

Title: D14.0a – Framework V0

Author: WP 14.0

Editors: Simone Fischer-Hübner (Karlstad University), Christer Andersson (Karlstad University)

Reviewers: Gerard Lacoste (Compagnie IBM France)
Peter Keller (Swisscom AG)

Identifier: D14.0a

Type: Deliverable

Version: 6

Date: 15 June 2005

Status: Public

Class: Final

Summary

This document establishes the initial framework (V0) for the PRIME (Privacy and Identity Management for Europe) project, which is a holistic framework that provides a detailed “map” of privacy-enhancing identity management: it defines the problem space, the vision of PRIME, lists the PRIME stakeholders and clarifies their roles and responsibilities. It provides a set of application scenarios and describes the legal and social environment of PRIME as well as business models and economic drivers. Besides, it defines PRIME concepts and terminology and discusses PRIME models for users and metaphors.

This initial PRIME framework describes work in progress and will be further elaborated and refined for the PRIME framework V1.

Members of the PRIME consortium:

Compagnie IBM France	France
IBM Research GmbH	Switzerland
Unabhängiges Landeszentrum für Datenschutz	Germany
Technische University Dresden	Germany
Deutsche Lufthansa AG	Germany
Katholieke Universiteit Leuven	Belgium
T-Mobile Deutschland GmbH	Germany
Hewlett-Packard Ltd.	United Kingdom
Karlstads Universitet	Sweden
Università degli studi di Milano	Italy
Joint Research Centre	Italy
Centre National de la Recherche Scientifique	France
Johann Wolfgang Goethe Universität Frankfurt	Germany
Chaum LLC	United States of America
Rheinisch-Westfälische Technische Hochschule Aachen	Germany
Institut EURECOM	France
Erasmus Universiteit Rotterdam	The Netherlands
Stichting Katholieke Universiteit Brabant	The Netherlands
Fondazione Centro San Raffaele del Monte Tabor	Italy
Swisscom AG	Switzerland

Published PRIME documents

These documents are all available from the project website located at <http://www.prime-project.eu.org>

Excerpt of project "Description of work"	03-2004
Project presentation	06-2004
Framework – Version 0	06-2004

Foreword

PRIME partners from various disciplines have contributed as authors to this document. The following list names the main contributors for the chapters of this document:

- Chapter 1 (Introduction): Simone Fischer-Hübner;
- Chapter 2 (Vision of PRIME): Simone Fischer-Hübner;
- Chapter 3 (PRIME Stakeholders): John Borking, Simone Fischer-Hübner;
- Chapter 4.1 (Application Scenario Requirements): Henry Krasemann, Martin Rost, Marit Hansen;
- Chapter 4.2 (Location Based Services Application Scenarios): Georg Kramer, Lothar Fritsch, Markulf Kohlweiss, Christer Andersson, Simone Fischer-Hübner;
- Chapter 4.3 (E-Science: Review Process Scenario): Henry Krasemann, Martin Rost, Marit Hansen;
- Chapter 4.4 (E-Shopping Scenario): Henry Krasemann, Martin Rost, Marit Hansen, Peter Keller;
- Chapter 4.5 (Task Assignment Scenario): Henry Krasemann, Martin Rost, Marit Hansen;
- Chapter 4.6 (Ambient Intelligence Scenario): Giles Hogben;
- Chapter 5.1 (The Legal and Regulatory Framework for PRIME): Anna Buchta, Jos Dumortier, Henry Krasemann;
- Chapter 5.2 (Social Aspects of Privacy and Identity Management in Online Relationships Environment): Miriam Lips;
- Chapter 5.3 (Business Models and Economic Drivers): Jimmy Tseng, Lucas Bergkamp, John Borking;
- Chapter 5.4 (The Necessity of a Multidisciplinary Regulatory Approach to Develop PRIME Solutions): Miriam Lips;
- Chapter 6.1, Annex A (PRIME Concepts and Terminology): Giles Hogben;
- Chapter 6.2 (PRIME Models for Users and Metaphors): John Sören Pettersson.
- Chapter 7 (Conclusions and Outlook): Simone Fischer-Hübner, Christer Andersson

Table of Contents

1	Introduction	9
1.1	<i>Aims and Scope of the PRIME Framework.....</i>	9
1.2	<i>Problem Space.....</i>	9
1.3	<i>Related work.....</i>	10
1.4	<i>Structure and Scope of this Document.....</i>	10
2	Vision of PRIME	12
3	PRIME Stakeholders	13
4	Application Scenarios.....	17
4.1	<i>Requirements for Identity Management Systems.....</i>	17
4.2	<i>Location Based Services Application Scenarios.....</i>	20
4.2.1	City Guide	22
4.2.2	Travel Information and Navigation	24
4.2.3	Friend Finder	25
4.2.4	Area Event Services.....	28
4.2.5	Mobile Marketing and Couponing Services	29
4.2.6	E-Government: The electronic Witness.....	31
4.2.7	Disaster Management with Mobile Phones	32
4.2.8	Mobile Dating.....	34
4.2.9	Toll Collection	35
4.3	<i>E-Science: Review Process Scenario.....</i>	36
4.4	<i>E-Shopping Scenario</i>	38
4.5	<i>Task Assignment Scenario.....</i>	42
4.6	<i>Ambient Intelligence Scenario.....</i>	43
5	Environment	49
5.1	<i>The Legal and Regulatory Framework for PRIME.....</i>	49
5.1.1	Privacy as a Fundamental Human Right.....	49
5.1.2	The European Data Protection Directive	49
5.1.3	Directive on Privacy and Electronic Communications	51
5.1.4	Requirements Imposed on Data Controllers by the Directive 95/46/EC	52
5.1.5	Liability of ISPs/data controllers	53
5.1.6	Mandatory Retention of Traffic Data and its Implications for Privacy Protection	55
5.1.7	Legal Research Challenges.....	56
5.1.8	Legal Evaluation of Application Scenarios	58
5.2	<i>Social Aspects of Privacy and Identity Management in Online Relationships Environment.....</i>	61
5.2.1	Privacy as a Situated and Dynamic Concept	62
5.2.2	The Need to Reconceptualise Identification and Identity Management in Online Environments ...	63
5.2.3	Social Scientific Research Challenges.....	64
5.3	<i>Business Models and Economic Drivers</i>	64
5.3.1	The Strategic Value of Personal Data.....	65
5.3.2	Problems in Building Business Models	66
5.3.3	The Market for Privacy Enhancing Identity Management Solutions.....	67
5.3.4	The Social Costs of Privacy.....	67
5.3.5	The Economics of Privacy Enforcement	68
5.4	<i>The Necessity of a Multidisciplinary Regulatory Approach to Develop PRIME Solutions.....</i>	70
6	PRIME Concepts, Models and Metaphors	72
6.1	<i>PRIME Concepts and Terminology.....</i>	72
6.2	<i>PRIME Models for Users and Metaphors</i>	73
6.2.1	Introduction	73

6.2.2 Discussion of Definitions	73
6.2.3 Examples for IDM Models and Metaphors	75
6.2.4 Testing to Derive and Develop Models that are Intuitive to Users	78
7 Conclusions and Outlook.....	79
Appendix A Concepts, Actions and Properties	80
A.1 Concepts.....	80
A.1.1 Access.....	80
A.1.2 Anonymity	80
A.1.3 Credential	80
A.1.4 Data	81
A.1.5 Data Subject.....	81
A.1.6 Data Controller	81
A.1.7 Identifier	81
A.1.8 Identity.....	82
A.1.9 Identity Management.....	82
A.1.10 Information.....	82
A.1.11 Personally Identifiable Information.....	82
A.1.12 Privacy.....	83
A.1.13 Private Space	83
A.1.14 Profile	84
A.1.15 Pseudonym	84
A.1.16 Trust	84
A.2 Actions	84
A.2.1 Authenticate.....	84
A.2.2 Authorise	85
A.2.3 Disclose	85
A.2.4 Discriminate	85
A.2.5 Exploit	85
A.2.6 Identify	85
A.2.7 Impinge.....	86
A.2.8 Link	86
A.2.9 Process.....	86
A.2.10 Trace.....	86
A.2.11 Track.....	86
A.3 Properties.....	86
A.3.1 Anonymous.....	86
A.3.2 Informed	86
A.3.3 Identified.....	86
A.3.4 Identical	87
A.3.5 Minimised.....	87
A.3.6 Pseudonymous	87
A.3.7 Relevant.....	87
A.3.8 Sensitive	87
A.3.9 Transparent.....	87
A.3.10 Trusted.....	87
A.3.11 Trustworthy	88
A.3.12 Unlinkable	88
A.3.13 Unobservable.....	88
References	89

Table of Illustrations

Figure 1	M-business stakeholders' relationships.....	21
Figure 2	Domain of authors and reviewers in review scenario.....	37
Figure 3	E-Shopping Scenario and Paying with a Credit Card.....	39
Figure 4	Pseudonym Domains of a Customer in an E-Shopping Scenario.	40
Figure 5	Pseudonym Domains in Assignment of Tasks.	43
Figure 6	Identity Protector illustrated through masks.....	77

List of Acronyms

AMI	Ambient Intelligence
ATM	Automated Teller Machine
BEUC	European Consumer's Association
CEN	European Committee for Standardization
DSL	Digital Subscriber Line
EPC	Electronic Product Code
EPTA	European Pultrusion Technology Association
EU	European Union
FTC	U.S. Federal Trade Commission
GPS	Global Positioning System
GSM	Global System for Mobile Communications
HCI	Human-Computer Interaction
ICPP	Independent Centre for Privacy Protection
ICT	Internet Communication Technology
ICT	Information and Communication Technology
IDM	Identity Management
IMA	Identity Management Application
IMS	Identity Management System
ISP	Internet Service Provider
LBS	Location Based Services
LEA	Law Enforcement Agency
MIT	Massachusetts Institute of Technology
OECD	Organisation for Economic Co-operation and Development
OASIS	Organization for the Advancement of Structured Information Standards
PET	Privacy-Enhancing Technology
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
PRIME	Privacy and Identity Management for Europe
P3P	Platform for Privacy Preferences
RFID	Radio Frequency Identification
SET	Secure Electronic Transaction
SMS	Short Message Service
SMTP	Simple Mail Transfer Protocol
SNG	Studio Notarile Genghini
TIA	Total Information Awareness
UI	User Interface
UPS	United Parcel Service
W3C	World Wide Web Consortium
WLAN	Wireless Local Area Network

1 Introduction

1.1 *Aims and Scope of the PRIME Framework*

This document establishes the initial framework for the PRIME project.

A framework can be defined as a skeletal, structural frame [1] which provides a particular set of rules, ideas, or beliefs which are used to deal with problems or to decide what to do [2].

The PRIME framework is a holistic framework for privacy-enhanced identity management that aims at serving as a forum to facilitate multidisciplinary exchanges between the PRIME partners to share their views, knowledge and experience about the definition of the PRIME problem space, the main directions and challenges of the project, and the basic concepts and terminology they will use to communicate and work in synergy. The PRIME framework provides a detailed “map” of privacy-enhancing identity management: it defines the problem space, terminology, concepts, models for users and metaphors, application scenarios, the legal, social and technical options, possible business cases, and the technical challenges. Moreover, the framework will encompass a technical architecture that specifically focuses on how the various mechanisms can or must interrelate.

The PRIME framework does not only establish a base for all PRIME partners for developing PRIME. It also aims to provide the basis for the widespread deployment of privacy-enhancing mechanisms and identity management. In particular, it is intended to enable the deployment of privacy-enhancing mechanisms and identity management by allowing all PRIME stakeholders to share concepts, terminology, requirements, best practices, evaluation methods, guidelines and recommendations. The PRIME framework is intended to serve as a reference for all concerned stakeholders and therefore it also clarifies the stakeholders’ roles and responsibilities.

This initial PRIME framework V0 describes work in progress and presents initial views and knowledge within the PRIME consortium. It will be further elaborated and refined for the PRIME framework V1.

1.2 *Problem Space*

The name PRIME standing for Privacy and Identity Management for Europe expresses the problem space and boundaries of PRIME project and of its framework.

The PRIME problem space is privacy-enhancing identity management.

Within the scope of PRIME, Identity Management (IDM) has earlier been defined to subsume all functionality that supports the use of multiple identities, by the identity owners (user-side IDM) and by those parties with whom the owners interact (services-side IDM) (see EC Contract for PRIME, Annex 1, p.1).

PRIME will address privacy-enhancing IDM to support strong privacy by particularly avoiding or reducing identification and by technically enforcing informational self-determination. The PRIME framework starts with the objective of PRIME to serve the individual users by helping them to keep their personal data under their control. It acknowledges that 1) individuals need to exchange data with individuals and with other organisations in specific contexts, and 2) the society (as a whole, e.g. a court) can access the individuals’ data in specific situations.

The PRIME problems space is primarily focused on Europe: PRIME will use European legislation as its basic reference, although PRIME might pinpoint areas where the European legislation could be improved. The PRIME framework’s starting points are the basic rights, values and behaviour of the European user. PRIME should help to enforce basic privacy principles as for instance those expressed

Privacy and Identity Management for Europe

by the Organisation for Economic Co-operation and Development (OECD) privacy guidelines. At the same time PRIME must take due account of the development of the information society.

1.3 Related work

There has been some previous work on holistic frameworks for Privacy-Enhancing Technologies (PET) and security that are mainly covering technical aspects. The first basic work on technical aspects of anonymity on communication and application levels was provided by David Chaum [3] [4]. Also Pfitzmann et al. have already in the eighties published a framework for anonymity technologies and for definitions of related terms [5]. Another example is SEMPER [6], which is a holistic e-commerce framework with multilateral security, which is addressing aspects of security, fair trade, credential management, pseudonymity, anonymous payment and anonymous communication.

The studies by the Dutch Data Protection Authority and the Information and Privacy Commissioner of Ontario/Canada on “Privacy-Enhancing Technologies: The path to anonymity” provides an early PET framework covering an overview to PET concepts and technologies, legal aspects of PET, application examples as well as surveys addressing consumer and business-related aspects [7] [8].

A Multilateral Security framework that focuses on reachability and security management and includes core elements of Identity Management was presented in [9]. This framework comprises factors from informatics, economics, business sciences, law, social and labour sciences.

Further related work on frameworks for identity management have been done and published by the Open Group and by the Independent Centre for Privacy Protection (ICPP) in cooperation with the Studio Notarile Genghini (SNG).

The Open Group White Paper on Identity Management [10] explores technical key concepts (trust, authentication, provisioning, authorisation, and directories) of identity management and examines identity management from various perspectives, including business, security, personal, and technical. A support for strong privacy is, however, not covered.

The “Identity Management Systems: Identification and Comparison Study” by PRIME partner ICPP and SNG [11] is the one that is most related to the PRIME framework. This study also presents a multidisciplinary framework for privacy-enhanced IDM, which includes technical, legal and sociological perspectives for the definitions of terms and presents usage scenarios. Some of these usage scenarios are also in slightly adapted form presented in the PRIME Framework V0. However, a major focus of the ICPP/SNG comparison study is also the analysis of available identity management applications and a survey on expectations on Identity Management Systems (IMS). In contrast to the ICPP/SNG study, the PRIME framework also investigates the business perspective including business models, is more broadly investigating the legal and social environment for PRIME, and will in its next versions also include a technical architecture (PRIME architecture) and PRIME-based solutions for selected application scenarios.

1.4 Structure and Scope of this Document

Partners from all involved disciplines have contributed to the initial PRIME Framework.

Chapter 2 summarizes the vision of PRIME as shared by project participants.

Chapter 3 identifies the stakeholders relevant to the PRIME problem space as well as their roles and responsibilities.

Chapter 4 presents a set of application scenarios to be considered for PRIME research. This set includes Location-Based Services (LBS) and Ambient Intelligence (AMI) Scenarios, which belong to the initial set of application scenarios that are listed in Annex I of the EC Contract for PRIME. Scenarios on e-health, privacy-preserving customer databases, and anonymous access to infrastructures for mobile workers, which are also listed there and for which application providers within the project have committed to collaborate on PRIME-based solutions, will be further elaborated and presented in PRIME Framework V.1.

Privacy and Identity Management for Europe

Chapter 5 introduces the non-technical environment of PRIME, including legal, social, and economic issues and their relationships.

Chapter 6 is devoted to PRIME concepts, terminology, for which definitions are presented in Annex A, and to IDM models for users and metaphors.

Chapter 7 is providing conclusions and an outlook to the next Framework version.

A chapter on the PRIME architecture will be introduced in later versions of the PRIME framework as the architecture reaches agreement and maturity.

2 Vision of PRIME

Information and Communication Technologies are pervading our Society that is rapidly transforming into an Information Society. High penetration of mobile communication and Internet, including broadband connections by means of cable, some type of Digital Subscriber Line (xDSL), Wireless Local Area Network (WLAN), Bluetooth, Radio Frequency Identification (RFID) tags will be used for ad-hoc communications at home, in the office, in cars, trains, airports, etc. Various technical trends and changes take place in PRIME application areas like e-government and e-voting, e-health, location-based services and e-commerce.

With the advent of the Information Society physical barriers of distance and time are abolished and our lives rely more and more on technological transposition and on the extension of our real physical world into a virtual world based on high-performance communications and information processing. With this extension of the real world into a virtual one where personal information meaning power is the asset, it is however essential to protect that asset to preserve the individual's autonomy.

Although the European regulatory and legal framework is an important instrument for data protection, individuals are nonetheless lacking effective control over their data in today's Information Society. The current development of technologies has been neglecting to maintain the protection of individual's sovereignty over his/her private sphere and particularly individual's control over personal data that the real non-electronic world naturally and culturally provides. It is however critical to our society and to democracy to retain and maintain individual's privacy and thus to protect privacy and particularly the individual's right to informational self-determination. Society needs to initiate a major shift from organisations' control back to the individual's control over personal data.

PRIME will develop the missing technological link towards restoring individual's privacy in the virtual world. PRIME will develop privacy-enhancing identity management tools and will promote the integration of these tools into legacy and new applications. These tools will enable individuals to increase their autonomy without undermining the foundations of democratic societies (by preventing misuse of these tools and by supporting legitimate law enforcement interests), to retain and maintain control and thus to technically enforce informational self-determination in the information society age.

In particular, PRIME tools will allow individuals to have control over their personal data including transparency about who has received what personal data related to them and possibilities to trace personal data being passed on. Besides, PRIME tools will include authorisation tools helping them to define who has the right to do what with one's personal data, as well as tools allowing them to define and switch identities, pseudonyms and related profiles. PRIME will help to establish privacy principles among various players (citizens, organisations, government and society) and will establish technical and procedural standards as well as technical tools supporting these principles.

Privacy-enhancing technologies represent a potential enabler for business. However, the PRIME approach must accommodate a migration path from the existing solutions, i.e. PRIME solutions have to fit into the reality of the market's development.

As users' needs make a market, PRIME will follow the strategy that, starting from the existing European legislation, it raises awareness of the layman about privacy threats, and the risks of losing autonomy and risks to democracy. At the same time it fosters business conducted with privacy-enhancing identity management technology that restores trust. PRIME will promote the use of privacy-enhancing identity management on broad scale by providing easy-to-use intuitive tools and educational tutorials for end users.

Historically, privacy has always been a particularly important right for European citizens. The advanced technology developed by PRIME will enable trust and confidence in the Information Society, will show how advanced technology can directly support European privacy regulations, and will increase European leadership in the area of privacy and privacy-enhancing technologies.

3 PRIME Stakeholders

The success of PRIME and beyond in the area of privacy and identity management will primarily rely on the capacity of its participating experts to establish credibility, to interact and exchange information about the vision of PRIME, its approach, progress and results.

PRIME is faced with the fact that the awareness of the EU Data Protection Directive 95/46/EC and of the EU Directive 2002/58/EC on Privacy and Electronic Communications and consequently the national privacy legislation of the EU Member States is low and that the fight against terrorism after 9.11 has not made privacy protection more popular. However, the EU privacy directives have great consequences for our information driven society. Decision makers and controllers of personal data in the public administration and commercial businesses have to be convinced why PRIME is beneficial to their organizations and businesses. Obstacles to introducing privacy-enhancing technologies have to be removed, as in many organisations the cultural attitude is anti-privacy as the short-term objectives are incompatible with privacy protection.

In order to support these objectives, the identification of the key actors and the creation of a wider permanent community of stakeholders are crucial.

