondly, introducing common principles for identity management – with integrated privacy features – could support the introduction of *privacy management tools* in selected areas, where the user perceives a benefit from simplified data access and control procedures.

Privacy frameworks, offering a suite of *user oriented privacy tools*, are likely to gain some acceptance in communities with a high level of privacy awareness, but it must be expected that such PET tools will be included in standard software packages over time, if the users find them relevant and useful.

It is expected, that companies delivering Internet shopping and other electronic services will respond to the customer's need for privacy, by offering appropriate functionality, such as

customer anonymity, when the customer prefers it. However, *third party anonymizer services* are not expected to gain significant popularity, since only few users will be willing to pay a third party for a service, that is already available in the shop.

11.4 WHO WILL PROVIDE THE PET SOLUTIONS?

It is often argued, that privacy tools must be delivered from an independent third party, in order to establish user trust in the privacy enhancing product or service. However, as the technology matures and the users' understanding of the issues improves, PETs will become mainstream commodities, similar to other security related technologies. An example of this is : Just a decade ago, setting up a firewall was a complicated expert task, and the cost was considerable. Today, firewall technology is embedded in many standard network components, e.g. modems and routers, and firewall functionality is an integrated part of the operating system (e.g. Windows XP).

In the future, privacy features are likely to be integrated in the IT infrastructure, as a part of the application platforms (in the operation system, database management system and development framework). This means that today's independent PET providers are likely to remain niche players – or to be acquired by major infrastructure suppliers, wanting to integrate the technology in their products and services.

11.5 WHERE CAN INTERNATIONAL COORDINATION HELP?

In Europe, the EU privacy directive has been widely implemented in national legislation, regulating e.g. exchange of private data between public administrations. The directive builds on many earlier sources, such as the OECD privacy principles, but it does not provide a comprehensive conceptual framework. On a national basis, many provisions must be coordinated, in order to be conceptually compatible, and support a common goal of privacy. The most important challenge is that no common concepts have yet been established for describing privacy issues and solutions, such as a common classification of private information, or common descriptions of usage scenarios, representing classes of privacy threats.

Because a large number of electronic services are offered and used in the global information society, it will require close cooperation between all countries to implement a common policy for protecting the privacy of the citizens. In related areas, such as the fight against spam, or the prevention of dialler abuse, it has proven difficult to involve all governments and private players in the implementation of common controls. Similarly, it is likely to be difficult to create a broad consensus about a specific common privacy policy.

International cooperation in the privacy field is expected to be most useful in areas of research and development of common terminologies and concepts for classification of private data, issues and usage scenarios. The international sharing of experiences from concrete initiatives can also be of significant value, but it must be recognized that the privacy awareness and end user attitude to possible solutions can vary significantly between countries, depending on e.g. cultural factors and IT maturity.

12 PRIVACY TRENDS AND ISSUES

As described earlier in this report, a number of privacy issues are still candidates for additional research and many privacy solutions are still at the stage of conceptual development. This chapter presents a number of significant trends and issues, illustrating possible ways of gaining a better understanding of today's privacy issues and applying relevant technologies and methods to protect the privacy for users of electronic services.

12.1 TREND: DEMONSTRATION PROJECTS

To improve the general knowledge and awareness of privacy issues and solutions, organizations are launching demonstration projects, where well known transactions or interactions are performed without the usual identification of the user, by using alternative means and technologies to establish the necessary link in the transaction. The technology used could be biometrics, smart cards or other ID tokens. Privacy demonstration projects are relevant in many sectors, such as health services, shopping, social benefits, investments, travel cards, etc. A valuable demonstration starts by analyzing and possibly redesigning the business model and the information flow of the transaction. Unfortunately, the results of the demonstrations (with respect to user acceptance, cost, effort, benefits and possible side effects) are not always published, but rather used as an internal tool to improve the traditional business processes.