The following stakeholders have been identified:

- *Individuals*, who are end users and/or data subjects (so-called uses, i.e. persons about whom personal data are processed) of Information and Communication Technology (ICT) systems and applications. As it will be illustrated in the following chapter, users can for instance perform the roles of service subscribers, citizens, witnesses, authors, customers or clients within PRIME application areas such as LBS, e-government, e-shopping, e-science. Users are also employees that use information systems inside their employers' premises, processing at the same time their personal data (time of access, own biometrics, etc.) as well as others personal data. They should be educated about the use of personal data and the deployment of PRIME applications.

PRIME will only be successful if user friendly PRIME tools will be broadly applied by users, and hence, PRIME will involve users in acceptance, usability and pilot studies to specifically take user needs into consideration;

- *User and consumer associations* on national and European level like The European Consumer's Association (BEUC). Also the cooperation with user/consumer associations will be helpful to elicit user's requirements for PRIME-based solutions;
- *Policy makers and parliamentarians*, nationally and on a European level. They are representatives of the citizens as potential users and data subjects and should protect the privacy interests and rights of them. They also have the possibility to promote PRIME-based solutions by for example creating legal rules for the obligatory deployment of privacy threat analyses, privacy audits and privacy-enhancing technologies and by facilitating this by budgetary allocation realising inter alia the public authorities to first hand purchase products which have been awarded a privacy seal;
- *Privacy commissioners and Data Protection Authorities* in the EU member states and subsequently *Art. 29 Working Party*. The existence of vigorous supervisory authorities has been regarded as a *conditio sine qua non* of good privacy protection as the law is not self-enacting and the culture of informational privacy protection does not develop itself without a body that can act when things go out of hand. Therefore they should be informed at regular intervals about PRIME and because of that they should use their influence to promote the large deployment of PRIME-based solutions in government and in commercial organisations;
- *Research communities* (governmental and commercial) dealing with privacy issues, technology assessment organisations on national and European level, like European Parliamentary

Privacy and Identity Management for Europe

Technology Assessment Association (EPTA), departments and faculties of universities that focus on privacy issues. They should be stimulated to cooperate with PRIME partners in a scientific discussion and research on privacy-enhanced identity management solutions;

- *Organisations that use information systems and process personal data* within the government, commerce and industry, like banks, insurance companies, credit card companies, toll collection companies, network operators, service providers (LBS providers, push service providers, internet service providers (ISP), internet access providers, content providers and certificate service providers), advertisers and governmental authorities. They perform the role of the data controllers (i.e. the entities that are responsible for the processing of personal data of users and uses), and as such they have to strictly follow data protection legislation.

Privacy-enhancing IDM can assist such organisations in guaranteeing law compliance. Privacy officials of these organisations should for this reason should be trained in using privacy-enhancing IDM and subsequently promote the deployment of privacy-enhancing IDM within their organisations;

Privacy legislation (and its implementation in the member states) is an important driver for enterprises to develop and implement privacy features into information systems. An enterprise does not achieve regulatory compliance without direct costs to itself. However, in addition to managing the risk of regulatory non-compliance, other economic drivers for good privacy practice do exist (see also chapter 5.3). Hence, these organisations should also be persuaded about the competitive opportunities (competitive edge) of the application of PRIME-based solutions, which will allow them to offer more privacy-friendly services to their clients and customers;

Furthermore, providers of infrastructures (service providers and network operators) should also be invited to participate in the discussions around the PRIME research;

- *Standardization organisations* on national and on international level like European Committee for Standardization (CEN), World Wide Web Consortium (W3C), and the Organization for the Advancement of Structured Information Standards (OASIS). Their cooperation will be important for the transfer of PRIME results into standardisation to ensure interoperability with existing systems and concepts;
- *System developers, system designers, suppliers of ICT products and services* should be motivated to see PET as a business enabler and to integrate PRIME concepts and solutions into their systems and products. Thereby they can help to trigger persuasive deployment of privacy-enhancing IDM solutions;
- *Business and industry associations, employer associations and Trade unions* on a national and European level; their support is also needed for a broad deployment of PRIME-based solutions within organisations. They have to be well informed about the opportunities that PRIME can provide from a business and from a user perspective;
- *Law enforcement authorities* on national level and international bodies like Eurojust, Europol and Interpol. Their representatives should participate in discussions with PRIME partners and advice them about legitimate law enforcement interests that have to be supported by PRIME-based solutions and that are in an appropriate balance with the privacy rights of users and uses. In particular circumstances under which anonymity should be revoked in order to prosecute criminals have to be well defined and agreed upon;
- *Media*, especially those specialised in information and communication technology should help to spread information about the PRIME project and its results to the public and to special interest groups (e.g. readers of technical papers or relevant scientific journals).

A cross-section of all these stakeholders will participate in the PRIME reference group. The Reference Group will be regularly updated on the results and plans of PRIME. Besides, the project will invite them to give their specific input and feedback on the results of PRIME to validate requirements and to support project dissemination and exploitation.

Broad support and commitment from the stakeholders about PRIME is highly needed. Therefore PRIME concepts have to be clarified and the benefits of proposed Privacy and Identity Management solutions have to be explained. This could for instance be achieved by the following means and strategies:

- **Workshops and visits:** Organising workshops and giving presentations are valuable tools in the promotion of PRIME, but might attract only those that already are convinced of the application of PRIME. Hence, also personal high-level visits to those people that still have to be convinced are the most effective way to achieve support and commitment. A visit plan has to be developed;

Special awareness seminar and workshops for consumers should be organized. A lot of citizens in EU-countries are afraid to use their credit card in online transactions via the Internet, often not as a result of former personal problems but as a consequence of disseminated anecdotal information in society. However, in many cases they do not know (exactly) what may happen to personal data provided in an online environment. Citizens, in using the Internet, are generally not aware of the variety of privacy risks and/or the ways to prevent them. Many Internet users do not know the basics of how their online activities are observed, nor do they use available tools to protect themselves. This situation of low transparency to citizens about the informing and observing capacities of ICTs is not limited to Internet use, but is applicable to other ICT-applications (e.g. video surveillance, smart card technology) as well;

Also, citizens may not be aware about (new) possibilities of data collection and data exchange, as a result of more or less 'hidden' ICT-applications in various social activities. For instance, citizens may not be aware of the fact that their local government has put surveillance cameras in several public places, with the aim to enhance public safety. Besides, general awareness of changing privacy concerns will usually be low for situations in which (public or private) organisations, to which citizens have a more or less durable relationship, are substituting technologies in their information relationships with citizens (e.g. using smart cards instead of pin cards; using the internet instead of a closed network system). Consequently in general, raising awareness of citizens on the one hand and improving the organisation's transparency on the collection and use of personal data on the other hand will be highly important to promote the use of ICTs in a privacy friendly way;

Thus the awareness of users and consumers in particular should be raised about privacy and identity management issues and how PRIME application can help;

- **Special attention has to be paid to the stakeholders in the public sector:** The public sector has to be convinced that PRIME and other Privacy-Enhancing Technologies solutions are a structural way to protect privacy as they are bound to implement the European Union (EU) directives by definition. They should educate and propagandize that: privacy is a public service! Especially the national data protection authorities are crucial in the promotion and application of PRIME and PETs. Together with the law enforcement police organisations, they are the first target to approach for PRIME for obtaining support and pro-active action for implementing PRIME solutions;
- **Bridge heads:** With the support of PRIME participants other stakeholders can be visited and as a result a national dedicated group of PRIME friends can be set up as bridge head promoting PRIME regularly and keeping the stakeholders awake. Press releases about PRIME should be translated and issued by these bridge heads. The visits will also reveal what obstacles have to be removed and what approaches are most successful;
- **Knowledge base:** The construction, population and maintenance of a comprehensive knowledge base are pivotal to sustaining the off-line and on-line activities of PRIME. It will provide members, as well as external interested parties, with added value access to information, contacts and activities. This knowledge base will ensure excellence by having links to the most up-to-date information available concerning privacy and identity management. It will contain the findings of PRIME, in the technical, legal, sociologic and economic field. It can be used to

Privacy and Identity Management for Europe

keep all stakeholders informed and to convince them about the relevance and importance of PRIME.

4 Application Scenarios

PRIME will base its research on a search for solutions to a set of well-defined application scenarios. A few of these applications scenarios will be subject to the development of applications prototypes.

In this chapter, after discussing general requirements for IDM systems, we present a first set of application scenarios that have been elaborated by PRIME participants for the applications Location Based Services, e-science, e-shopping, task assignments within organisations as well as for AMI applications. Each application scenario is providing a description of how services are provided today within the application area (status quo), what are problems and requirements to be addressed by PRIME, and what is the motivation and/or vision for a PRIME-based solution.

The scenarios E-Science, E-Shopping and task assignments within organisations are based on scenarios that were developed in the IDM system study of ICPP/SNG [11]. These scenarios use the concept of a *pseudonym domain*¹ in which a subject is known under a unique identifier or pseudonym. Each pseudonym domain defines the scope of the pseudonym; outside it may not be relevant anymore. For each pseudonym domain the properties the pseudonym must have can be different. The user himself/herself or third party entities which are in multiple pseudonym domains may perform the task of creating new pseudonyms and assigning them.

4.1 Requirements for Identity Management Systems

Standard demands to IDM systems that were elaborated in the ICPP/SNG study are listed in Table 1 below. These requirements should be mandatory for Identity Management Applications that are designed for consumer and organisational acceptance. They may be extended in specific contexts and scenarios. The categories have been chosen according to Consumer Requirements in Standardisation relating to the Information Society [12].

Taking into account the views of all actors, an IDM system should fulfil a specific functionality: It should help the user to manage his/her identity. For identity management, we distinguish between a general, prior identity administration which is independent from current communications and the management of identities during specific communications and situational contexts. For the latter, it is necessary for the Identity Management Application (IMA) to have a gateway functionality, i.e. to have interfaces to the communication partners, especially to digital networks. Management always is defined as taking decisions based on notice and control. These requirements apply to the process of identity management, i.e., informing the user about a situational context and offering choices if appropriate.

This means in more detail:

a) Identity administration:

The IMA has to provide the possibility to administrate the partial identities and identity data, i.e., handling and representation of identities. The technical processes for creating the data set

¹ Pseudonym Domains are similar to "pseudo-identity domains", which have been introduced earlier by John Borking when proposing the concept of the identity protector: "To implement matters technically, a system element called the 'identity protector' is used within the data system to convert the identity of the person involved (the person whose data are being processed - the 'data subject') into one or more pseudo-identities. The placement of the identity protector provides for at least two different domains within the data system; one domain where the identity of the person involved is known or accessible (the identity domain) and at least one domain where this is not the case (the pseudo-identity domain). The aim of the pseudo-identity domain is to make sure the person involved cannot be traced on the basis of previously obtained personal data, and vice-versa, to make sure the personal data cannot be found on the basis of the obtained identity." [cf. John J. Borking, Charles D. Raab: Laws, PETs and other Technologies for Privacy Protection; Refereed Article; Journal of Information, Law & Technology (JILT), Issue 1, 2001; <http://elj.warwick.ac.uk/jilt/01-1/borking.html>].

entry and updating or deleting it on demand have to be implemented. This data set entry may also comprise digital signatures, certificates, or credentials.

b) Gateway:

The IMA can act as a gateway for digital communication. Thus it has to provide functionality to manage data exchange with all communication partners.

c) Notice and control:

The core functionality of an IMA is the option of choosing partial identities as required or desired in a specific context and situation. Firstly, the user has to be aware of context and situation. This may comprise information about the communication partner, about the role the user is acting in, about former transactions, about the conditions for data exchange. This transparency function is necessary for an informed choice which data to transmit and for a later examination of data exchange. Secondly, the user should be able to control when to release which personal data to whom. The process of choosing partial identities and identity data can be explicit, e.g., by asking the user in a pop-up window, or the desired behaviour of the IMA can be pre-defined in policies which contain rules on the decision between partial identities or act according to default values. External information may be integrated in this process of choosing personal data as well.

The following table contains a summary of the requirements for an Identity Management System compiled out of the different scenarios. It is arranged in the main categories functionality, usability, security, privacy, law enforcement / liability, trustworthiness, affordability, and interoperability.

Table 1 Requirements for Identity Management Systems

Category	Characteristics and substantiation
Functionality	<ul style="list-style-type: none"> • Identity Administration <ul style="list-style-type: none"> • Transaction pseudonym², group pseudonym possible³, addressable pseudonym⁴ • AMI: unstructured pseudonym unique to sensors (keys to a database) • Communication gateway <ul style="list-style-type: none"> • Handling of communication between user and other parties

² The scope of the *transaction pseudonym* is only the transaction itself. This means, for each transaction a completely different transaction pseudonym is used, e.g., randomly generated transaction numbers for online-banking. Thus, there is at least no possibility to link different transactions by these pseudonyms. Therefore, transaction pseudonyms can be used to realize as strong anonymity as possible.

³ A *group pseudonym* is a pseudonym which is used by different subjects, i.e., a group of persons. They could use the group pseudonym simultaneously or in turn. The use of a group pseudonym decreases the degree of information of linkage to a specific subject. The group of pseudonym holders acts as an anonymity set. A similar effect over time can be achieved by transferring pseudonyms to other people so that they are used by one after the other.

⁴ An *addressable pseudonym* can be used as an address by which messages reach the pseudonym holder. The address may reveal no (additional) information about the pseudonym holder. It only gives an address for an appropriate communication procedure, e.g. the pseudonym may be a phone number, an e-mail address or a mailbox address. (Note that there may be other possibilities to find out who the pseudonym holder is, e.g., by tracing messages sent or by sending specific content which leads to a revealing action of the pseudonym holder.) Normally the pseudonyms are specific addresses which reach only one pseudonym holder, but addressable group pseudonyms are also possible. Note that the pseudonym may be only addressable by specific parties and not by everybody. The operational quality of the addressable pseudonym may be extended e.g. by notice of receipt.

	<ul style="list-style-type: none"> • LBS: mobility of the user and terminal/location sensitivity • Sensors in the user's environment possible • Notice: <ul style="list-style-type: none"> • Identifying the interacting parties, verifying "who" "did what" and "when" in an electronic interaction on a network • Control <ul style="list-style-type: none"> • Pseudonym <i>addressable</i> by organisation • <i>Re-use</i> of pseudonym⁵ possible for special advantages/establish reputation • Possibility of reliable re-pseudonymisation/identification • Possibility to use real name/identity • LBS: user can easily stop localisation at any time while they are using the service
Usability	<ul style="list-style-type: none"> • <i>Basic usability and easy to use</i> functionality for all participants in the system, which is implemented/addressed in system design, documentation, and possibly support, is a mandatory requirement • More complex usability (only if necessary and essential) possible in case of use by professionals/well-skilled users
Security	<ul style="list-style-type: none"> • Availability • Integrity <ul style="list-style-type: none"> • Prevention of manipulation; non-repudiation • Prevention of accidentally false addressing • Reliability of service; "what you see is what you sign" • Confidentiality <ul style="list-style-type: none"> • Particularly for sensitive data • Prevention of identity theft, reputation theft and misuse of, e.g., credit card numbers; non-repudiation; prevention of accidentally false addressing • Prevention of unauthorised access • Prevention of plagiarism, i.e., authenticity and in some cases also non-reputability desired
Privacy	<ul style="list-style-type: none"> • The legal requirements, which can differ in the various scenarios, have to be fulfilled (control, information for users,

⁵ A *re-usable pseudonym* can be used more than once by the pseudonym holder, i.e., for multiple actions. A *durable pseudonym* characterises a longer binding between pseudonym and pseudonym holder. A transaction pseudonym where the linkage between pseudonym and pseudonym holder is not stored is non-durable.

	<p>purpose of data processing, etc.)</p> <ul style="list-style-type: none"> • Prevention of profiling / linkability / location tracking by organisation / companies – minimisation of cross-referencing • Data minimisation and avoidance, possibility of <i>anonymity</i> of the user (e.g. anonymous payment) • Prevention of hidden data collection / spam • At the user's side possibly <i>logging</i> of the relevant communication (inquiry and response) • <i>Transparency</i> (what happens to what kind of data and what data are transferred to whom – e.g. local position / identity)
Law Enforcement / Liability	<ul style="list-style-type: none"> • The legal requirements for law enforcement (e.g. data retention in some countries), which can differ in the various scenarios, have to be fulfilled • Generating auditable data: digital evidence with probative value necessary in case of identity theft, reputation theft, warranty claims, wrong delivery, tax fraud, unauthorised access, civil action, ... • Clear line of responsibility
Trustworthiness	<ul style="list-style-type: none"> • Measures for objective trustworthiness of the Identity Management System (by implementing usability, security, privacy and law enforcement functionality where appropriate) should be taken, supported by measures for gaining trust
Affordability	<ul style="list-style-type: none"> • The integration of IDM functionality should not make transactions far more expensive than it would cost without IDM functionality. If possible, by integration of this functionality the participants also gain additional economical advantage by creating new business models and services • Cheap in case of every-day use and every-person use • Usage could be in the interests of the government • E-Court: within the limits of the normal fees by court • E-Government: maybe paid by society • For important business with very high security / probative value more expensive than for every day usage
Interoperability	<ul style="list-style-type: none"> • The new functionality should be both compliant to legacy systems and to new standards

In the following application scenario descriptions, the privacy requirements and other more scenario-specific requirements will be elaborated in more detail for each scenario.

4.2 Location Based Services Application Scenarios

Location based service applications are different from general Internet applications in two aspects:

- **Mobility of the user and terminal:** a user / terminal accesses services from a variety of networks with changing network parameters and possible periods of no connectivity;

- **Location sensitivity:** applications can process location information to add value to an application.

Giovanni Camponovo [13] describes a generic m-business model as shown in Figure 1 below. Mobile commerce applications, as all applications, generally consist of services, technology, users, communication and regulation.

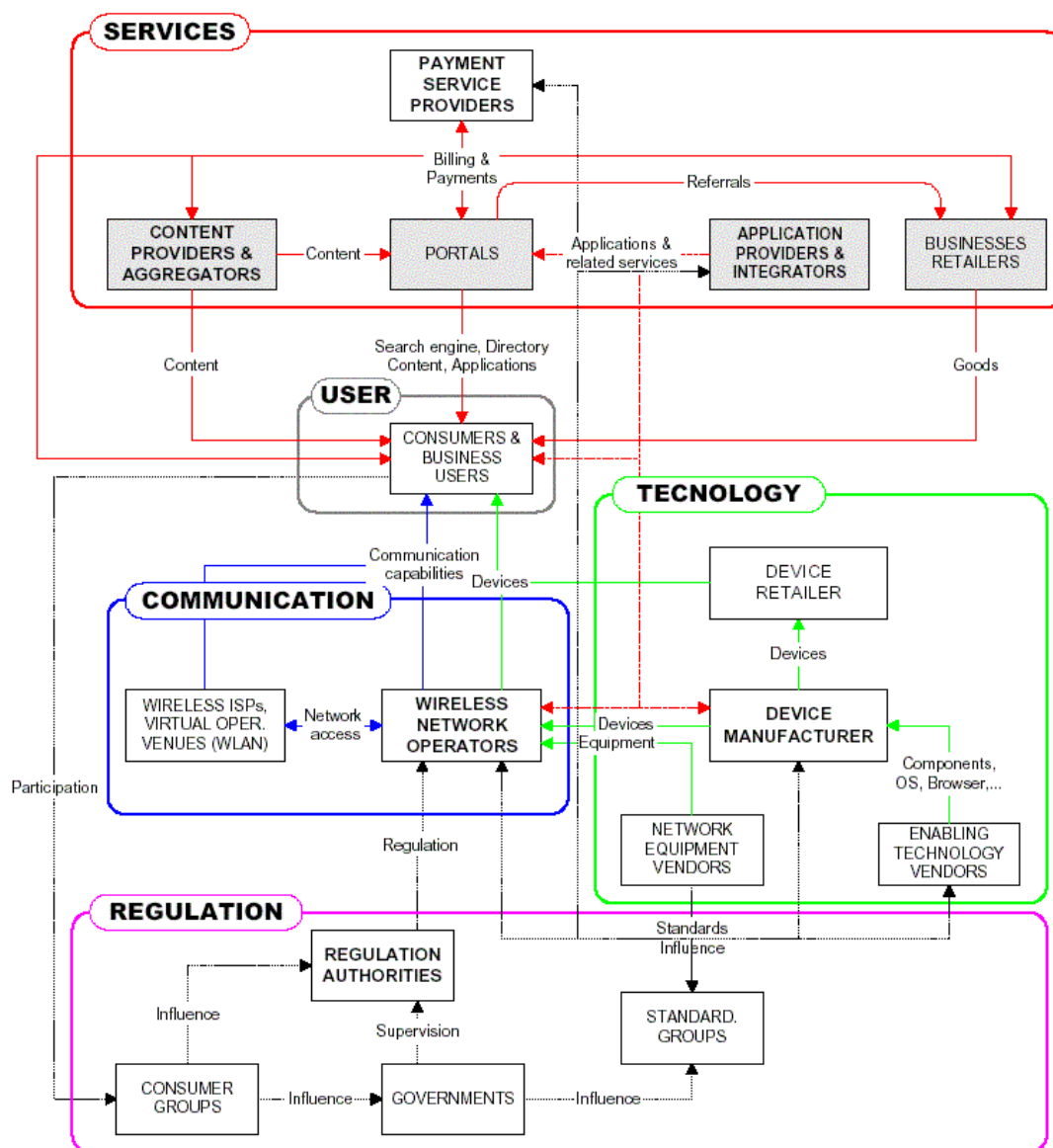


Figure 1 M-business stakeholders' relationships.