12.2 TREND: ACCEPTANCE SURVEYS

Another common initiative is to conduct surveys of the public perception of privacy issues and the value of privacy. However, it is our view, that surveys including respondents that have experienced the issues and tried the solutions, will be much more qualified than opinion polls that include a random audience. The most valuable acceptance surveys are conducted in combination with selected demonstration projects, where the participants have first hand experience with using PET solutions, e.g. an acceptance survey connected with implementing P3P technology for selected sites or services.

12.3 TREND: PRIVACY CONSIDERATIONS IN E-GOVERNMENT SERVICES

A large number of e-Government services are currently being deployed, in order to introduce self-service and reduce the administrative cost. However, the services are often built as an electronic copy of the manual administration process. It would be of considerable value to introduce privacy protection as part of the solution design, when the service is built or revised. A privacy-aware design means that the user has access to a good and well-structured privacy policy, certainty that the service complies with the policy, an easy choice of privacy options – with sensible defaults – and a helpful guide explaining the choices. The privacy protecting components of the design could very well be developed as common patterns, to be included in several different eGovernment applications. Key sectors for the introduction of privacy enhancing technologies are the health sector (communication between doctors, hospitals, insurance, authorities), and other public authorities handling sensitive private information (tax, employment, social services, etc).

12.4 TREND: REVIEW OF PUBLIC E-SERVICES INCLUDES PRIVACY

For several years, an annual review of selected public Internet sites/services has been conducted by The Danish Ministry of Science, Technology and Innovation (*Bedst på nettet*). In its current form, the review criteria include a simple check of the existence of a privacy policy on the site. Following the increasing awareness of privacy issues, the review is likely to be developed further, e.g. by evaluating the contents of the policy, checking the compliance of the service, and possibly evaluating the required private information against the richness and usefulness of the service.

12.5 TREND: CORPORATE PRIVACY SOLUTIONS ARE ADVANCING

Large public and private organisations are increasingly assuming responsibility for guarding the privacy of their customers and employees. Managing the identity and permissions of internal and external users is becoming an important part of corporate applications and services, and implementing a reasonable privacy policy is increasingly important for the image of the service provider. This indicates that user controlled privacy technologies, offered by third parties (e.g. as infrastructure services or user tools) are less likely to gain a high popularity, because some PET functionality is already included in many of the standard services. However, for some legacy services (without PET functionality) and for some users (with little trust in the service provider) the user controlled PETs will still be a viable option.

12.6 ISSUE: LACK OF A TRUST MODEL

One of the most important barriers for the implementation and adoption of privacy enhancing solutions is the lack of a clear classification of the privacy vulnerabilities and threats. Unlike the loss of material assets, the value of a privacy impact is depending on the situation, so a classification of the information sensitivity is not enough. A "Privacy Trust Model" would be a valuable step towards standardizing the area of privacy: The establishment of a common understanding of privacy threats through research would be a valuable input to the design of both demonstration projects and the planning of full scale privacy enhancing solutions.

12.7 ISSUE: SPECIFIC PROVISIONS ARE LIMITING DESIGN CHANGES

A number of privacy problems with legacy systems (especially in the public sector) can be traced back to the fact, that the original design has been developed to comply with specific regulatory provisions, which are not including a requirement for privacy protection. The owners of the legacy systems will most likely be reluctant to change the design, unless a clear signal is given from the legislators. This could suggest a revision of the specific provisions, in order to balance the administrative efficiency requirements with the need for privacy protection.

12.8 ISSUE: NEW TECHNOLOGIES ARE CHALLENGING OLD LEGISLATION

New and emerging technologies e.g. advanced SIMs, Smartcards and RFIDs open new possibilities of tracking the individual and his actions, but the perspective of consequences is often unclear (due to the lack of a privacy classification). The current legislation of privacy (in Denmark mainly expressed in *Persondataloven*) may need to be supplemented with some regulation of the rights and duties of the different parties involved in protecting privacy,

when new technologies are applied. However, new regulation in this area will probably benefit from some additional research in the field of privacy – and from following the results from other countries and international working groups, e.g. the PETTEP project (see chapter 10).