Location data for LBS is either provided by the communication network (e.g. a mobile phone network) or by specialized hardware at the user terminal, which could be a beacon or a Global Positioning (GPS) receiver. The players in Figure 1 thus can be assumed to be the same for m-commerce with location based services.

We generally assume that LBS application providers are separate organisations from the mobile network operators. However network operators may deploy location based services themselves.

This creates the problem that the application and the location generation are owned by the same organisation that can collect and store personal data of their customers. Until there are networks that

Privacy and Identity Management for Europe

securely manage location it is necessary to separate the network from the application by means of an identity protector. This is the exact scenario as dealing with external application providers.

The figure above illustrates several flows of information that are present in business applications. Data flows exist from the user via the infrastructure to the portal/application. Also, flows exist for payment and delivery of goods. Thus, any application that is to be protected by PRIME must consider all flows of information that appear.

User mobility among the LBS / M-Commerce infrastructure is another dimension to be considered: users of mobile applications “roam” from one particular network access point to another. Also, they “roam” from one service provider to another. On top of this, they re-use applications or use applications for the first time.

The following sections describe and analyse some example applications of LBS that are either operational, or will be available in the near future.

4.2.1 City Guide

Description of the Status Quo

When a tourist arrives to a foreign city, he/she can use different kinds of city guide services to get information about nearby restaurants, hotels, places of interest, exhibitions, ATMs (Automated Teller Machines), pharmacies, cinema programmes, nearest taxi stands and much more. This information is dependent on the user’s location (or more specifically, the location of his/her mobile device), which normally is determined by the mobile network.

In general, when a tourist wants to use a city guide service, he/she explicitly selects the service he/she wants to use. When using the service, the LBS provider initiates a localisation to learn about the current location of the user. The user has the possibility to avoid the localisation by typing in the address manually into the mobile phone, but this is less convenient and often the user does not know the local address of his/her current position.

The user of this service either pays the LBS provider directly, or via the network operator. Currently, anonymous payment is not possible.

Location-based mobile gaming is another example of an application that shares many of the properties of a city guide service.

Problems and Requirements

Main privacy risks are unsolicited profiling, location tracking and hidden data collection. LBS providers and mobile network operators could easily track their customers’ current position and profile their customers’ activities, interests, and movements, and further they could possibly share such customer profiles with other service providers. Also, if these profiles fall into the hands of unauthorised persons (criminals), they could be a source for crimes such as blackmailing, raping, kidnapping, etc. Currently there is little transparency about what data are collected and how it will be used. Users could be unaware of the extent of lawful interception of their location and use of LBS. Depending on national law, different lawful interceptions may be provided for. As privacy is also a civil right, users should be informed that the location data collected for a service may be used by law enforcement agencies. It is also part of their civil right to use other services, that do not collect this data, or promise to delete it after a certain time.

Table 2 below describes a number of possible privacy problems that must be considered in a PRIME-based solution.

Table 2 Problems in the City Guide Scenario

Problem type	Textual description	Examples
Unsolicited profiling	The long term collection of personal information with the aim of creating detailed profiles	Blackmailing of politicians, digging in the past
Unsolicited tracking	Use of information about the current position and movement of persons	Kidnapping, burglary
Merging data sources	The merging of data sources may intensify the problems related to profiling and tracking	Collaboration of different service providers or of service providers with network operators
SPAM	Marketing information is valuable for spammers. User loses control over his/her reachability	Unsolicited email sent to persons with matching profiles

The privacy requirements are as follows:

- LBS can only be activated by the users, and data is only collected with the users' informed consent;
- The users have control over what information is released about them and for what services. The users must also have the possibility to set their privacy preferences on "per service" basis, which means that different settings could apply for different services. Users need to maintain and provide a proof of the consent they have given to a particular service;
- The principles of data minimisation and avoidance should be followed. No more data than necessary should be collected by the LBS providers and they should not be kept longer than necessary. It should be possible for users to be anonymous towards a third party LBS provider if the identities of the users are not needed for providing the service;
- User-related data used by different third party LBS providers should not be linkable;
- Anonymous payment services should be available.

Vision for a PRIME-based Solution

To make use of a city guide service, the user explicitly activates the desired service, and specifies what kind of local information he/she is interested in. The user is presented with information telling him/her what kinds of data (e.g., local position and/or identity) are transferred and to whom it is transferred. For convenience reasons the user can configure his/her privacy settings to specify that some information is transferred by default. These kinds of decisions can be stored either per service or in general. A reconfiguration of the privacy setting is possible at any time.

No additional data is collected besides the data necessary in order to provide the service. Services where no other data but the current position is needed can be provided anonymously by third party LBS providers. In these cases, the user has the possibility to pay for the service using an anonymous payment scheme.

For enforcing their policies, the users are provided with proof of the consent they gave to LBS business partners. Proof should be supported by generating auditable data, e.g. digitally watermarked policies and other ways of creating audit evidence. Such schemes could include electronically signed policies and receipts from the application provider and steganography to ease audits.

4.2.2 Travel Information and Navigation

Description of the Status Quo

When driving from one location A to another location B, the user of a travel information service can receive such information as routing, information about the traffic situation at the user's current location, or at the destination B. If there is a traffic jam on the motorway somewhere around B, or if the user is approaching a portion of the road that is very slippery, the user can be notified.

The travel information service works by tracking the user in order to provide the user's mobile device with current traffic information in the whereabouts of the user. The user can also check the traffic conditions in other locations by manually entering the locations.

One productive solution is provided by T-Traffic on T-Mobile's GSM (Global System for Mobile Communications) network. The "NaviGate" product connects a GPS receiver to mobile phones to localize a vehicle, and then compute a route on a server. Frequent updates of traffic situations are sent to the phone. The routing server knows about the subscriber ID and the travel destinations.

Problems and Requirements

Also in this scenario, potential privacy problems could be location tracking, profiling and hidden data collection. There is a risk that the LBS provider creates user profiles based on the different locations the users have visited, as well as the information they have requested at each location. Another potential problem is that the users can receive much unwanted information in their mobile devices. Further, there is little transparency, the users may not be aware of what kinds of data are collected by the LBS provider, how they are processed and for what period of time they are kept. Users could be unaware of the extent of lawful interception of their location and use of LBS. Depending on national law, different lawful interceptions may be provided for. As privacy is also a civil right, users should be informed that the location data collected for a service may be used by law enforcement agencies. It is also part of their civil right to use other services, that do not collect this data, or promise to delete it after a certain time.

Table 3 below describes a number of possible privacy problems that must be considered in a PRIME-based solution.

Table 3 Problems in the Travel Information Scenario

Problem type	Textual description	Examples
Unsolicited profiling	The long term collection of personal information with the aim of creating detailed profiles	Blackmailing of politicians, digging in the past
Unsolicited tracking	Use of information about the current movement of persons	Kidnapping, burglary
Merging data sources	The merging of data sources may intensify the problems related to profiling and tracking	Collaboration of different service providers or of service providers with network operators
Extraction of sensitive information	Use of location information to extract sensitive information	People that consult medical specialists
SPAM	Marketing information is valuable for spammers. User loses control over his/her reachability	Unsolicited email sent to persons with matching profiles

The privacy requirements are as follows:

- Transparency for users and no hidden data collection or processing;
- The users have control over what information is released about them and for which services and for how long. Besides, they can control what kind of information should be presented to them. The users also have the possibility to set their privacy preferences on “per service” basis, which means that different settings could apply for different services. For enforcing their policies, the users are provided with proof of the consent they gave to LBS business partners. Proof should be supported by generating auditable data, e.g. digitally watermarked policies and other ways of creating audit evidence;
- The principles of data minimisation and avoidance should be followed. No more data than necessary should be collected by the LBS providers and they should not be kept longer than necessary. It should be possible for users to be anonymous towards a third party LBS provider if the identities of the users are not needed for providing the service;
- User-related data used by different third party LBS providers should not be linkable;
- Anonymous payment services should be available.

Vision for a PRIME-based Solution

When using the travel information service, the users are regularly located for either a specific period of time or until they reach the previously announced destination. If an accident occurs or if the road conditions are poor in the whereabouts, the users are immediately notified. The users can configure their privacy settings in order to decide what kind of information is released by default to the LBS provider, as well as configuring the regularity and duration for the localisations. The users can easily stop the localisation service at any time. Furthermore, the collected location information is only used for the purpose of the service, and it is deleted immediately afterwards.

4.2.3 Friend Finder

Description of the Status Quo

In the traditional Internet, so called “buddy lists” are popular services. For example Yahoo or MSN Messenger offers people to register themselves for these services. By doing this, the users can see whether their friends are currently online, and if so, start a chat, voice or video session. Some LBS providers offer these kinds of services (commonly called “friend finders”) in the mobile world, now including the users’ physical locations as a parameter. By using a friend finder, a user can keep a list of his/her friends together with an indication where they located are at the moment. If a user sees that a friend is situated in his/her whereabouts, he/she can send a message to his/her friend to call him/her or initiate a spontaneous meeting.

If the user does not wish his/her friends to know about his/her location, he/she can turn off the possibility to be localised, and thus become “invisible”. When a user is invisible he/she cannot localise any of his/her friends. However, it is generally not possible for a user to be visible (i.e. can be localised) for some friends in his/her friend list, while being invisible for others. Either all friends can localise a user, or none of the friends can⁶.

Today, Swedish mobile operator Telia offers a LBS service called “Friend Finder” [14] which is functioning similarly to the above description of a generic friend finder service. Friend Finder is supposed to prevent the identities of the users to be connected with their actual locations through the use of “encrypted aliases” instead of identities/telephone numbers. Two more examples of companies

⁶ The underlying reason for this is the architecture of GSM. The interesting bits are the Home Location Register and the Visitor Location Register (HLR/VLR) in GSM - they store the location information of a handset (originally for routing purposes of calls). The only way to avoid being in these registers is to turn the GSM chipset of the phone off, and thus disappear from HLR / VLR.

offering friend finders are Mobiloco, which offers a friend finder service utilized by several German mobile operators and Swisscom's friend finder solution friendZone.

Other possible appearances of a person-finder LBS application may include services like:

- Child control services: Parents can subscribe to a LBS that provides them with the current location of their children and gives them alerting services, e.g. when the child enters or leaves an area that was programmed by the parents;
- Pet control service: a lost pet can be localised using a collar equipped with a GSM chipset;
- Medical special needs support services: a person with a critical medical condition or a mental disability can be supported with a mobile monitoring/localization LBS for emergency and assistance. These kinds of services could be combined with health sensors measuring heartbeat frequency, blood pressure, body temperature, etc.

Problems and Requirements

One potential problem is the low granularity of the privacy settings. The users have to allow for the possibility to be localised by all their friends in order to make it possible for one of their friends to localise them. Also, the users do not have any possibility to configure their privacy settings in such a way that they only allow for friends to localise them if the matter is very urgent.

Child localisation might provide kidnappers with the whereabouts of children, while pet control services can reveal the daily route of pet owner's dog walking as well as their absence from a property. This is particularly dangerous, as this information is long living. Your children's way to school, or your walk with your dog may remain unchanged over many years. Consequently a person obtaining an old hard disk containing these data can spare the work of physically observing their victims. Moreover a well educated selection of victims becomes possible. If unauthorised people get hold of authorised tracing devices, this linkage between location and a particular service context can leak deep insight into an individual's private life to the observers.

Another problem is that users may be unaware of the extent of lawful interception of their location and use of LBS. Depending on national law, different lawful interceptions may be provided for. As privacy is also a civil right, users should be informed that the location data collected for a service may be used by law enforcement agencies. It is also part of their civil right to use other services, that do not collect this data, or promise to delete it after a certain time. Also, users may forget or do not realise who they authorised to access their location or other data.

Table 4 below describes a number of possible privacy problems that must be considered in a PRIME-based solution.

Table 4 Problems in the Friend Finder Scenario

Problem type	Textual description	Examples
Unsolicited profiling	The long term collection of personal information with the aim of creating detailed profiles	Blackmailing of politicians, digging in the past
Unsolicited tracking	Use of information about the current movement of persons	Kidnapping, burglary
Merging data sources	The merging of data sources may intensify the problems related to profiling and tracking	Collaboration of different service providers or of service providers with network operators
Disclosure of social network	Information about social contacts is often of a private nature	Danger of interference of group with interpersonal relationships in the group

Special properties of peer to peer features	Information that is known to a group is more easily leaked to the public	Not every member of a peer group can be trusted all the time – if trust changes, the untrusted party can exploit the group trust mechanism
Extraction of sensitive information	Use of location information to extract sensitive information	People that consult medical specialists
Harassment	Potential victims of harassment could be located using LBS	Misuse of dating service, stalking
Peer pressure	The privacy decisions of individuals in a group may be biased by peer pressure	Street gang that requires their members to share location information
SPAM	Marketing information is valuable for spammers. User loses control over his/her reachability	Unsolicited email sent to persons with matching profiles

The privacy requirements are as follows:

- Reachability functionalities (e.g., see [15]) allowing the users to specify under which circumstances they are willing to be localised. Possibility to specify privacy preferences on a “per-friend” basis. In-depth control over what information are released to which friends;
- The privacy principles of data minimisation and avoidance should be followed. No more data should be collected by the LBS providers than necessary, and they should not be kept longer than necessary;
- Since a friend finder is a peer-to-peer service, the users should preferably be anonymous toward the LBS providers, or at least only pseudonyms should be linked with locations. For enforcing his/her policies, the user is provided with proof of the consent he/she gave to the LBS business partners. Proof should be supported by generating auditable data, e.g. digitally watermarked policies and other ways of creating audit evidence.

Vision for a PRIME-based Solution

In the context of telephone communications, *reachability management* [15] means that the callees (receivers of a phone call) have the possibility to specify the circumstances under which they are willing to receive a call. Then, when a caller calls a callee, he/she attaches extra information explaining the reasons for making the call. This information could include the urgency level and the subject of the phone call. This information is compared to the preferences of the callee to make a decision whether the call should be accepted or not. Further, a caller has the possibility to make an anonymous phone call, and the callee has the possibility to specify whether he/she accepts or rejects such call. If a call is rejected by a callee, it is possible to initiate a negotiation session with the caller. For example, the callee could inform the caller that he/she will not accept the call unless the caller does not reveal his/her identity.

In the context of a friend finder, reachability functionalities could be implemented that makes it possible for users not only to specify which other users can localise them, but also *under which conditions* they are willing to be localised. When the user Alice wants to localise the user Bob, she can provide additional information to Bob, specifying the reason for the localisation. As in the example with callers and callees, this information could include the urgency level and the subject for the localisation. For example, Alice could request for an urgent localisation in order to initiate a spontaneous meeting. Further, corresponding to the example above where the callees could specify whether they accepted anonymous phone calls or not, the users of a friend finder service can specify whether they accept to be localised by a user not in their friend list.

Hence, the users have full control over both which users are able to localise them and under which circumstances. At any point in time the users can alter their privacy settings. Furthermore, only other end users have the possibility to connect a user's current location to his/her real identity. LBS providers do not link users' locations to their real identities; instead they are using schemes based on pseudonyms.

4.2.4 Area Event Services

Description of the Status Quo

In Singapore, the government called the industry for collaboration in 2003 with the aim of developing a nation-wide LBS pilot supporting event- and location-triggered push services. Applications are sought in tourism, consumerism and personal navigation. Details can be found within the call for collaboration⁷.

Problems and Requirements

Push services may have access to location data, may track users and may have access to information about their interests, preferences, etc. Hence, it may be possible for them to create extensive consumer profiles. Users could be unaware of the *extent* of lawful interception of their location and use of LBS.

Depending on national law, different lawful interceptions may be provided for. As privacy is also a civil right, users should be informed that the location data collected for a service may be used by law enforcement agencies. It is also part of their civil right to use other services, that do not collect this data, or promise to delete it after a certain time.

Or they may simply forget to whom they have authorised access to location information.

Table 5 below describes a number of possible privacy problems that must be considered in a PRIME-based solution.

Table 5 Problems in the Marketing and Area Event Scenario

Problem type	Textual description	Examples
Unsolicited profiling	The long term collection of personal information with the aim of creating detailed profiles	Blackmailing of politicians, digging in the past
Unsolicited tracking	Use of information about the current movement of persons	Kidnapping, burglary
Merging data sources	The merging of data sources may intensify the problems related to profiling and tracking	Collaboration of different service providers or of service providers with network operators
Extraction of sensitive information	Use of location information to extract sensitive information	People that consult medical specialists
SPAM	Marketing information is valuable for spammers. User loses control over his/her reachability	Unsolicited email sent to persons with matching profiles

The privacy requirements are as follows:

- Transparency for users and no hidden data collection or processing;

⁷ Call for Collaboration on LBS for Singapore, February 2003, http://www.ida.gov.sg/idaweb/doc/download/I794/LBS_CFC_Public_Document-Amended.pdf

- The users must have the possibility to configure which push service providers can receive their position and context data for what purposes and under which conditions. The users must be able to specify their privacy setting on a “per service” basis;
- The users must be able to configure with a fine granularity the conditions under which they allow what kind of information about an event to be pushed to them;
- The principles of data minimization and avoidance should be followed. No more data than necessary should be collected by the LBS providers, and they should not be kept longer than necessary. It should be possible for users to be anonymous towards a third party LBS provider if the identities of the users are not needed for providing the service;
- User-related data used by different third party LBS providers should not be linkable;
- Anonymous payment services should be available.

Vision for a PRIME-based Solution

When a user is approaching a public event, he/she can receive information about such things as where to find free parking slots. When he/she enters the event area he/she receives the timetable of events on his/her mobile device. During the event he/she receives such information as event news, changes in the programme, etc. Another option is that the user is strolling through the city and accidentally passing by the event location. In this case, he/she will be informed about what is happening at the event, and possibly receive an invitation. The user can specify what kinds of events he/she is interested in so that he/she does not have to receive unwanted information.

The user can easily specify whether he/she wants his/her location to be transferred automatically to a nearby event of interest, or if the user has to initiate the exchange of information. There is transparency as the user knows exactly what kind of information the event organiser receives and what will happen to the information after the service has been carried out. The granularity of the privacy settings allows the user to specify that, for example, during the next two hours he/she is interested in receiving information about sporting events. After this period of time has passed no more location information is determined and propagated. For the cases when the user’s real identity is not required only a pseudonym is sent to the LBS providers.

4.2.5 Mobile Marketing and Couponing Services

Description of the Status Quo

Mobile marketing and couponing services target individuals and their mobile communication devices. They transport personalised advertising, offers and coupons on behalf of businesses.

Contrary to classic advertising and online marketing on the Internet, mobile marketing knows an individual’s profile as well as the location. Both data sets are used to sell marketing opportunities to businesses. The advertiser might gain a customer, or provide a service to a frequent buyer. The individual might receive a rebate, special offer or gift with the advertisement.

Several campaigns with coupons and vouchers sent by SMS (Short Message Service) to mobile phones have happened in the past. Yet, location information had to be entered by the user. Platforms for multi media advertising to mobile devices with localization and profiling are being developed, and will be ready soon [16].

Problems and Requirements

Table 6 below describes a number of possible privacy problems that must be considered in a PRIME-based solution.

Table 6 Problems in the Marketing and Couponing Services

Problem type	Textual description	Examples
Unsolicited profiling	The long term collection of personal information with the aim of creating detailed profiles	Blackmailing of politicians, digging in the past
Unsolicited tracking	Use of information about the current movement of persons	Kidnapping, burglary
Merging data sources	The merging of data sources may intensify the problems related to profiling and tracking	Collaboration of different service providers or of service providers with network operators
Extraction of sensitive information	Use of location information to extract sensitive information	People that consult medical specialists
SPAM	Marketing information is valuable for spammers. User loses control over his/her reachability	Unsolicited email sent to persons with matching profiles

The privacy requirements are as follows:

- Transparency for users and no hidden data collection or processing;
- The users must have the possibility to configure which profiling and context data for what purposes and under which conditions it is stored, and used. The users must be able to specify their privacy setting on a “per service” basis;
- The users must be able to configure with a fine granularity the conditions under which they allow what kind of information to be pushed to them; in particular, they have to be able to turn off offenders and limit the amount of information received;
- The principles of data minimisation and avoidance should be followed. No more data than necessary should be collected by the LBS providers, and they should not be kept longer than necessary. It should be possible for users to be anonymous towards a third party LBS provider if the identities of the users are not needed for providing the service;
- User-related data used by different third party LBS providers should not be linkable;
- Anonymous payment services should be available.

Vision for a PRIME-based Solution

When a user is approaching a location, he/she can receive information about rebates. When he/she enters the area he/she receives information about products and services that match his/her profile. He/she might receive coupons, invitations or advertising.

A trusted intermediary ensures that no identifying information about the user is passed on to the advertisers. Advertisers only receive information about profile matches. In return, neither the mobile operator nor the intermediary can collect information about the user’s shopping behaviour without the user’s consent.

Intermediaries cannot sell profiles with identifying information to other parties.

If a user wishes to terminate the marketing service, he/she is able to quit receiving the messages for the future.

4.2.6 E-Government: The electronic Witness

Description of the Status Quo

Mobile phones equipped with digital cameras can be used for an infrastructure that empowers citizens and authorities to prosecute felonies and crimes and collect witnesses. Many misdemeanours and light felonies lack prosecution, e.g. parking cars on bike routes. The reason is the size of the police force, and the extensive size of the areas to be policed in towns.

The electronic witness involves the citizens who suffer from or witness a misdemeanour or felony. The government authority plays the role of the LBS application provider. A digital photo, along with time stamp, location stamp and a description of the event are transmitted to the authorities over a mobile network, securing evidence and reporting the event. Time and place are being certified by the mobile network. The authorities can react upon the reporting. In our example, the offender would receive a ticket for parking on a suburban bike route where authorities rarely patrol.

In this scenario, the citizen would not enforce any law, but report to the responsible authority just as he would do with a written letter. The LBS system adds precision and real-time notification to the paper-based process. Still, the responsible authority would decide whether the offence is worth prosecution.

Such a system is not realised yet. Nevertheless, some cases of curfew violation or robbery have been investigated using bystanders' mobile phone photos that were taken to the police. Also, the story of Dutch soccer champion Kluyvert tells of new uses of public mobile camera infrastructures. He broke his team's curfew the night before a game, and was photographed by numerous visitors of a night club – which in the end led to Kluyvert being expelled from the team [17].

Problems and Requirements

Table 7 below describes a number of possible privacy problems that must be considered in a PRIME-based solution.

Table 7 Problems in the Electronic Witness Scenario

Problem type	Textual description	Examples
Unsolicited profiling	The long term collection of personal information with the aim of creating detailed profiles	Blackmailing of politicians, digging in the past
Unsolicited tracking	Use of information about the current movement of persons	Kidnapping, burglary
Merging data sources	The merging of data sources may intensify the problems related to profiling and tracking	Collaboration of different service providers or of service providers with network operators
Delinquent's privacy	Criminal records need to be protected	Prosecution shall not reveal sensitive private data about delinquents, e.g. the location of their daytime parking spot. Otherwise, they might face threats and damage
SPAM	Marketing information is valuable for spammers. User loses control over his/her reachability	Unsolicited email sent to persons with matching profiles
Witness privacy	Anonymity of witnesses is important for law enforcement and	A witness might be threatened if he/she is not anonymous

	for the users themselves to protect them from accused parties taking revenge	against the reported suspects
Claimant privacy	Informants may remain anonymous; information should not leak to suspect	Claimants whose identity gets well-known might face social repression and violence

The privacy requirements are as follows:

- Security and anonymity for witnesses' identity;
- Security and anonymity for suspects' identity against the witness and the public;
- Security and privacy for victims' identity;
- Transparency for users and no hidden data collection or processing at the mobile network and other parts of the infrastructure;
- The principles of data minimisation and avoidance should be followed. No more data than necessary should be collected by the network operators, and they should not be kept longer than necessary.;
- User-related data from subsequent uses of the electronic witness should not be linkable.

Vision for a PRIME-based Solution

Witnesses of misdemeanours can contribute to public security by (possibly under a pseudonym) transmitting evidence to authorities who can react upon the complaint by processing the evidence. Witnesses are protected within the electronic witness system with respect to their identity against possible revenge from suspects. Also, suspects' privacy must be maintained according to the legal practice. Thus, no network operator, telecommunications operator and system administrator can receive information about the witnesses' identity and other personal data. This information is only available for authorised personnel. Witnesses can also choose to report incidents anonymously.

Location and time stamps of witnesses' contributions shall only be stored for a single case, and never be linked together to profile the whereabouts of a witness in combination with his/her identity over a period of time longer than the events involved.

Besides filing claims to law enforcement, another usage area for this scenario could be assuring proofs for personal needs, e.g. for accidents, contract fulfilments or disputes. For example, a user could document the time the rental car was given back to the rental agency, the place at which a rental car was damaged, bruises from a fight caused by an attacker, etc.

4.2.7 Disaster Management with Mobile Phones

Description of the Status Quo

Location of human beings is an important information asset for a disaster manager. In the event of a disaster, localisation of mobile phones in certain areas of a town can help evacuation planning. The individuals who are closest to the danger can be informed first and selectively to avoid traffic jams and panic. Movements of mobile devices could be used to send rescue teams and police forces into an evacuated area to retrieve survivors or arrest burglars. Victims could be identified by their mobile phones.

Disaster management can collect location information and other data from mobile network operators to save lives. Individuals could also receive disaster warnings for the area they are in, for their property when they are away from home, or members of their families when in separate locations.

Disaster Managers could collect identity information for lists of missing persons or to inform relatives under certain circumstances.

Privacy and Identity Management for Europe

Early implementations of emergency call location transmission in the E911 project in the United States of America have revealed many standardisation needs for a working infrastructure. In Germany, SMS based disaster alerts have been discussed since 2001. Further, some scientific examination is in progress [18]

Problems and Requirements

Table 8 below describes a number of possible privacy problems that must be considered in a PRIME-based solution.

Table 8 Problems in the Disaster Management Scenario

Problem type	Textual description	Examples
Unsolicited profiling	The long term collection of personal information with the aim of creating detailed profiles	Blackmailing of politicians, digging in the past
Unsolicited tracking	Use of information about the current movement of persons	Kidnapping, burglary
Merging data sources	The merging of data sources may intensify the problems related to profiling and tracking	Collaboration of different service providers or of service providers with network operators
Disclosure of social network	Information about social contacts is often of a private nature	A list of close friends and private locations can be gathered by unauthorised reading the alerting configuration
Looting	Information about disaster location may lead to more efficient looting	After evacuation, a gang exploits LBS information to identify evacuated areas to loot

The privacy requirements are as follows. “User” here refers to a person being localised by the disaster manager:

- Transparency for users and no hidden data collection or processing;
- The users must have the possibility to configure who is allowed to receive disaster warnings in their whereabouts; property owners must consent in alerts generated about their property;
- Information about the users’ identity shall not be available to anyone on the disaster management system unless there is strong evidence for a crime or a very critical individual situation. All disaster services should refer to pseudonyms;
- The general observation mode shall only be available after a disaster has been declared;
- The principles of data minimisation and avoidance should be followed. No more data than necessary should be collected by the LBS providers, and they should not be kept longer than necessary. It should be possible for users to be anonymous towards a third party LBS provider if the identities of the users are not needed for providing the service;
- User-related data used by different third party LBS providers should not be linkable.

Vision for a PRIME-based Solution

A PRIME supported disaster management infrastructure with mobile phone networks manages subscriber identities. By means of anonymisation, pseudonymisation and data minimisation and based

on stringent access control and authentication, only the information necessary is revealed at any given time. The disaster status of a region triggers permissions to be granted in a particular situation.

In general, when users register other persons or locations for disaster information, no location or person shall be observed without consent. Mobile operators shall provide pseudonymisation technologies on the interfaces to the disaster management system, even though in some emergency situations, it is in the interest of the user that the disaster manager knows his/her identity, e.g. for finding and notifying his/her relatives. Furthermore, clear policies of use and guidance for users (e.g. with respect to lawful interception or the exact circumstances of disaster situations) shall be documented. Depending on national law, different lawful interceptions may be provided for. As privacy is also a civil right, users should be informed that the location data collected for a service may be used by law enforcement agencies. It is also part of their civil right to use other services, that do not collect this data, or promise to delete it after a certain time.

4.2.8 Mobile Dating

Description of the Status Quo

Mobile dating with localisation enables partner-search in the area where a person is currently in. User profiles are stored with the service, and whenever a person seeks company, the dating LBS looks for matching interest profiles in close proximity. Pseudonymous messaging services and recommendations for meeting locations as well as navigation to the location add up to a comfortable service.

Dating services extend their business from Internet desktop computers to mobile terminals. Examples are findtheone.com and match.com. Usually, they develop a mobile channel for their already existing business.

Start-up companies aiming at the mobile operator industry provide software or application services for mobile dating, e.g. Mobiloco with Vodafone in Germany or Landmat's DateTrek service enabling operators to provide mobile dating. DateTrek currently is online in Scandinavia – and surprisingly also in the Far East, where it is said to generate high profits by providing the socially discriminated gay communities with a contact channel.

Problems and Requirements

Table 9 below describes a number of possible privacy problems that must be considered in a PRIME-based solution.

Table 9 Problems in the Mobile Dating Scenario

Problem type	Textual description	Examples
Unsolicited profiling	The long term collection of personal information with the aim of creating detailed profiles	Blackmailing of politicians, digging in the past
Unsolicited tracking	Use of information about the current movement of persons	Kidnapping, burglary
Merging data sources	The merging of data sources may intensify the problems related to profiling and tracking	Collaboration of different service providers or of service providers with network operators
Disclosure of social network	Information about social contacts is often of a private nature	A dating service employee might collect and store their members' intimate relationships to blackmail

		them later
Special properties of peer to peer features	Information that is known to a group is more easily leaked to the public	A rejected lover might disclose a part of a person's network of intimate contacts
Extraction of sensitive information	Use of location information to extract sensitive information	People that consult medical specialists
Harassment	Potential victims of harassment could be located using LBS	Misuse of dating service, stalking
SPAM	Marketing information is valuable for spammers. User loses control over his/her reachability	Unsolicited email sent to persons with matching profiles

The privacy requirements are as follows:

- Transparency for users and no hidden data collection or processing;
- The users must be able to activate and deactivate the service;
- The users must be able to configure with a fine granularity the conditions under which they allow what kind of information about an event to be pushed to them;
- The users must be able to manage their identities, pseudonyms and other identifiable information, in particular their mobile phone numbers;
- The principles of data minimisation and avoidance should be followed. No more data than necessary should be collected by the LBS providers, and they should not be kept longer than necessary. It should be possible for users to be anonymous towards a third party LBS provider if the identities of the users are not needed for providing the service;
- User-related data between different third party LBS providers should not be linkable;
- Anonymous payment services should be available.

Vision for a PRIME-based Solution

Users on mobile dating services can act based on various pseudonyms. The dating agency does not get to know the users' identity. Under no circumstances, the dating service can reveal a user's identity to another user without explicit consent. Any personal data stored in profiles and preferences can only be accessed when they were classified for publication to other users of the service. Unless the users choose to use a journal of their dates, no history of user interactions should be stored on the dating system.

The interfaces to the mobile operators and towards the payment systems must support anonymity. No operator and no bank should know where, and how often, the dating service is being used by the users.

To counter harassment, pseudonyms are revocable.

4.2.9 Toll Collection

Description of the Status Quo

Toll collection systems are in use all over Europe. Toll bridges, cash- or ticket driven systems or simple toll bars are traditionally used for this purpose. Some countries introduced stamps that have to be displayed in a vehicle's window.

Recent developments target mileage based charging. Location based services using RFID or GPS technology can track a vehicle's route with high precision and generate toll bills based on the mileage, the type of road used or the kind of truck that was used for the voyage.

Privacy and Identity Management for Europe

The German company Toll Collect is currently installing a system to collect truck toll on highways. It uses GPS and mobile data connections to track routes. Other systems use cash cards that interact with radio enabled toll collecting equipment. In fact, Germany's Toll Collect was awarded with the German Big Brother Award in 2002 for its architecture that stores movements of individual trucks in a centralised database [19].

Problems and Requirements

Table 10 below describes a number of possible privacy problems that must be considered in a PRIME-based solution.

Table 10 Problems in the Toll Collection Scenario

Problem type	Textual description	Examples
Unsolicited profiling	The long term collection of personal information with the aim of creating detailed profiles	Blackmailing of politicians, digging in the past
Unsolicited tracking	Use of information about the current movement of persons	Kidnapping, burglary
Merging data sources	The merging of data sources may intensify the problems related to profiling and tracking	Collaboration of different service providers or of service providers with network operators
Extraction of sensitive information	Information about logistics may be valuable to competitors or spy on the driver's behaviour	Movement of lorry fleet, their destinations and their driver's detours to private places can be tracked

The privacy requirements are as follows:

- No other organisation than the toll collection company and the vehicle operator may have access to routes, destinations and mileage;
- No linkage between individual drivers and the data of the vehicles they drive shall be stored in toll collection systems;
- No information about the destination of freight or travel shall be known to the collection system.

Vision for a PRIME-based Solution

PRIME could provide identity management techniques to protect drivers' identities. The processing of mileage data for billing purposes is separated from the trucking company's business secrets like destinations and routes as well as the frequency of the transports.

4.3 E-Science: Review Process Scenario

Description of the Status Quo

The author delivers an article to the editors (see 1 in Figure 2) who are responsible for a formal evaluation. If the editors accept an article for publication, they forward it to the reviewers (see 2 in Figure 2) who evaluate the content. They give feedback on the text to the editors (see 3 in Figure 2) who send the reviewers' comments to the author (see 4 in Figure 2). After revising the text, he/she sends it back to the editors (see 5 in Figure 2). If they regard the article as finished, they send it to the publishers (see 6 in Figure 2) who publish the text.

Traditionally editors ensure by organisational means the author's anonymity against the reviewers and/or the reviewers' anonymity against the author. This reflects society's interest in freedom of science (cf. Art. 13 Charter of Fundamental Rights of the EU) and in freedom of speech (cf. Art. 11 Charter of Fundamental Rights of the EU) by supporting fairness in the evaluation process.

On the other hand after the reviewing process, the author normally does not want to stay anonymous any more: By using his/her name or a chosen pen-name in his publications he/she establishes a reputation, e.g., according the academic tradition.

Requirements

Table 11 below summarises important requirements that have to be fulfilled by a PRIME-based solution.

Table 11 Requirements for the E-Science Scenario

Requirement Category	Characteristics and substantiation
Usability	Goal is as much usability / ease of use as possible. An alternative and more complex user interface is acceptable for professional and well-skilled users
Security	Prevention of reputation theft and plagiarism, i.e., authenticity and in some cases also non-reputability are desired
Privacy	Anonymity of the authors and reviewers during the review process (double blind reviewing process). Anonymous publication if desired: no linkability between text and author
Law Enforcement / Liability	Digital evidence is necessary in case of plagiarism, identity theft, reputation theft, unlawful content ...

Motivation for a PRIME-based Solution

An identity management system can be used to technologically implement the tradition of anonymity in the review process and in some cases even enhance today's state-of-the-art. Figure 2 below shows two de-coupled pseudonym domains (pseudonym domain 1 and 2), which represent different stages in the review process from the author's point of view:

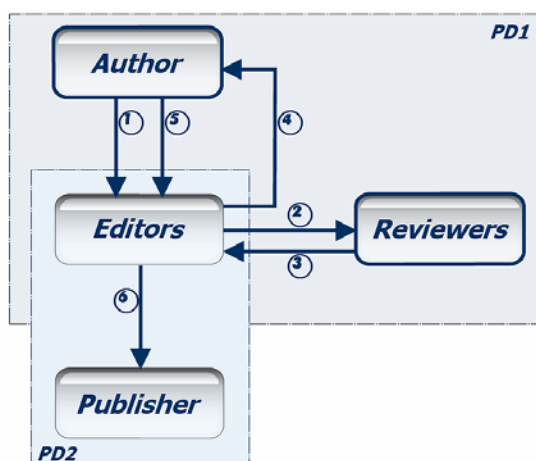


Figure 2 Domain of authors and reviewers in review scenario.

Pseudonym domain 1 describes the process of text evaluation where the author can use a pseudonym from the beginning on, i.e., delivering the text to the editors until handing over the revised version according to the reviewers' comments. Thus, he/she may stay anonymous against both reviewers and

Privacy and Identity Management for Europe

editors, if so desired. The pseudonym in pseudonym domain 1 has to be durable for the transaction until submitting the finished article, and addressable by the editors. For maximum privacy the pseudonyms should not be re-usable.

In pseudonym domain 2, the author can be known by a different pseudonym (or his/her real name) under which his/her text is published. The pseudonym in pseudonym domain 2 has to have a long durability. Re-use should be possible to establish reputation. If the possibility of discussion is desired, an addressable pseudonym should be used. If one should be able to identify the author to make him/her accountable, an addressable pseudonym that lasts over time can be taken.

The author's anonymity even against the editors may support equal treatment without distinction of person.

4.4 *E-Shopping Scenario*

Description of the Status Quo

The main actors in this scenario are the customer and the seller (e.g., in an Internet shop). The customer visits the site of the seller and inspects the offerings. When he/she has questions about a product or needs advice what to buy, he/she asks the seller using web forms, e-mail, fax or telephone. The seller usually answers the request using the medium_chosen by the customer.

After the customer has decided to purchase something in the Internet shop, he/she places an order. For this he/she can use the shop web site, e-mail, fax, telephone, mail etc. Generally, this order contains not only the declaration about the good to deliver, but also the name of the customer and address information. The customer usually needs to give_the seller also his/her credit card number_or state that he pays in advance by bank transfer or check.

The customer may submit special sub-attributes like, e.g., vouchers, trading stamps or his/her customer ID for special discounts; the seller may also ask for an age verification etc. in particular situations.

Both the seller and the buyer are interested in the other party fulfilling its obligations, i.e., that the seller sends the ordered goods and the buyer pays the price as agreed. If there were business connections before, the gained reputation influences the current transaction. The seller's reputation is also influenced by a professional and respectable appearance or other peoples' experiences. If the seller does not trust in the buyer's solvency or payment pattern, he/she can ask for an advance payment or the buyer's bank account data for a direct debiting. On the other hand, the buyer can ask for an advance delivery of the products.

Either the buyer asks his/her bank to transfer the purchase price to the seller's account. Or he/she uses his/her credit card. If he/she uses his/her credit card, he/she gives his/her credit card number, the valid date and name to the seller (see 1 in Figure 3). The seller asks the credit card company to remit the money (see 2 in Figure 3) and the company will do so if the data check yields positive results (see 3 in Figure 3). Normally at the end of a month the credit card company charges the customer (see 4 in Figure 3), and the customer transfers the money to the credit card company (see 5 in Figure 3) or grants the permit to debit it directly from his/her bank account.

A system that works with pseudonymity and separates different duties within the e-shopping process is the SET (Secure Electronic Transaction) protocol, proposed by Visa and MasterCard a few years ago. It enables a three-party transaction between sellers, buyers, and banks / credit card processors ("acquirer") on the Internet using a SET Payment Gateway. The SET protocol includes a transaction identifier that should insulate the parties: the seller is unaware of the buyer's credit card number and the bank is unaware of the goods. Most of the SET services use a back channel where the payment gateway notifies the seller for every payment about the name and the account information of the buyer. The seller needs this data to get to know if the payment was successful or if he/she has to contact the customer directly. Examples of other e-payment systems are eCash (using anonymous "electronic coins"), S-ITT / PAGO (using trustees) or PaysafeCard (a one-time smart card).

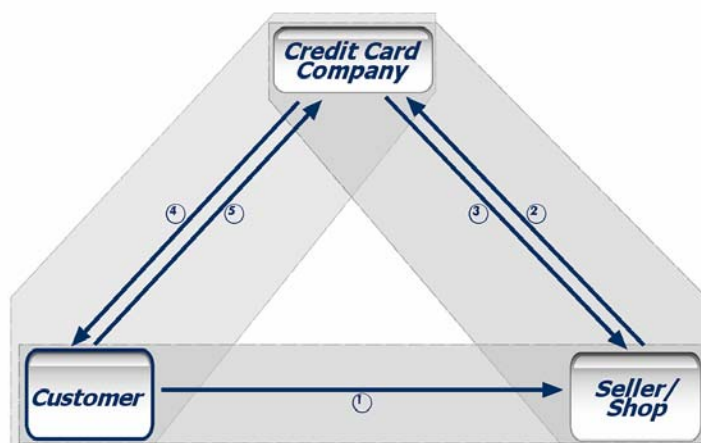


Figure 3 E-Shopping Scenario and Paying with a Credit Card.