12.9 ISSUE: LACK OF STANDARDS

Today's PET solutions are rarely interoperable (with the notable exception of P3P and EPAL, see chapter 10), because a common understanding of the concepts and requirements has not been established. However, as a predecessor to firm standards, it could be valuable to develop and propose a Best Practice for the privacy protection of private and public electronic services. Building on the existing legal foundation of *Persondataloven* and the supplementing rules and guidelines from The Danish Data Protection Agency (*Datatilsynet*), a privacy practice recommendation could provide guidance and examples of e.g. appropriate privacy policies, implementation principles and compliance evaluations that would help builders of e-services create solutions that fulfil both the user expectations and the legal requirements for privacy.

12.10 ISSUE: PRIVACY REQUIRES AN ARCHITECTURE

Most of the privacy enhancing technologies of today are offered as add-on products that can reduce or eliminate the effect of privacy flaws in the applications, in the infrastructure, or even in the business processes. The use of privacy enhancing technologies must be carefully planned, in order to achieve the set goals. Architecting privacy starts with establishing the privacy principles that must be met by the end-to-end solution, and implementing these principles in the design of applications and/or the IT infrastructure. For this reason, it could be valuable to establish a set of architecture principles for privacy, and to include the privacy requirements in the enterprise architecture work currently in progress under the Danish IT architecture and software strategy.

APPENDIX A: METHODOLOGY

The thought leader interviews have been conducted using the following questionnaire.

PRIVACY ENHANCING TECHNOLOGIES IN EUROPE - QUESTIONNAIRE

This questionnaire serves as a guideline for about a dozen 'thought leader interviews'. META Group uses this method to gain a thorough understanding of a market with a restricted number of interviews. Selected privacy practitioners from government, enterprise and consumer organizations are asked to give their opinion on Privacy Enhancing Technologies, representing their respective organizations.

This META Group study has been commissioned by the Danish Ministry of Science, Technology and Innovation. The interviews target thought leaders in Denmark, the UK, Germany and at EU level. The interviews are conducted throughout June and July 2004, the report will be published in August 2004. The names of all quoted respondents or of their organization will be made available to the Ministry. This questionnaire is sent to interviewees by email, to allow time for preparation. The interview is conducted over the phone by a META Group representative and should not last more than an hour.

QUESTIONS

- 1. Please describe your organizations approach to privacy.**
- 2. What are privacy enhancing technologies (PETs)? Please give some examples of vendors or products.**
- 3. Are there different classes of PETs?**
- 4. What are major features of PETs (in the different classes)?**
- 5. Who uses PETs? Please describe some scenarios.**
- 6. How do you see PETs evolving over the next few years?**
- 7. What drives market demand for PETs?**
- 8. Which technologies would you not consider as PETs? Spam filtering? Identity management? Content filtering?**
- 9. With whom do you work together outside of your organization, your country?**
- 10. Please comment on the following initiatives: P3P, PETTEP, EPAL.**
- 11. What is your opinion on privacy seals (such as TRUSTe, TÜVit TrustedSite, Privacy BBBOnline)?**
- 12. Would you allow a monitoring technology (such as a content security product for web or email) to filter data streams, which may contain personal data in order to find privacy leaks, even if this monitoring process reveals personal data and in a way violates privacy laws?**

APPENDIX B: REFERENCES

The following organizations have been contributing to the study in thought leader interviews.

Organization	Country	Type
Danish Data Protection Agency	Denmark	Government
Open Business Innovation	Denmark	Vendor
Copenhagen Hospital Cooperation (H:S)	Denmark	User
European Commission, DG Internal market	Europe	Government
IBM Zurich Research Lab	Switzerland	Vendor
Independent Centre for Privacy Protection	Germany	Research
Amadeus	Germany	User
MTU Aero Engines	Germany	User
SIGNAL IDUNA Gruppe	Germany	User
Microsoft	UK	Vendor