In return for the bank transfer or the usage of the credit card, the seller ships the goods. With digital products, this can be achieved directly, e.g., by enabling a download. With respect to non-digital products, there is a need of physical delivery by a transport company, such as post, UPS (United Parcel Service), etc.

The delivery finally takes place at the buyer's place or at a pickup point (e.g., “poste restante”, neighbours, gas station, etc.) where the buyer picks up the goods after identity verification.

The currently most popular way of ordering or buying products is the enabling of the shipment by giving the customer's name and address. Often, credit card payments are the only supported payment method.

Problems and Requirements

In the current situation, data about the customer’s shopping habits and interests are exposed at the seller’s and at the credit card company’s site. This information could be stored and used for extensive consumer profiling, which could possibly be shared with other sites. For payment, the customer usually has to give his/her credit card number, leading to the risk that the merchant charges more money on it than the customer is willing to pay. Whenever the customer needs to provide some form of assertion or authorisation or certificate, he/she has to send a copy by mail, fax it or present it physically, which is cumbersome. The degree of anonymity is very low, especially with assertions, authorisations or certificates.

The requirements in Table 12 below should be addressed by a PRIME-based solution for E-commerce applications:

Table 12 Requirements for the E-Shopping Scenario

Requirement Category	Characteristics and substantiation
Usability	Easy to use because it should be used by all ordinary customers
Security	Prevention of identity theft and misuse of, e.g., credit card numbers; non-repudiation of the user; prevention of accidentally false addressing
Privacy	Prevention of profiling, anonymity of the customer, linkage of data only where necessary (i.e., if possible separate processes of browsing, of seeking for advice, of choosing the product, of payment, and of delivery, meaning that different pseudonyms can be used)
Law	Digital evidence necessary in case of identity theft, reputation theft,

Enforcement / Liability	warranty (e.g., receipt), wrong delivery, ... At the user's side: logging of legal acts, storage of contracts / general terms and conditions
-------------------------	---

Motivation for a PRIME-based Solution

The identity management system can be deployed for the technical guarantee of the buyer's anonymity. This can be desired to avoid the creation of a profile and therefore linkability of the purchase of sensitive products, or to enable an independent consultation, or to prevent an undesired mailing of promotional material.

In order to achieve this kind of data minimisation as a PRIME-based solution, the customer can act under different pseudonyms. The customer may already use a pseudonym in the consultation phase, which cannot be traced back to him/her (pseudonym domain 1 in Figure 4). This pseudonym is only valid during this consultation phase and is addressable by the seller or advisor. For the actual purchase, a different pseudonym can be used that cannot be related to the consultation pseudonym (pseudonym domain 2 in Figure 4). This pseudonym can be linked to a certain reputation or payment guarantee provided by a third party to ensure the seller that the payment will be made. Alternatively, a special, individual pseudonym might be assigned to be used for each seller. This pseudonym can be used every time the buyer gets in contact with the specific seller, in order to build up the reputation of a regular customer and at the same time to avoid a linkage of the customer's data with those data of the customer collected by other sellers. The second pseudonym should have a long durability; its re-use should be possible to establish reputation. Moreover, it should be addressable if the customer wants to get further information from the seller.

If a customer wants to profit from a warranty given by the seller for a bought merchandise, the customer needs to make a warranty claim to the seller and identify the buying transaction to the seller so the latter can judge if the warranty claim is justified or not. However, the customer does not necessarily need to provide his/her identity or even the pseudonym used for the purchase, *if* the transaction can be identified by itself, e.g., through a (digitally signed) transaction number or electronic warranty slip number or bill number. Even for issuing bills or invoices in tax declarations, personal data of the customer on the receipt itself is not necessary.

For recalls of the bought product, e.g., for security reasons, addressable pseudonyms could be useful, so that the customer can be informed about the problem with his/her product. However, when customer data are not being stored (as in many cases nowadays), recalls can be done by broadcast announcement, e.g., in newspapers or on TV.

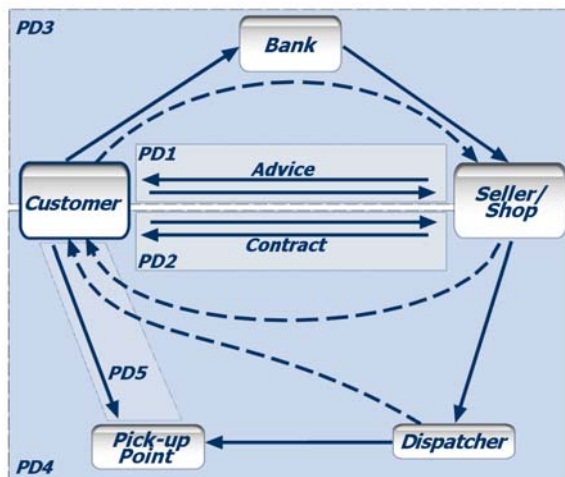


Figure 4 Pseudonym Domains of a Customer in an E-Shopping Scenario.

Furthermore, the issuing of reputation credentials by different sellers could be useful for building a reputation. Such a reputation could serve as a basis for a trustworthy third party that guarantees the payment for the purchase up to a certain sum (e.g. a bank – cf. pseudonym domain 3 in Figure 4). Such a trusted third party (a so-called value broker) would need to be directly involved in the ordering and payment procedures as a broker who assures the seller that he/she will receive his/her money while keeping the real identity of the buyer secret. Additionally a value broker can take care for the synchronous exchange of money and goods. However, it is not mandatory to take use of a third party. It is also possible for the customer to pay directly e.g. by sending cash money or using a prepaid account of the seller (cf. dashed line in pseudonym domain 3 in Figure 4).

If physical goods are to be shipped (rather than goods delivered online – cf. dashed line from seller to customer in pseudonym domain 4 in Figure 4), delivery can take place by using a trusted delivery broker / a dispatcher, to whom the seller sends the goods to and who forwards them to the buyer. Thereby, seller and dispatcher use a separate pseudonym for the buyer, known to the seller and dispatcher only i.e. hidden to the banks of the customer and seller respectively (pseudonym domain 4 in Figure 4). Moreover, the physical address of the customer is only known to the dispatcher, not to the seller. The dispatcher knows the address of the recipient but not what he/she handles. The seller knows the sold object but not who is the real recipient (cf. dashed line from dispatcher to customer in pseudonym domain 4 in Figure 4). Or, in order not to force the customer to disclose his/her physical address at all, a pick-up point can be used where the dispatcher sends the goods to and where customers go to in order to pick up the goods. This kind of delivery as well can be carried out with the customer only using a pseudonym (cf. pseudonym domain 5 in Figure 4). At the pick-up point, the customer is authenticated as the owner of the pseudonym, e.g., by presenting a password transmitted to him/her from the seller when concluding the online order, and transmitted at the same time to the dispatcher or directly to the pick-up point.

The Identity Management System takes on the function of dealing with various institutions in a secure, simple and privacy-compliant way. In addition to the task to achieve unlinkability between different actions in the e-shopping scenario, the Identity Management System could help the customer in administrating the various contacts, e.g., by providing address book functionality, and transactions, e.g., by storing contractual information of the purchases.

Further on, a shopping tool provider / offer broker collecting offers at various sellers on behalf of the customer and presenting the customer a list of offers could use pseudonyms and thereby hide the customer's identity to the various sellers. This is both economically rational and positive for data protection, because this would not include any complete or central storage of all transactions (provided no third party instance is needed for every transaction).

One solution of a PET-enabled e-service under development is the idemix system by IBM Zurich Research Laboratory in Rüschlikon, Switzerland⁸ which is being integrated in the IDM prototype DRIM by TU Dresden and will be one component of a PRIME prototype. Idemix (identity mixer) is an anonymous credential and pseudonym system, which keeps the amount of data revealed to a minimum. It supports full pseudonymity and one-time assertions for pseudonyms from third parties. Using idemix a user would first select a pseudonym, then register using this pseudonym and receive the corresponding credentials with an electronic signature. If later on the user wants to access the service, he/she only must first provide proof to the service that the corresponding, digitally signed credentials are in his/her possession. Pseudonym and credentials are given to the on-line service in encrypted form. Although the on-line service cannot decrypt the information, it can still employ an interaction method with the user to verify the authenticity of the encrypted pseudonym and that the digitally signed credential owned by the customer is correct.

In an equally secure manner the user can supply credentials received from another organisation to the on-line service. E.g. a car rental agency could in this way receive proof of possession of a valid driver's license from the authorities, and of a valid credit card from a bank. A user can in principle present his/her credentials any number of times in this way. Because the encryption is changed for every use of the credential, the repeated use is hidden from the on-line service, i.e., the user is not re-

⁸ C.f. <http://www.zurich.ibm.com/security/idemix/>.

Privacy and Identity Management for Europe

identified and thus can act anonymously. If e.g. a rented car is not returned, the identity of the person who rented the car has to be retrievable. Therefore, the idemix system also allows a designated authority who can uncover such an identity. In the case of a driving license, it could for example be the office that issued the license; in a business context it could be a third party trusted by both business partners.

Other possible scenarios for idemix are, e.g., handling of insurance contracts or air line travel.

4.5 Task Assignment Scenario

In some cases, it may make sense for an organisation's internal identity management system to support pseudonyms or anonymous communications or actions. One basic scenario is the ordinary process of assigning tasks in an organisation without giving the staff the real name of the requesting person. While at first glance this seems to be a sophisticated undertaking, it is sometimes common not to give the real name to the staff if, e.g., a medical lab performs an examination by order of a doctor or if an academic text is passed to reviewers for being evaluated. This internal pseudonymisation in an organisation does not only realise privacy and security principles like restricting the access to information only to authorised people ("need-to-know principle"), but also aims for a fair and equal treatment of requesting persons without special conditions, risk of loss of privileges or discrimination.

Description of the Status Quo

In a typical workflow, a client is requesting an organisation (e.g., a sales company or a local authority in an e-government application) to perform a task. The organisation employs several staff persons (officials or clerks) in charge to whom those requests could be assigned by the organisation office according to a certain distribution key. The first contact of the client is made under an address to which the response will be sent later on. For performing the given task, the job is completely with all (personal) data forwarded to a staff person. Sometimes internal reference numbers are used instead of the real name. After having carried out the task, the staff person reports the result to the office which may take further steps and eventually send a response to the client.

Problems and Requirements

A major problem is that the organisation office is a single point of trust and potential failure. It gets all client requests and can compile profiles of the clients' request behaviour. If the organisation office service is down, the organisation will be unable to perform tasks for their clients. It has to be trusted to do a correct and reliable re-pseudonymisation.

Table 13 below lists specific requirements that have to be fulfilled by a PRIME-based solution in this area.

Table 13 Requirements for the Processing of Orders Scenario

Requirement Category	Characteristics and substantiation
Usability	Easy to use by ordinary clients
Security	Reliable forwarding of task assignments and responses by the organisation office, availability of the organisation office's forwarding service
Privacy	Anonymity or pseudonymity for clients, prevention of profiling by the organisation
Law Enforcement / Liability	Possibly requirement of linkability in the organisation office

Motivation for a PRIME-based solution

Figure 5 illustrates the workflow of a client requesting an organisation to perform tasks in a privacy-enhanced identity management system. Pseudonym domain 1 exists between the client and the organisation office. If it is an order relationship that is based on the possibility of a repetition, both parties may be interested in the possibility to use the same pseudonym more than once, e.g., for building up a certain reputation, for reconsiderations and checks or for offering client-related benefits. If this is not desired, the client can use a new pseudonym for each order. This pseudonym is only valid and can be addressed by the organisation until the order has been finished.

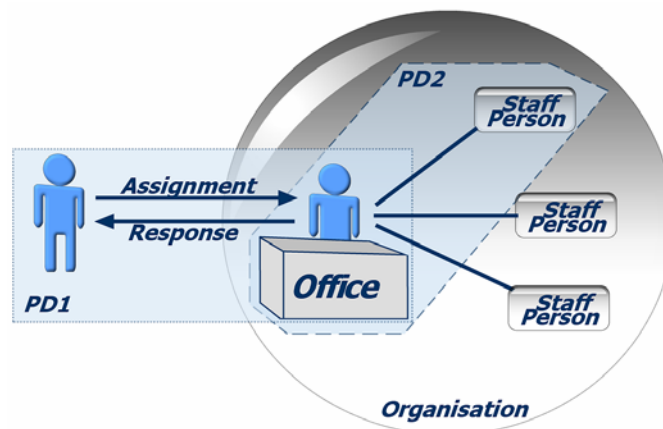


Figure 5 Pseudonym Domains in Assignment of Tasks.

Pseudonym domain 2 comprises the organisation office and its employees. In order to guarantee the independence of the judgement of the person in charge, this pseudonym can be de-coupled from pseudonym domain 1. The people in charge are then not able to access any client data other than those transferred.

The organisation office provides a reliable re-pseudonymisation, i.e. the translation between both pseudonyms has to work properly so that the result elaborated by the staff person really reaches the right requesting person. The office as both separating and linking instance is very important in this scenario, acting as an Identity Protector. The internal use of a pseudonym (e.g., a reference number) is not necessarily known to nor can it be influenced by the client.

However, in some cases anonymising the request makes no sense, e.g., when personal data is directly bound to the request and cannot be stripped off without losing information.

4.6 Ambient Intelligence Scenario

Description of the Status Quo

The vision of Ambient Intelligence is that the computer as we know it has "disappeared" and has been integrated into the environment of the user. Instead of data being input via a keyboard and mouse, it enters the system via sensors in the user's environment. These sensors can often collect information which the user is not aware of, via for example passive RFID Tags (which return unique numbers when interrogated by a reader), pressure sensors, gesture recognition in clothes etc ... The services are then delivered by actuators which are also integrated into the environment. These may be anything from a lock on a food cabinet, to a lighting level controller or an element in a supply chain application which alters delivery amounts based on the contents of a smart fridge. The system is able to communicate back to the user through very diverse means, from speech synthesis and display devices to vibration. All sensors and actuators are integrated seamlessly into a system which may span a user's home, work and public spaces.

Specific example: Pressure sensors and RFID tags

A type of pressure sensor is embedded in flooring systems and at regular intervals or when significant changes of values occur, it returns tuples of:

- An unstructured pseudonym which is unique to each sensor e.g. B1HA006. These pseudonyms act as keys in a database which link to the location of the sensor;
- The pressure currently registered;
- A timestamp.

For example it might return <B1F78A, 10000 N/m², 1999-12-31 23:59:59> when someone weighing 100kg stands on it.

This type of sensor becomes an industry standard and is ubiquitous in flooring systems used in business, domestic and commercial context. The pressure sensor might be used for example to adjust music in a discotheque based on the level of activity or to detect when a person is standing in front of a certain product in a supermarket.

Suppose a customer of a certain supermarket chain buys a pair of shoes with an RFID tag embedded in each shoe. These RFID tags allow customers to pay for their shopping without the need for checkout staff, simply by pushing their shopping cart past an RFID reader and swiping a credit card (or even just having an RFID enabled electronic wallet in their pocket).

The supermarket takes privacy seriously, however and so the naming system of this RFID tag is linked not to individual products but to product batches (i.e. sets of perhaps 1000 products all produced on a certain day in a certain factory). There is also no link created between the Electronic Product Code (EPC – the number returned by RFID's when queried by a reader) and any customer's purchase details.

Nevertheless, suppose that a single organisation has access to all values returned by such pressure sensors and RFID readers. This would usually be a law enforcement agency. If blanket data-collection practices such as Total Information Awareness (TIA) are put in place by anti-terrorism lobbies it is easy to imagine that such data could be in the possession of a single law enforcement authority. However, it may occur as a value-added service if the vendor of the pressure sensor were also to offer to store and analyse the data from the sensors on behalf of the buyer, as an value-added service.

The vendor might then for example sell a set of 20 pressure sensors, and a data collection and analysis service, which combines their data with product RFID data, ostensive for advertising products to customers when they are standing at certain places in the supermarket. If the same company also has access to data from pressure and RFID sensors in domestic environments, they would be in a position to process and sell analysis of address and other personal information about customers.

So it can be seen that, depending on the ubiquity of the sensors and the ability of single entities to cross-reference databases, a sensor vendor may be able to track the movements of individual customers between their homes, offices and shopping locations by correlating:

- The locations of RFID readers;
- The values returned by pressure sensors (one can assume that weights of customers buying shoes *within a certain batch* will be unique);
- Locations linked to weight sensors.

An application could even deduce the address of customers buying various products. Such a system may also, for example, log a user's movements around a supermarket and make product suggestions based on his/her previous purchases. It is also theoretically capable of making similar suggestions within the customer's own home, car or even in public places.

Specific Components

Actors:

- Service requesters - the individuals buying shoes and interacting with pressure sensors;
- Data controllers - the legal persons responsible for collection of data. In this case these could include:
 - The supermarket;
 - The advertisers;
 - Any parties using pressure sensors in their applications;
 - The company producing the weight sensors who might manage a central database for customers using the sensors so that the sensors provide a complete service and do not require data to be stored separately.
- Attackers – illegitimate actors in such a scenario could use the infrastructure in place to collect Personal Identifiable Information (PII) about individuals using the systems.

Technical components:

- Pseudonyms - RFID numbers, real names of individuals, product names associated with the individual, etc;
- Sensors - RFID readers, pressure sensors returning location and time stamps;
- Actuators - channels for product suggestions (e.g. audio advertisements from loudspeakers in supermarket aisles).

Problems and Requirements

Key threats in such scenarios are:

- Data is collected without the subject's knowledge;
- The increase in the ability to profile and track individuals based on highly incidental information;
- Boundaries of control become blurred and it becomes very difficult to define who is responsible for a given data collection act;
- Users no longer have true freedom of choice because they are forced to participate in Ambient Services in order to carry out their every day activities;
- Users' "spatial privacy" is much more under threat. That is the system is able to communicate back to the user in ways which are much more invasive of the user's control of the information entering his/her personal sensory space.

This creates the following specific functional requirements:

- **Transparent disclosure:** It is impossible in such scenarios for users to keep track of all the data collection events taking place around him and the consequences of each one. However, an electronic agent acting for the user should be aware of the information being collected about its owner and able to warn the user of any events which conflict with his/her previously stated preferences for data collection or usage;
- **Minimisation of cross-referencing (related to inference control):** Access control systems and application architectures have some understanding of which combinations of data may compromise anonymity when combined in certain configurations;
- **Freedom from conditions on informational self-determination:** The user is able to make free decisions about whether to enter into data collection scenarios i.e. without being forced to

trade his/her personal information for authorisation to carry out daily necessities such as travel, shopping, etc.;

- **Clear lines of responsibility:** The areas of responsibility of data collection acts are clearly defined. This allows a system to better track profiling, data collection and access by each controller (one controller should be responsible for each data collection activity). It also gives clear lines of legal recourse for end-users;
- **Collection Minimisation:** Access control systems should be set up to ensure that collection and combination is minimised to the amount necessary to carry out the service and that information is available to access control systems on how to make this a well-defined property. This should be achieved not only by examining declared practices but by examination and enforcement of actual activities;
- **Secure communication:** Even if all legitimate actors in this scenario transparently disclose data collection acts as above, the field is wide open for the use of e.g. RFID and sensor values by illegitimate and/or malicious actors to gather and misuse such information. In order to mitigate such a possibility, it is therefore necessary to authenticate legitimate actors and to secure end-to-end communication between them.

Vision for a PRIME-based solution

To generate a technical framework capable of providing the amount of privacy desired by the users in ambient intelligence scenarios, PRIME solutions would ideally include:

- **Semantics** for provision of information about data collection activities including but not limited to data types, entities having access to data collections, lines of responsibility and primary and secondary purposes.

Because of the very dynamic nature of ambient intelligence data collection contexts and the high potential for combining incidental data, applications should be able to provide machine readable descriptions of data protection contexts, which may be used to make intelligent automated decisions based on machine readable preferences and descriptions of privacy and IDM events and practices. This semantic framework can be used both by user-agents, access control engines, and audit and assurance engines.

For example, in the above scenario, semantic infrastructure should be in place for a user's electronic agent to detect RFID's and pressure sensors, to understand their purposes and any potential secondary usage of information collected, and thus to be able to deduce potential threats from the privacy knowledge published (probably wirelessly) in a given context. Similarly, users should be able to release privacy policies which are capable of being understood and respected by service providers. Service providers should be able to understand policies beyond simple string matching.

Semantics and reasoning engines should be flexible enough to match concepts rather than merely strings. For example a system should be able to deduce that a rule stating that data should not be used for marketing purposes, also intends that it should not be used for telephone-marketing, etc. (i.e. conceptual matching techniques should be used rather than simple string matching).

Semantics should also be capable of providing background knowledge such as legal and technical information required for decision making (e.g. the jurisdiction in which then data will be processed, the location of secondary use policies, the transitivity of policies etc...). In order to achieve this, it should be capable of drawing on multiple heterogeneous knowledge sources and orchestrating knowledge sources in order to provide maximum information, as in the web services paradigm;

- **Contextual analysis** of data processing policies for informing and protecting end-users and for providing anonymised access control mechanisms. PRIME systems should be capable of

understanding contextual information, such as jurisdiction, legal background, special privileges for law enforcement, etc.;

- **Basic inference control** as access control systems should be designed to enable deduction of threats from inference. Inference control does not have a specific work package in PRIME, but PRIME systems working in a pervasive computing context must be designed to control risks of the kind described above, which are a simple form of inference threat. In terms of the above scenario, PRIME systems, should be able to control access to data so that the same entity may not have access to for example RFID reader data for shoes and weight sensor information unless it can prove that it needs it for a legitimate purpose;
- **Enforcement and accountability systems** for declared data collection policies. Examples of relevant technologies include sticky policies⁹, audit and assurance methods;
- **Secure end-to-end wireless and wired communications.** Technologies exist for minimising tracking in such systems. For example RFID response values may be secured from tracking by unauthorised entities by hashing them with a random number which is also returned with the RFID value. This is a technique developed by Massachusetts Institute of Technology (MIT) scientists, whereby the RFID returns a tuple of <random number, hash of EPC concatenated with random number (also random)>. Then, as hashing is a one way function, you need to have a database of the EPC numbers in your domain to be able to deduce the EPC. This is done by computing the hash of the random number and EPC numbers of all entries in the EPC number database and comparing the results with the hash returned by the RFID;
- **Advanced Human-Computer Interaction (HCI) systems** capable of warning users of risks (or opportunities) in such scenarios. Interfaces need to be designed in order to capture user preferences and for implementing semantics in policy descriptions for service providers.

AMI presents particular challenges because of the explosion of devices which cannot all be described. The need for metaphors capable of capturing a context and a user's reaction to it becomes greater than in traditional scenarios.

The technicalities of inference are also impossible to describe to the lay person and higher level metaphors would be needed.

If AMI applications are to be accepted, the perception of ubiquitous sensor environments as a spying and surveillance apparatus a la Big Brother needs to be addressed.

Practically speaking, user interfaces could be achieved through explicit policy editing interfaces, or alternatively through inline preference induction engines which are able to deduce user preferences from their behaviour (e.g. detecting which parts of his/her identity a user habitually reveals in which contexts and extrapolating preference rules from this). AMI environments allow the possibility of multi-modal (e.g. haptic) interfaces so this should be taken into account in designing interfaces;

- **Protection of personal information space** as users should be given control of what enters his/her personal informational space based on the ambient information collected about them.

Personal space in this context is not yet a well-defined notion legally speaking (it is hoped that PRIME will shed some light on this). Clearly however, every person should have certain rights over what is presented to their senses.

For example if a satellite TV company were to install a TV which cannot be switched off and which plays non-stop advertising in a person's home, this would be considered a definite violation of personal informational space, even though there would be no physical violation. More contentious issues concern advertising in more public places. For example, should it be considered a violation of personal informational space to put TV's with advertising on them in queues for essential services such as benefits, or healthcare?

⁹ A "sticky policy" is a policy that is stored together with the data and travels with the data it relates to.

Another example which is already happening is the use of television screens to advertise to "captive audiences" in hospital beds. The other end of the spectrum would be if a person enters someone else's home, they clearly have no right for example to claim that music or advertising should not be played if it is chosen by the owner of the home.

This links to the control of personal information where personal space is being invaded with content which has been tailored to target a given person, using previously collected personal information.

It is an important question whether the scope of PRIME is to cover privacy in the sense of control of personal information becoming known to (and used by) unwanted parties (informational privacy) – or

Privacy in the sense of shelter from unwanted information (spatial privacy) or in this case, policies and intelligent filtering mechanisms developed by PRIME would include filters for incoming information.

A third alternative is to cover privacy in the sense of shelter solely from information which is based on the collection of personal information. One example is invasive advertising based on personal profiling.

Systems controlling such events would need to be placed at the control layer of any actuator systems within the environment (e.g. audio streams, tactile feedback, etc) and in sensitive information streams (in the same way as current spam filters operate);

- **Proactive anonymisation techniques:** Given the passive nature of data collection activities in ambient scenarios, users may need to have proactive means at their disposal for anonymising their activities in a given scenario, e.g. RFID detection and even jamming, "killing" and disabling mechanisms.

Systems should be developed to maximise anonymity in authorisation systems. This would build on the anonymous credentials research to provide systems for service authorisation based on a minimal identity required, rather than on unique key based identification.

5 Environment

The privacy space addressed in the PRIME framework encompasses the current European regulatory framework, social environment, business environment, and technological capabilities. We describe in this section some of the privacy issues from a multi-disciplinary perspective, and the research challenges it presents. The PRIME framework addresses how we intent to tackle these challenges in an integrated manner.

5.1 *The Legal and Regulatory Framework for PRIME*

From a legal perspective, the rules with regard to privacy and identity management are mainly laid down in Article F of the Treaty of the European Union, Article 7 of the European Charter of Fundamental Rights, Article 8 of the European Convention on Human Rights, the European Directive 95/46/EC¹⁰ and the European Directive 2002/58/EC¹¹. The principles of these texts have been further refined and explained in numerous other documents, e.g. the Opinions and Recommendations adopted by the “Article 29 Working Party”¹². Besides, self-regulatory initiatives have been developed, such as codes of conduct, industry guidelines and seal programs.

5.1.1 Privacy as a Fundamental Human Right

The right to privacy protection is considered as a core value of a democratic society. It is recognised as a fundamental right in all major international treaties and agreements on human rights and in the constitutions of most countries in the world, either explicitly or implicitly.

In Europe, the fundamental right to respect for privacy is recognised, among other texts, in Article 8 of the European Convention of Human Rights and Fundamental Freedoms which states that everyone has the right to respect for his/her private and family life, his/her home and his/her correspondence. The EU Charter of Fundamental Rights of 7 December 2000 confirms in Art. 8 that everyone has the right to the protection of personal data and that such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law.

5.1.2 The European Data Protection Directive

Directive 95/46 of 24 October 1995 aims at promoting the free movement of personal data within the European Union, providing for a high level of protection of the fundamental rights and freedoms of the individuals with regard to the processing of personal data in all the Member States of the European Union and, in particular, of the right to privacy.

This Directive has a very broad scope. For example, the concept of “personal data”, applies not only as well to text as to sound and image data but, more generally, all information relating to an identified or identifiable person is considered as personal data. “Identifiable” is every “person who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his/her physical, mental, economic, cultural or social identity”. Information

¹⁰ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L No. 281, 23.11.1995, p. 31.

¹¹ Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, Official Journal L No. 201, 31.07.2002, p. 37.

¹² The Working Party is instituted by Article 29 of the Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data, OJ L 281, 23.11.1995, p. 31. The Working Party examines questions related to the application of the Directive and advises the European Commission. The Working Party documents are available at: http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs

relating to a person is consequently considered as personal data as soon as it is possible for somebody, using reasonable means, to identify the person to whom the information refers. The term “processing” has an equally wide definition for it includes any activity that someone can perform on personal data. The Directive is applicable where the equipment for processing the personal data is located on the territory of the European Community.

Article 6 of the Directive enumerates some important principles relating to data quality. Firstly, any processing of personal data should be carried out in a fair and lawful way with respect to the data subjects. Secondly, personal data must be collected for specified, explicit and legitimate purposes and may not be further processed in a way incompatible with those purposes. The purpose of the processing should thus be defined at the moment of the collection and the purposes of further processing should not be incompatible with the purposes initially defined. The third principle of Article 6 of the European Directive is that data should be adequate, relevant and not excessive in relation to the purposes for which they are collected and further processed. Data should further be accurate and, where necessary, kept up to date. The last principle refers to the delay of storage of data and sets out that data may not be kept in a form permitting identification of data subjects for longer than is necessary for the purposes for which the data were collected or for which they are further processed.

The European Directive explicitly lists the cases in which personal data may be processed. This means that for each processing of personal data - collection, recording, storage, adaptation, alteration, retrieval, consultation, disclosure, dissemination, etc. - the controller has to verify if the processing falls under one of the criteria for making data processing legitimate. Pursuant to Article 2(d) of the Directive, a controller is the natural or legal person, public authority, agency or any other body which (alone or jointly with others) determines the purposes and means of the processing of personal data. In other words, the controller is the person responsible for the processing of personal data.

The first case in which processing of personal data can be considered as legitimate is when the data subject has unambiguously given his/her consent. The “data subject’s consent” is defined as any freely given specific and informed indication by which the data subject signifies his/her agreement to personal data relating to him/her being processed. The processing is equally legitimate when it is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject for entering into a contract. The processing is in the third place authorised when it is necessary for compliance with an obligation to which the controller is subject. In the fourth place, processing of personal data is legitimate when necessary to protect the vital interest of the data subject. Finally, processing personal data is legitimate when it is necessary for purposes of the legitimate interests pursued by the controller or by a third party or parties to whom the data are disclosed, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject.

According to Article 8 of the Directive, Member States have to prohibit the processing of “personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data that concern health or sex life”. Member States may lay down exemptions to this prohibition, for example for processing of personal data with the consent of the data subject or for reasons of substantial public interest. According to Article 8, paragraph 7, Member States have to determine the conditions under which a national identification number or any other identifier or general application may be processed.

Article 10 provides that, as a general rule, the identity of the controller and the purposes of the processing should always be communicated to the data subject.

Where the information was not obtained directly from the data subject, Article 11 of the Directive establishes that the information should be provided at the time of the recording of personal data or if a disclosure to a third party is envisaged, no later than the time when the data are first disclosed.

Last but not least Article 12 grants the data subject a right to ask for the rectification, erasure or blocking of data the processing of which does not comply with the provisions of the Directive, in particular because of the incomplete or inaccurate nature of the data.

Privacy and Identity Management for Europe

According to Article 14 of the Directive, Member States should grant the data subject the right to object, on compelling legitimate grounds relating to his/her particular situation, to the processing of data relating to him.

The Directive further contains an obligation to notify the purpose of the processing to a supervisory authority. The obligation to notify does not refer to individual processing operations but to the purposes for which one or several processing operations are performed.

The Directive contains extensive regulation concerning transfer of personal data to countries outside the European Union. Such a transfer is only allowed if the third country in question ensures an adequate level of protection.

5.1.3 Directive on Privacy and Electronic Communications

Directive 2002/58/EC particularises and complements the principles of the Directive 95/46/EC into specific rules for the electronic communications sector. Its provisions apply to the processing of personal data in connection with the provision of publicly available electronic communications services in public communication networks in the Community.

According to the Directive, providers of publicly available electronic communications services must take appropriate technical and organisational measures to safeguard security of their services, if necessary in conjunction with the providers of the public communications networks with respect to network security. Having regard to the state of the art and the cost of their implementation, these measures have to ensure a level of security appropriate to the risk presented.

The E-Communications Privacy Directive further aims to protect the confidentiality of the communications. Member States have to prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned and except when legally authorised to do so. Legal authorisation for the monitoring of electronic communications is possible when it constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security, defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the communications system.

To this end Member States may adopt legislative measures providing for the retention of data for a limited period. Data retention for state security or law enforcement purposes is an exception to the general rule of Article 6 which stipulates that traffic data relating to subscribers and users processed and stored by the provider of a public communications network or publicly available electronic communications service must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication. Traffic data necessary for the purposes of subscriber billing and interconnection payments may be processed but such processing is permissible only up to the end of the period during which the bill may lawfully be challenged or payment pursued.

Another important provision of the Directive requires Member States to ensure that the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information and is offered the right to refuse such processing by the data controller. This rule should protect users and subscribers against cookies, spyware, web-bugs and other hidden intrusions of service providers on the users' personal computers, mobile phones and other personal devices.

Particularly relevant for the mobile communications sector are the rules of the Directive concerning location data. Where location data can be processed, such data may only be processed when they are made anonymous, or with the consent of the users or subscribers to the extent and for the duration necessary for the provision of a value added service. The service provider must inform the users or subscribers, prior to obtaining their consent and give them the possibility to withdraw their consent for the processing of location data at any time. Moreover, where consent of the users or subscribers has been obtained for the processing of location data, the user or subscriber must continue to have the

Privacy and Identity Management for Europe

possibility, using a simple means and free of charge, of temporarily refusing the processing of such data for each connection to the network or for each transmission of a communication.

In the context of identity management, it is further necessary to mention the provisions of the Directive related to subscribers' directories. Subscribers should have the opportunity to determine whether their personal data are included in a public directory. Not being included in a public subscriber directory, verifying, correcting or withdrawing personal data from it has to be free of charge.

Particularly relevant is Article 14, paragraph 3, underlining that where required, measures may be adopted to ensure that terminal equipment is constructed in a way that is compatible with the right of users to protect and control the use of their personal data. Recital 30 states that systems for the provision of electronic communications networks and services should be designed to limit the amount of personal data necessary to a strict minimum.

5.1.4 Requirements Imposed on Data Controllers by the Directive 95/46/EC

1. The data minimisation principle

It should be emphasised that all collecting of personal data must take place in accordance with the basic principles following from the two European data protection directives. In particular, personal data may be collected only as far as it is necessary in order to achieve the specified purpose and processed only in so far as it is legitimate on the basis of one of the criteria enumerated in Article 7 of the Directive 95/46/EC (e.g. the data subject has given his/her unambiguous consent or the processing is necessary for the performance of a contract to which he or she is a party). In particular, the finality principle requires that, without a legitimate reason, personal data may not be used and the individual concerned must remain anonymous (Article 6(1)(b) of the Directive 95/46/EC).

2. Information requirements

Any collection of personal data implies prior supply of certain information to the individual concerned. Pursuant to Article 10 of Directive 95/46/EC, the person whose data is collected must be provided with at least the information about the identity of the controller (which includes the name as well as the physical and electronic address), the intended purpose(s) of the processing, the recipients of the data, the existence of the right of access and to rectify the data concerning him (see below), as well as whether replies to the questions are obligatory and the possible consequences of failure to reply. Obligatory information is information which is necessary to carry out the requested service. All other information qualifies as "optional". It should be noted that the fact that someone does not provide such optional information cannot count against him or her in any way.

Where the controller anticipates that the personal data will be transferred to countries outside the European Union, he/she is obliged to inform data subjects whether or not the countries in question provide adequate level of protection of individuals with regard to their personal data within the meaning of Article 25 of the Directive 95/46/EC. The decision which countries do provide such adequate level of protection is taken by the Commission. Where such a transfer is planned, additional information concerning the identity and address of the recipients should be provided.

3. Automatic data collection procedures (cookies et al.)

It should be emphasised that the information requirements are also applicable in case of automatic data collection procedures. Typical examples of such invisible processing include "browser chattering", automatic hyperlinks to third parties, active content (e.g. Java) and cookies. Again, the necessary information must be given before any personal data is collected. In particular, the use of cookies (or other tools for storing information on the user's terminal equipment) is only allowed if the user may refuse the cookie to be installed. However, this condition does not apply if the use of the cookie is strictly necessary in order to provide a service explicitly requested by the user (Article 5(3) of the Directive 2002/58/EC).

4. The right of access

Another important point is the requirement to ensure effective exercise of the right to access and to rectify the data concerning an individual (Article 12 of the Directive 95/46/EC). Ideally, it should be possible to exercise these rights both at the physical address of the controller and on-line. Of course, adequate security measures should be taken in order to guarantee that only the data subject has on-line access to information that concerns him or her.

5. Notification requirement

Another important obligation of data controllers is the requirement to notify the respective national data protection authority before any data processing operation is carried out (Article 18 of the Directive 95/46/EC). The Directive leaves to the Member States the possibility to simplify the notification procedure or to waive it altogether in certain situations. However, for the vast majority of entities engaged in any form of automated processing of personal data (whether on the Internet or other networks) the notification remains obligatory.

The information to be given in a notification must include at least:

- a) The name and address of the controller and of his/her representative, if any;
- b) The purpose(s) of the processing;
- c) A description of the category or categories of data subjects and of the data or categories of data relating to them;
- d) The recipients or categories of recipients to whom the data might be disclosed;
- e) Proposed transfers of data to third countries;
- f) A general description allowing a preliminary assessment to be made of the appropriateness of the measures taken pursuant to Article 17 to ensure security of processing.

The Article 29 Working Party has recommended that the registration number of the notification could appear on the controller's website.

It should be kept in mind that the above remarks are very general in nature. The ultimate way of applying them to the PRIME framework will depend among others on the characteristics of the adopted solutions. For instance, an IDM system based entirely on a user's terminal equipment will give rise to different legal issues than one based on a proxy server or a special protocol. The detailed obligations and responsibilities of each player (Internet Access Providers, authentication providers, websites, Internet Service Providers (ISPs)) will depend on the role they perform in the process.

5.1.5 Liability of ISPs/data controllers

1. Liability regime according to the Directive on electronic commerce

Liability of Internet Service Providers is regulated in Articles 12-14 of the Directive 2000/31/EC on electronic commerce. The Directive takes a horizontal approach to liability, i.e. it concerns liability for all types of illegal activities initiated by third parties on-line (e.g. copyright piracy, unfair competition practices, misleading advertising, etc.). It establishes a number of limitations on the liability. Such limitations are based on the specific types of activities undertaken by operators, as opposed to different categories of operators. The fact that an ISP qualifies for an exemption from liability as regards a particular act does not provide him with an exemption for all of his/her other activities. It should be noted that the provisions of the Directive do not affect the underlying material law governing the different limitations on the liability. Thus, if a service provider fails to qualify for such limitations, the nature and scope of his/her liability will be established on the basis of Member States legislation.

The Directive does not impose a general obligation to monitor or actively to seek facts or circumstances indicating illegal activities and expressly forbids Member States from imposing such obligations on intermediary service providers (Article 15). However, Member States may impose on information society service providers the obligation to promptly inform public authorities of allegedly

illegal activities undertaken by recipients of their services. Furthermore, the limitation of liability for intermediary service providers regarding the transmitted information does not affect the possibility of injunctions of different kinds, such as orders by courts or administrative authorities requiring the termination or prevention of any infringement, including the removal of illegal information (Recital 45).

According to the Directive, on-line service providers have a duty to act, under certain circumstances, with a view to preventing or stopping illegal activities. The exemptions apply only to intermediary service providers, i.e. those service providers whose activities are limited to the technical process of operating and providing access to communication networks. These activities are of merely technical, passive nature and the service provider has neither knowledge nor control over the information that is transmitted or stored.

A service provider may benefit from the “mere conduit” exemption when he/she does not initiate the transmission, does not select the receiver of the transmission and does not select or modify the information contained in the transmission (Article 12(1)). The transmission and provision of access include the automatic, intermediate and transient storage of information in so far as this takes place for the sole purpose of carrying out the transmission (Article 12(2)). “Caching”, i.e. automatic, transient, intermediate and temporary storage of information performed for the sole purpose of making the transmission more efficient, is also exempted (Article 13). “Hosting” activities are exempted from liability as long as the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent. Upon obtaining knowledge or awareness, the hosting provider has to remove expeditiously or disable access to the information (Article 14).

2. Liability regime according to the Directive on electronic signatures

The Directive on electronic signature expressly states that certification service providers, issuing certificates or providing other services related to electronic signatures¹³, cannot be prevented from indicating in the certificate a pseudonym instead of the signatory’s name. In this context, the liability regime of certification service providers is relevant for our research.

The Directive on electronic signatures concentrates on the relation between certification service providers issuing qualified certificates and any entity or legal or natural person who reasonably relied on that certificate. It does not affect the contractual relationship between certification service providers and the recipient of a certificate nor the relationship between the certification providers and public authorities.

In the first place, a service provider issuing a (pseudonymous) certificate is liable for the damage resulting from the inaccuracy and incompleteness of information contained in the qualified certificate at the time of the issuance of the certificate. Indeed, one can reasonably not expect that the certificate service provider would permanently verify the accuracy of the information. This is a responsibility of the recipient of the certificate, who possibly will have to revoke the certificate.

A service provider issuing a (pseudonymous) certificate should also guarantee that the recipient of the certificate holds, at the time of the issuance of the certificate, the signature-creation data corresponding to the signature verification data given in the certificate. If the certification service provider generates both, he/she should assure that they can be used in a complementary manner.

Finally a service provider issuing a (pseudonymous) certificate should ensure that the date and time of revocation of the certificate are accurately registered.

The certification service provider is liable for damage caused by non-compliance of the above mentioned obligations, unless the certification service provider proves that he/she has not acted negligently. It could be for instance foreseeable that the certificate service provider registered the revocation of a certificate via a register accessible on his/her website, but that third parties had no access to the website for a reason out of control of the certification service provider. The certificate

¹³ Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, Official Journal L No. 13, 19.01.2000, p. 12.

service provider can limit his/her liability on two grounds only: by indicating in a qualified certificate limitations on the use of that certificate or on the value of transactions for which the certificate can be used, provided that the limitations are recognizable to third parties.

At this stage we could conclude that the existing liability regimes with a possible flexibility and clarification developed in user agreements on a contractual basis should be sufficient to provide for a liability legal framework for anonymity services.

3. Liability regime according to the Data Protection Directive

The data protection Directive 95/46/EC also contains a liability provision. Pursuant to Article 23, any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national data protection legislation is entitled to compensation from the controller for the damage suffered. The controller may be exempted from liability, in whole or in part, if he/she proves that he/she is not responsible for the event giving rise to the damage.

5.1.6 Mandatory Retention of Traffic Data and its Implications for Privacy Protection

Traffic data are the data relating to subscribers of communications networks processed by service providers in order to establish connections and to transmit information. General definitions of traffic data can be found in a number of legal texts. For instance, the Council of Europe Convention on Cyber Crime defines traffic data as 'any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service'¹⁴. Pursuant to Article 2(b) of Directive 2002/58/EC on privacy and electronic communications, traffic data means 'any data processed for the purpose of the conveyance of a communications on an electronic communications network or for the billing thereof'. The Data Protection Working Party specifies in its Working Document on Privacy on the Internet of 21 November 2000 that – applied to e-mail communication- traffic data consists partly of information supplied by the sender (e.g. e-mail address of the recipient) and partly of technical information generated automatically during the processing of the e-mail (e.g. date and time sent, type and version of 'e-mail client'). The Working Party considers the following items to be included under the definition of 'traffic data': e-mail address and IP address of sender; type, version and language of the client agent; e-mail address of receiver; date and time of sending the e-mail; size of the e-mail; character set used; subject of the mail that can generate information about the content of the communication too; name, size and type of any attached documents; lists of Simple Mail Transfer Protocol (SMTP) relays used for the transmission¹⁵.

Law enforcement authorities claim that traffic data are essential to effectively trace perpetrators of all types of crimes involving the use of communications networks, such as unauthorised access to computer networks (hacking), theft of trade secrets, sabotage of critical IT systems, abuse of telephone systems, theft of telephone units, but also crimes that are not strictly related to, neither automatically associated with computer networks, including fraud, drug trafficking, human smuggling, blackmail, harassment, defamation and terrorism. The purpose of general retention of traffic data is to be able, in case of a crime, to trace back and locate geographically and chronologically the end-user device that was used to transmit the initial information. From this perspective, erasing electronic communications trails would have the same effect as wiping all fingerprints or bloodstains at the crime scene before any police investigation could start. The problem with mandatory general retention of traffic data that puts Law Enforcement Agencies (LEAs) at odds with privacy and human rights advocates is, however, that not only the digital 'fingerprints' of suspected criminals are being stored, but also those of the whole population that is beyond suspicion.

14 Article 1(d) of the Convention on Cyber Crime, text available at: <http://conventions.coe.int/Treaty/en>

15 Data Protection Working Party, Working document 'Privacy on the Internet an integrated EU approach to on-line data protection', 21 November 2000, 5063/00/EN/Final/WP3, 13; text available at: http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs

Under current EU data protection rules, the confidentiality of traffic data remains the principle¹⁶. Traffic data may only be stored to the extent that it is necessary for the provision of the service for the purpose of billing and for interconnection payments, and for a limited time¹⁷. Traffic data necessary for the purposes of billing and interconnection payments may be processed only up to the end of the period during which the bill may lawfully be challenged or payment pursued¹⁸. However, as prices charged for communication services become less dependent on distance and destination and evolve towards flat rate billing, there will no longer be any need to store traffic data for billing purposes. This is one of the reasons why law enforcement authorities had advocated that service providers keep certain traffic data for at least a minimum period of time so that these data may be used for law enforcement purposes; their claims have been taken into account and reflected in the provisions of the 2002/58/EC Directive.

On the one hand, Article 6 prohibits listening, tapping, storage or other kinds of interception or surveillance of communications *and the related traffic data*, but this is subject to an important exception. Namely, Article 15 authorises Member States to retain traffic data “when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security, defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system.” For those, quite broadly defined, purposes Member States may render the retention of traffic data mandatory for a limited period of time. All such measures must, of course, be in accordance with the general principles of Community law, i.e. the principles recognized by the Charter of Fundamental Rights of the European Union, including the right to privacy, the right to protection of personal data and the freedom of expression and information (Articles 7, 8 and 11 of the Charter).

Within the EU the issue of the mandatory retention of traffic data has been on the political agenda for quite a while now¹⁹. In particular, the terrorist attacks in the United States in 2001 and recently in Madrid have been used to put some legislative initiatives in the spotlight. Nevertheless, for the time being, the mandatory retention of traffic data remains an exception – for law enforcement purposes and for a limited period only – to the general rule of immediate erasing or anonymising traffic data. In any case, future developments in this field must be followed closely in order to assess their potential implications for the use of on-line anonymity.

5.1.7 Legal Research Challenges

5.1.7.1 Privacy Enhancing Technologies

Article 6(1) of the Directive 95/46/EC embodies the principle of data minimisation in its letter c) by stating that the processing of personal data should be limited to data that are adequate, relevant and not excessive. This idea is reinforced by its letter e) adding that data should only be kept in a form that permits identification of data subject for no longer that is necessary for the purposes for which the data were collected or for which they are further processed. As a consequence, technical tools and PETs in particular, should be available to contribute to the effective implementation of these requirements.

Article 17 of the Directive requires that controllers implement security measures which are appropriate to the risks presented for personal data in storage or transmission, with a view to protecting personal data against accidental loss, alteration, unauthorised access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

16 Article 5 of Directive 2002/58/EC

17 Recital 26 to Directive 2002/58/EC

18 Article 6(2) of Directive 2002/58/EC

19 See e.g. the draft Council Framework Decision on data retention and access by the law enforcement agencies prepared by the Belgian Presidency in 2001. The document had apparently been considered confidential, but it was disclosed by Statewatch on August 21, 2002 and made available on the organisation’s website.

Striving towards an optimal collaboration of regulatory instruments and privacy enhancing technologies should also be combined with effective solutions for monitoring the development and the introduction of privacy *decreasing* technologies.

In order to increase the effective use of privacy enhancing technologies, possible obstacles should be removed to create a favourable environment for the use of these technologies. For instance, how could we avoid that users of PETs are not discriminated against in consulting websites (e.g. when using cookie blockers)? How to avoid that users of PETs (e.g. when using anonymisers) are not discriminated against in criminal or civil investigations? The emergence of new legal obstacles to freely use some types of PETs is also not illusory²⁰. Service providers also have controlling rights and duties over traffic and/or content according to the type of services offered, particularly in respect with the EU Directive on electronic commerce. One could also question how the right to use cryptography will develop?

5.1.7.2 *Multiple Digital Identities and Anonymity*

According to the Directive, an identifiable person is one "who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his/her physical, physiological, mental, economic, cultural or social identity". The EU Directive specifies in its Recital 26 that to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person.

It is generally known that opportunities to create fictitious virtual identities, potentially in fully fictitious environments are highly exploited in a digital context. The creation of virtual identities can be motivated by privacy and security concerns, convenience or leisure. Virtual identities may disappear without leaving traces. This may raise legal questions concerning accountability, legal representation (for instance, when minors adopt 'virtual' identities), as well as contractual and tort liability and law enforcement issues.

The concept of on-line identity is related to the one of on-line anonymity. Interdisciplinary research shows that legal definitions do not necessarily match with technological concepts, which is also the case for the concept of on-line anonymity. Currently there is no legal 'answer' to the whole taxonomy of technical properties and degrees of on-line anonymity (unlinkability, untraceability, unobservability, condition/unconditional on-line anonymity). In a legal context, the type of anonymity is usually not specified but limited to a mere ruling on an explicit or implicit authorisation or - on the contrary - a ban to use anonymity or pseudonymity. For instance, the EU Directive on electronic signatures provides for an express right of the signatory to mention a pseudonym instead of his/her real name (Art.8), whereas - on the contrary - the specific data protection Directive regarding the electronic communication sector bans explicitly the use of anonymity for sending commercial communications (Art.13(4)).

5.1.7.3 *Public Key Infrastructures*

Public Key Infrastructure (PKI) commonly supports four functions - authentication, integrity, non-repudiation and confidentiality - to guarantee security and reliability of electronic exchange of

²⁰ E.g. in Belgium, a provision recently inserted into the law of 21 March 1991 on the reform of certain economic public companies allows the King (i.e. the Federal Government) to fully or partly forbid the rendering of telecommunication services which make impossible or could hinder the identification of the user or the interception of telecommunications by law enforcement agencies. In other words, the law opens the possibility to ban anonymity service by means of a Royal Decree. Also recently, several Member States have proposed a draft EU Framework Decision that if adopted will mandate the retention of all communications location and traffic data for between 1 and 3 years, or longer. The proposal, which will apply to the: 'prevention, investigation, detection and prosecution of crime or criminal offences including terrorism' was endorsed by the EU summit on 25 March 2004.

information. Whilst PKI applications can enhance privacy, there are serious privacy risks linked with the use of PKI. Currently PKI is still very often entirely based on the use of identity certificates. In order to improve privacy protection, researchers have proposed to make more use of attribute certificates or, more generally, certificates which certify a credential, rather than an identity.

5.1.7.4 E-government

The development of e-government raises numerous privacy issues. The need for more transparency and efficiency within administration has to be reconciled with privacy requirements.

Citizens have to identify themselves to benefit from a whole range of public services, such as e.g. health and other social services, or to fulfil certain obligations, e.g. taxation. The effective need for identification varies considerably according to the type of service asked for. In the field of e-government, the access to social security rights will require a high identification whereas a citizen should principally benefit from an anonymous access to tax simulations. In between, a whole taxonomy of identification and authentication degrees can technically be envisaged for different types of requests or activities.

According to Article 8, paragraph 7, of the European Data Protection Directive, Member States have to determine the conditions under which a national identification number or any other identifier or general application may be processed.

At the same time, a large number of public services should indeed be accessed anonymously, in particular when there is no purpose for identification, such as gathering information or tax simulations. In several countries initiatives are taking place to develop an electronic ID card. How to regulate the use of electronic ID cards for different functionalities, e.g. simultaneous control of identity and access to administrative services?

5.1.7.5 State Security and Law Enforcement

The right to privacy as guaranteed by the European Convention on Human Rights, allows no interference by a public authority with the exercise of this right except if the interference is "in accordance with the law and is necessary in a democratic society for the protection of public order, prevention of crime."

With the increase and diversification of law enforcement activities, a considerable number of privacy decreasing regulations and technologies have been widely adopted the last years, for the sake of public security. New law enforcement policy trends that have been identified are: increased communications surveillance; search and seizure powers by reducing authorization requirements and oversight; increased data sharing, e.g. relating to traveller's information, financial information. These trends result in an increased profiling and identification. As a matter of example, regulations on mandatory retention of traffic data have raised privacy concerns.

Moreover, the additional threat with privacy decreasing technologies developed for law enforcement is their overall opacity for citizens. Consequently, questions to resolve are: How can developers of privacy decreasing technologies for law enforcement purposes be monitored timely to ensure a right balance between security and privacy? How to effectively educate and control implementers of law enforcement technologies, and how to control the controllers?

5.1.8 Legal Evaluation of Application Scenarios

5.1.8.1 Location Based Services Scenarios

The not anonymous location of a person is personal data that is subject to data protection law. Location data may refer to the latitude, longitude and altitude of the user's terminal equipment, to the direction of travel, to the level of accuracy of the location information, to the identification of the network cell in which the terminal equipment is located at a certain point in time and to the time the location information was recorded. Digital mobile networks may have the capacity to process location data which are more precise than is necessary for the transmission of communications and which are used for the provision of value added services such as services providing individualised traffic

information and guidance to drivers. For processing of this data the prior consent of the affected person is needed. This includes that the person is informed of the type of location data which will be processed, of the purposes and duration of the processing and whether the data will be transmitted to a third party. Where the provision of a value added service requires that traffic or location data are forwarded from an electronic communications service provider to a provider of value added services, the subscribers or users to whom the data are related should also be fully informed of this forwarding before giving their consent for the processing of the data.

This kind of contract could be in writing or (more practical for mobile services) in electronic form. For Europe, Art. 9 of the Directive 2002/58/EG is applicable for “location data other than traffic data”:

- Where location data other than traffic data, relating to users or subscribers of public communications networks or publicly available electronic communications services, can be processed, such data may only be processed when they are *made anonymous*, or with the *consent of the users* or subscribers to the extent and for the duration necessary for the provision of a value added service. The service provider must *inform the users* or subscribers, *prior to obtaining* their consent, of the type of location data other than traffic data which will be processed, of the purposes and duration of the processing and whether the data will be transmitted to a third party for the purpose of providing the value added service. Users or subscribers shall be given the *possibility to withdraw* their consent for the processing of location data other than traffic data at any time;
- Where consent of the users or subscribers has been obtained for the processing of location data other than traffic data, the user or subscriber must continue to have the possibility, using a simple means and free of charge, of *temporarily refusing the processing* of such data *for each connection* to the network or *for each transmission* of a communication;
- Processing of location data other than traffic data in accordance with paragraphs 1 and 2 must be *restricted* to persons acting under the authority of the provider of the public communications network or publicly available communications service or of the third party providing the value added service, and must be restricted to what is necessary for the purposes of providing the value added service.

Open questions are about conditions regarding the consent of the user and about possibilities for special services to rely on only one acknowledgement of the user for actual and future communications. It is the task for the European countries to transcribe the Directive in these points. Inadmissible is in any case to require consent of the user for all kind of services in advance because in this case it is unclear for him to see what services are affected.

5.1.8.2 E-Science Scenario

Since the Scientific Review process is an internal process within for instance a publishing company, it is basically the challenge of the publisher itself to organise a review process. There is no legislation that regulates the review process of a private publisher. Nevertheless, the publisher and the reviewer have to take notice of the copyright aspects. The publisher has to ensure that the work does not leave the internal sphere and that the attention of the reviewer is drawn to the copyright law.

In order to ensure confidentiality and to enable authors to demonstrate a possible plagiarism by a reviewer (or to establish priority in case of patentable material), it seems to be necessary to foresee some form of traceability of the reviewers. For instance, the text for review could be time-stamped at its arrival at the publisher and signed with an electronic signature. This would allow the author to demonstrate later that he had sent the document to the publisher at the time specified. In order to prove which reviewer had reviewed the text, pseudonymous electronic signatures could be used.

Public institutions particularly have to pay attention to fundamental rights like equality of treatment and non-discrimination. In some cases and countries it could be necessary to have a formalised call for tenders (cf. also government procurement).

5.1.8.3 E-Commerce Scenario

According to European continental law tradition, a binding legal transaction takes place where there is agreement between two or more parties regarding a number of obligations. The fact that parties come to this agreement without knowing each other's identity does not in principle prevent a transaction from being legally binding. However, anonymous transactions may pose problems with respect to the assessment of the capacity of the contracting parties to enter into a given contract (e.g. age, capacity as a consumer, professional etc.). Transactions entered into anonymously are also quite difficult in terms of presenting evidence in case of a dispute or breach of contract.

The legality and feasibility of fully anonymous payment system needs to be further analysed. Banking sector, including electronic banking, is heavily regulated because of its importance for a country's welfare. The state usually imposes controls requiring identification and authentication to ensure that movements of money are legitimate, to combat fraud, counterfeit and money laundering. Most of these issues have been addressed at the EU level.

5.1.8.4 Task Assignment Scenario

In this scenario, a client is requesting something from an organisation. Private organisations are free to decide how they assign tasks as long as there is no contract about it. Only some special cases like warranty are settled by law.

Governmental organisations have to take notice of the civil rights like equality of treatment. The usage of pseudonyms where the officials cannot see the name of the client could help to ensure this non-discrimination requirement.

However, special laws and regulations regulate the administrative procedure today. This belongs to the countries itself. On the one hand governments have to observe privacy protection law and have to avoid collecting too much personal data. On the other hand there are documentation obligations to the public for administrative matters. Especially in Scandinavia there are rights to obtain information for every citizen about administrative action. So there are some special laws and regulations about keeping records. Also if a decision by the officials / government is expected that affects third parties these parties must have the possibility to answer back by knowing the facts. This includes the possibility to reveal pseudonyms for vested interests.

5.1.8.5 Ambient Intelligence Scenario

This scenario is likely to prove very challenging from the data protection point of view. In the proposed Ambient Intelligence scenario, data is no longer recorded/input via a keyboard or a mouse, but collected automatically via sensors (e.g. RFID tags) in the user's environment.

In the first place, it will have to be determined to what extent the data gathered qualifies as personal data within the meaning of the Directive 95/46/EC. Pursuant to Article 2(a), personal data is defined as "any information relating to an *identified or identifiable natural person* (data subject). An identifiable person is "one who can be identified, directly or indirectly, in particular by reference to an identification number or to one of more factors specific to his/her physical, physiological, mental, economic, cultural or social identity."

The concept of identifiability, while fundamental for the whole system of legal protection of privacy, has been interpreted in a divergent way by various Member States. Most of them took the position that data had no connection with an identifiable person if the controller (i.e. the person responsible for the processing of personal data) could not retrieve the identity of the person without unreasonable efforts. In such cases, the information was not considered as personal data as far as the controller was concerned. However, in countries like France and Belgium a different view was taken. It has been based on the wording of Recital 26 of the Directive that specifies that to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or *by any other person* to identify the said person. Consequently, only fully anonymous data, which could by no means and by nobody be linked to an individual, would fall outside the scope of the "personal data" within the meaning of the Directive.

Consequently, where the data gathered by means of RFID tags (or other sensors) is made anonymous (it seems possible that even then it would retain its commercial value) and can no longer be linked to an identified or identifiable individual, it will not qualify as personal data and will fall outside the scope of the EU legislation. In all other cases, however (i.e. where the data is not entirely anonymous, but a link with an individual still exists) the data protection principles will apply in full. In particular, any information concerning a physical location of an individual will qualify as personal data if it is not made entirely anonymous (see above remarks concerning the Location Based Services).

A problematic issue is the fact that data collection through RFID tags often takes place without the subject's being aware of it. This contradicts the basic principle of legitimate data processing, according to which personal data may be processed only if the data subject has unambiguously given his/her consent. Under certain circumstances it could be argued that the processing is legitimate even without the data subject's consent, for instance where it is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract. However, in most cases the general principle will apply. Consequently, in all cases of "invisible data processing" the individual concerned should be informed *in advance* that his/her personal data are being collected. At the same time, he or she must be provided with the necessary information concerning the identity of the data controller, the purpose of the collection, the possible recipients of data, as well as the existence of the right of access.

The transparency concerning the fact and the purpose(s) of data processing and, in particular, the identity of the controller, are crucial for determining who is liable for possible damage resulting from unlawful processing of personal data.

According to the finality principle (Article 6), personal data may only be collected for specified, explicit and legitimate purpose and not further processed in a way incompatible with those purposes. That would mean that if data is gathered for the purpose of facilitating the purchasing process (e.g. easier, automated check-out and payment) it may not be further used e.g. to provide a value-added service.

5.2 Social Aspects of Privacy and Identity Management in Online Relationships Environment

Privacy is an important topic in the media these days. Reports of threats and worries about privacy, the invasion, loss or even death of privacy appear regularly. Identity theft for instance has been reported to be one of the fastest growing crimes in many countries. In general, public-opinion surveys indicate that by far the majority of people are very concerned about their privacy. At the same time we may observe a development that, with the advent of the online world and new possibilities of digitising user characteristics and behaviour, the ways of identifying, profiling, tracking and tracing of individuals are further increasing. The design of trust in online relationships therefore gains in importance. As a result, solutions to protect privacy, such as privacy-enhancing technologies, are asked and sought for. As these solutions stand or fall with their adoption in society, there is a clear need to understand criteria for social acceptance. This is the more important from the perspective that social adoption of solutions, such as intended to be developed by PRIME, is currently lacking: privacy-enhancing technologies in general have yet to achieve widespread acceptance.

To be able to determine criteria for social adoption of PRIME solutions, we would need to have knowledge of peoples' perceptions and practices of online privacy and privacy protection. So far however, there is not much empirical knowledge available on user attitudes, knowledge and practices of online privacy. Available user survey data turn out to be difficult to compare because of differences in applied methodologies, samples and application areas. Besides, empirical evidence at present suggests a significant discrepancy between privacy principles and privacy practices [20]. Consequently, there is a clear need to more systematically explore social aspects playing a role in online privacy perceptions and practices, and particularly also in the adoption of solutions to enhance privacy, such as developed in PRIME. To be able to do so, we first need to determine how we perceive the concept of privacy. We will do that in paragraph 5.2.1. Secondly, we will argue that we will need to get more knowledge about the ways in which newly available technologies offer new possibilities to

construct, verify and challenge people's identity in online relationships in different institutional arrangements (section 5.2.2).

5.2.1 Privacy as a Situated and Dynamic Concept

Research done so far on the way people conceptualise their privacy in relation to ICT-applications, points towards the fact that privacy is perceived to be a complex notion, which has a different meaning in different contexts to various individuals. A research project in the Netherlands for instance led to the identification of a number of core values related to the concept of privacy, varying from individual autonomy to prevention from stigmatisation and manipulation [21]. Besides, characteristics of different physical locations (e.g. at home, at school or at work) seem to affect peoples' perceptions of privacy with regard to their online activities.

Also in literature we may come across many definitions and interpretations attached to the concept of privacy, stemming from diverse perspectives. Legal, policy, philosophical and sociological views on privacy for instance have resulted in a large variety of rights and values that can be related to this concept, such as human dignity, personhood, identity and anonymity, freedom of thought, freedom of expression or freedom from surveillance (see for instance respectively [22] [23] [24] [25]). Efforts to arrive at one unifying definition or interpretation of privacy therefore seem to be hopeless. According to a long-time privacy scholar Alan Westin, no definition of privacy is possible, because privacy issues are fundamentally matters of values, interests, and power (Westin 1995, cited in [22]).

Distinctions between privacy definitions and interpretations increase even further, if we take into account that different regions around the world employ different values, interests and power towards privacy issues. For instance, privacy and privacy protection will have a different meaning in countries with varying social and ethical traditions regarding the collection, use and management of personal data, such as Singapore, the United States or Germany. But also within the EU itself, we may expect to find differences in privacy perceptions and practices as a result of different socio-historical cultures towards the exchange and use of personal data. For instance, from a perspective of the past communistic regimes in former Eastern European countries, a Hungarian citizen likely will have a different perception of privacy in dealing with institutions, compared to a Swedish, Italian or UK citizens, who are living in countries with different cultures regarding the exchange and use of personal data. Trust in information relationships with institutions therefore seems to be varied for each of these societies. Related to this, varying identification and identity management practices have developed so far across European countries. As a result, trust in emerging online relationships might have different meanings for different parts of Europe, and, consequently, solutions to enhance trust in these relationships may need to be different, or differently designed.

In addition, a so-called 'privacy gap' in the privacy experience of individuals, i.e. a disconnection between privacy perception and actual practice, can be observed in several cases. Attitudes of individuals with regard to their privacy practice are different for different relationships. Individuals may be for instance willing in certain relationships to give up their privacy and provide specific personal data, whereas to provide the same personal data in relationships with other parties might be a privacy concern to the same individual. Examples are to provide financial data to the taxation office or to a loyalty programme of a private company; or to provide medical data to a medical doctor or to a fitness centre. Often, the will of individuals to provide personal data seems to be a trade-off between benefits (e.g. gain of comfort, increased functionality, discounts) and risks or costs (e.g. mistrust, disadvantages, risk of misuse or manipulation). Besides, citizens may have different attitudes with regard to their privacy practice in initial and ongoing information relationships respectively. Accordingly, varying information relationships with different organisations may require other ways of dealing with privacy and identity management issues. In looking for ways to establish trust in information relationships with different organisations in online environments, it therefore is important to take a socio-cultural as well as an institution-relational approach in exploring privacy perceptions and practices.

That is not to say that privacy perceptions and practices, once determined, will always stay the same. Privacy turns out to be a concept which is continuously developing through time. For instance, [26]

points at several shifts in dominant interpretations of privacy in the Netherlands since the end of the 19th century: examples of successive trends are the interpretation of privacy as a kind of individual autonomy, the restriction to informational privacy, the emergence of the notion of informational self-determination and the increasing attention for the legitimacy of privacy infringements. The concept of privacy can in fact be perceived as a social value competing with other social values through time, such as public safety at present. '9/11' for instance can be acknowledged as an important social driver for shifts in balancing these values in political decision making, resulting in this particular case in privacy restrictions in many countries.

Given these varied, relational, socio-cultural and shifting interpretations of privacy, there is a need for a contextualised approach to explore privacy issues. Privacy should be viewed as a concept that stands, not above individuals and their activities, but between them, and as one that is regularly being (re)defined (see [20] and [27]). A concept which also needs to be related to a country's socio-historical culture regarding the exchange and use of personal data in information relationships. As a result, social factors influencing the adoption and regulation of privacy-enhancing technologies may differ across Europe and through time, both in terms of nature and degree of magnitude. Further research therefore needs to be done to explore social requirements for the adoption of privacy-enhancing technologies in different application areas in different European countries at present.

5.2.2 The Need to Reconceptualise Identification and Identity Management in Online Environments

Before the information age, a person's identity and information related to his or her identification, seemed to be more or less controlled. But with the advent of the information society, all that has changed. ICTs have become pervasive in our society and offer new possibilities to construct, verify and challenge identities in unprecedented ways. By now, identity and personal information have become essential vehicles for the materialisation of e-commerce, e-government, e-health and other applications of the information society. Emphasis is on user-friendliness, more efficient services support, law enforcement, user-empowerment, user mobility and support for human interactions. But identity and identification in online environments have a second angle as well. With the advent of the online world and new possibilities of digitising identity-related characteristics, the ways of identifying and profiling individuals are increasing. With the introduction of new technologies, such as mobile location based services or ambient intelligence, the range of possibilities to identify individuals is further increased. At the same time, we do not know exactly yet what kind of effects these new possibilities will have upon users and their privacy perception and practice.

Both in the developing online and offline world, we may perceive identities to be socially constructed in private relationships, but also in institutional arrangements where persons are identified and classified and in which decisions are taken about their desires and needs, their rights and claims. Identity therefore is not a constant but a process. Our identity is not developed by keeping ourselves separate from others: our identity is what others know about us. In knowing about us, power is already exercised (see [28]). In addition, having knowledge or power may imply the risk of power abuse.

In European countries in general, we may observe a development as a result of opportunities offered by new ICTs that the means of identification are increasingly being geared to the individual, creating an almost comprehensive picture of a person's identity (see [29]). For instance, the use of numbers is increasing, with the same numbers being used for multiple purposes. Besides, a general trend in identity management is to more and more require identification with the heaviest possible means of identification, i.e. biometrics (idem). The balance of power therefore seems to be more and more shifting towards institutions, at the expense of the individual. Arguments for using far-reaching forms of identification like biometrics are often related to convenience (e.g. efficiency and increased speed of service delivery) and combat of fraud or even crime. However, the question remains to what extent citizens of European countries find biometrics an acceptable means for identification purposes. An important issue in this respect is whether this high identification level and, with that, the potential violation of the citizen's privacy, is in all cases needed.

Consequently, with the increasing use of new ICTs in our society, there currently seems to be an urgent need to re-examine the concepts of identity and identification in different application areas. The new possibilities offered by ICTs may not only lead to changes in various social processes, but are also challenging existing organisational, legal and democratic arrangements for identity construction and identification in our society. Therefore, also the institutional context needs to be taken into account in re-examining processes of identity construction and identification.

5.2.3 Social Scientific Research Challenges

With identification, in multiple variations, becoming a key concept in our information society, private organisations, public sector organisations, policy and law makers, regulators, courts and others are forced to rethink and redefine identity, identification interests and the mechanisms for identification, having in mind that privacy perceptions can be different for different people in different relationships, and may shift over time. Such an exercise is of crucial importance for the further development of our information society, since in the end identity-related interests and values must be offset against and balanced by other interests and values, amongst them privacy and anonymity. Related to this, it is increasingly important to look at solutions for privacy-enhanced identity management, and to explore social factors influencing the adoption of these solutions in society.

With the current lack of knowledge on the social implications of new ICTs for privacy and identity management, there is a clear need for social scientific research to explore new ways of identification and identity management in different e-service relationships (e-commerce, e-health and e-government) compared to traditional 'face-to-face' service relationships, and their implications for individual users. Additionally, criteria for social adoption of opportunities, such as the solutions developed in PRIME, to enhance user trust in these relationships, need to be further examined. Acknowledging privacy as a situated and dynamic concept, social scientific research can contribute to explore whether and to what extent social criteria to establish trust in online relationships between users and service providing organisations are different for different parts of Europe with varying socio-historical cultures towards the exchange and use of personal data.

5.3 Business Models and Economic Drivers

Initial assessments of the business of privacy present a rather pessimistic outlook for consumers in the information society. For example, it has been suggested that the ready availability of ICTs is making it easier for businesses to use personal data for commercial advantage. Furthermore, the strategic value of personal data for businesses today implies that developments in ICTs can pose a threat to privacy. Not only are there economic incentives for businesses to maximize the commercial value of customer data, there are few economic incentives for businesses to comply with privacy regulations. In this view, privacy protection is a cost to business. And, at the same time, while consumer surveys indicate that consumers value their privacy, the lack of transparency regarding privacy practices makes it costly for consumers to determine which businesses actually take the protection of personal data seriously. Economic theory can help to analyse this dilemma and provide a framework for redressing this imbalance.

The economics of privacy is an emerging area of research and its results are often counter-intuitive. Section 5.3.1 examines the strategic nature of personal data in ICT-enabled businesses today and the threats to privacy. It can be argued that the strategic value businesses attach to personal data does not automatically imply a threat to privacy. Instead, personal data and consumer confidence is an asset that businesses need to protect.

Section 5.3.2 examines some of the cost variables that fit into a cost benefit equation for protection of personal data. These business models are highly subjective, and studies based on such analysis are still being debated.

Section 5.3.3 examines the lack of adoption of PETs in the market and the consequences of information asymmetry. The difficulty in understanding privacy policies means that consumers can not easily differentiate between businesses that take data protection seriously, and those that do not.

Privacy and Identity Management for Europe

Some market mechanisms to create transparency in the marketplace through for example privacy seals is suggested as a means of overcoming such barriers to adoption.

Section 5.3.4 examines the threats to privacy in terms of externalities. Utilizing this concept we explain the right to privacy in terms of a public good that may be underprovided by the market. We then explain why business models need to incorporate the social costs in addition to private costs in order to create the right market incentives.

Section 5.3.5 examines the economics of privacy enforcement. It can be argued that the cost of enforcing privacy needs to be considered. Privacy enhancing technologies have the potential to reduce the cost of enforcing privacy, thereby attaining socially desirable results.

5.3.1 The Strategic Value of Personal Data

Proponents of free markets argue that information facilitates the matching of buyers and sellers, reduces search costs, and increases business efficiency. Rapid developments in information and communications technologies are enabling businesses and markets to utilise information more effectively. Having better information increases transparency and competition in the marketplace. Privacy or more specifically the protection of personal data in business data processing is often regarded as a constraint on business efficiency and hence counter-productive to business. Personal data is enabling a new degree of customisation in products and services that are transforming businesses today. Vendors with access to personalised data can target their customers more effectively and provide them with tailored products and customized services. Many consumers coping with a deluge of information today regard targeted marketing and personalised content as a valuable service. Developments in Customer Relationship Management, Information Portals, and Internet Commerce lend further support to such a business trend. Customer profiling and relationship management are strategic to business competition within the new ICT enabled business environment. The notion that businesses would abuse this relationship need to take into account the strategic importance businesses attach to personal data for today. Since businesses need to build long-term relationships with their customers to benefit from the marketing campaign, maintaining consumer confidence in their privacy practices is taken very seriously. This is best espoused in Godin's concept of "permission marketing" [30].

The proponents of markets and industry self-regulation argue that if consumers value their privacy more than their suppliers do, they would choose to deal with businesses that implement stricter privacy policies, and those that do not provide the desired level of privacy protection, would ultimately lose out in sales. In this view, privacy regulations that force businesses to comply are adding to the costs to business rather than contributing to business value-added, and more importantly, it is distorting the amount of privacy protection consumers want. This viewpoint reflects unproven assumptions about the ability of technology and market mechanisms in providing a socially desirable level of privacy, in particular, it assumes consumers have perfect information about the purposes that their personal data is used for, and are able to differentiate between good and bad data protection practices in a costless manner. We explain in section 5.3.3 why this is not always the case.

Having shown that processing of personal data can be beneficial to businesses; it can be argued that it is also in a businesses' interest to protect personal data. Given the strategic and competitive value of personal data, businesses also recognise the need to protect these information assets. In this view, the protection of personal data is not an additional cost to business that does not add value; it is an opportunity that needs to be nurtured. It is not a source of inefficiency, but a goldmine that needs to be protected. Why would businesses want to abuse the trust that the data subjects placed in these organizations in handling their personal information in first place? They have more to lose than to win, since losing customers can have dire consequences.

The threat to privacy is rarely the illegitimate collection, retention, analysis and consolidation of personal data by responsible businesses approved by data subjects. Nor does the threat emulate from business that spent time developing and then implement organisation wide privacy policies that

comply with national legislation. Sometimes, the threat to privacy comes from organisations not recognising the consequences of failing to provide adequate controls on personal data. Sometimes it comes from businesses that purposely value the exploitation of personal data and the violation of privacy to their benefits more than the fulfillment of their customers' privacy expectations. However, more often, the threat to privacy comes from use of personal data for purposes for which it was not originally intended. To illustrate, some conference and exhibition organisers can charge in excess of one Euro per record for access to attendee data records for direct marketing campaigns. Credit reference agencies provide for a fee customer profiles based on wealth, propensity, shopping preferences and other segmentation techniques. The consolidation of public and private data sources for acquiring customers and initiating business contacts has spurred entire new businesses that collect and resell such personal data.

While many customer loyalty and relationship marketing schemes may be inconsistent with existing privacy regulations, as far as we are aware, the direct economic consequences of invasions of privacy are minor compared to the indirect effects of poor data management practices that result in identity theft, junk mail, spamming, and computer viruses. We address the economic consequences of the enhancing of privacy and the lack of privacy in the following section.

5.3.2 Problems in Building Business Models

Acknowledgement of the threat to privacy is rather different from reaching consensus on how to address this threat to privacy. A debate has been open for several years now on whether a market-based approach or a regulation-based approach is more suitable for regulating privacy. The debate as to the market alone can provide an adequate level of individual privacy and whether some form of regulation is necessary for a socially desirable level of individual privacy poses challenges to computing professionals and policy makers alike. Anecdotal evidence has been proffered to suggest that markets are inadequate in providing a socially desirable level of individual privacy [31] [32], and hence some form of regulation is desirable. However, dissenting arguments abound due to the lack of empirical evidence pinpointing the costs of privacy.

Modelling the cost of privacy to consumers and businesses can be highly subjective. For example, Robert Hahn [33] estimates the cost of compliance to US privacy rules to be US\$ 100,000 per company. Gellman [34] rebukes that figure and argues that a privacy sensitive family can spend up to US\$ 300 to protect their privacy. Miyoshi and Ho [35] identify some of the cost and benefits of compliance and the risks of non-compliance to privacy rules for service providers. These costs are summarized in Table 14 below.

Table 14 Cost of Compliance and Non-Compliance

Cost of Compliance	<ul style="list-style-type: none"> • Personnel costs • Developing and implementing privacy policies • Education and training • Monitoring and audit • Implementing privacy-enabling technologies
Cost of Non-compliance	<ul style="list-style-type: none"> • Regulatory fines • Lawsuits • Decline in stock price • Damage to public reputation • Reduced value of business products

Business models can be constructed based on the risks organisations are willing to incur by either complying or not complying with privacy regulations. However, such cost/benefit analyses still involve highly subjective figures. It is therefore difficult to make a business case for privacy-enhancing technologies based on for objective figures. Instead, we recommend that empirical studies in this area consider the relative costs between the cost of compliance and the cost of non-compliance to assess the whether the economics incentives are in place for businesses to comply with the law, and whether the sanctions are effective enough to change businesses behaviour. We make a case for adopting privacy-enhancing technologies in section 5.3.5 after describing the social costs of privacy.

5.3.3 The Market for Privacy Enhancing Identity Management Solutions

Anecdotal evidence suggests that the market for privacy enhancing technologies currently suffers from a problem of low adoption. Previous research on the low adoption rates in public key infrastructures and certification services market [36] indicates a problem of quality uncertainty that can be applied equally to the PETs and PIMs market. Privacy policies can be difficult to understand, hence the need to shared standards like ontologies, semantics, policies and practices. Because it is difficult for consumers to understand these terms and their consequences, it is difficult to differentiate between businesses that take data protection seriously, and those that do not. The information asymmetry between businesses and consumers in market means neither has the incentive for investing in state of the art technology of best practices, resulting in a kind of market failure. The mechanism used to illustrate this within the economics literature is known as the ‘lemons principle’.

The reason for market failure stems from the inability to signal quality in the market. Guarantees, brand names, and licensing are some of the countermeasures for reducing quality uncertainty in the market. Privacy audits carried out by private (e.g. consultancies and consumer associations) or governmental organizations (e.g. data protection authorities) can enhance compliance, and it can also serve as a means of reducing quality uncertainty and even signal quality. Privacy seals can incorporate various guarantee, branding, and licensing schemes have the effect of reducing quality uncertainty in the market by creating some kind of homogeneity. It can also signal quality by differentiating the good from the bad. Various assurance techniques can be introduced to create standards, increase transparency and hence bolster adoption in the marketplace. However, as shown in the certification services market [37], the lack of an agreed standard, or having too many different standards once again makes it difficult to signal quality in the market.

5.3.4 The Social Costs of Privacy

One of the insights provided the literature on law and economics is the concept of *externalities* - when the actions of one party have an effect on the welfare of others that it does not have a direct business relationship. The concept of externalities is often applied in the domain of environmental protection, and increasing in information security and privacy. The inability to internalise such costs makes it difficult to incorporate total costs in the economic system. The right to privacy can likewise be regarded as a public good with the tendency to be underprovided by the market. In a similar vein, the indirect effects due to poor privacy practices such as intrusion of privacy through unintended use of personal data, identity theft, junk mail, spamming, and computer viruses can be described as a negative externality. The effect of such negative externalities is analogous to pollution of the information environment. It can be argued that compliance with privacy has a dimension of social cost and therefore should not be reduced entirely into private cost (economic impact on a single party).

Economic theory describes commercial activity as the voluntary exchange of property rights through the price mechanism. Contracting parties transfer ownership of private goods when there is agreement on the terms of the exchange. Private goods tend to be excludable due to the property rights associated with ownership; and they tend to be rival in the sense that parties compete for the rights to the same scarce good. The market mechanism is efficient in economic terms if there is equilibrium between the supply and demand for private goods. While economics theory deals predominantly with the efficient exchange of private goods through the market mechanism, it also recognises a class of goods with very different characteristics. In contrast to private goods, public goods that enhance social welfare are non-excludable and non-rival in consumption. If one were to analyse the right to privacy in economic

terms, one could view it as a public good. Similar to other basic human rights, the right to privacy is a public good because it is non-excludable and non-rival. It is non-excludable because the acceptance of privacy as a universal principle implies that it applies to all parties in all places. It is also non-rival in the sense that if one person is given the right to privacy, it that does not diminish the right of another person to be given the same treatment. The more widely accepted the principle and practice of privacy, the more confidence all parties will have on benefits of the public good, and hence contribute to its production. The less the right to privacy is practiced, the less incentive there is for any party to provide the public good for others to enjoy. If the right to privacy has the characteristic of a public good, private actors are inclined to behave opportunistically by trying to free-ride on the public good without contributing to its production. Kaul describes this dilemma as follows:

“This is, indeed, a dilemma, that public goods face. Without some sort of collective-action mechanism they risk being under-provided. Conversely, without collective action public bads – such as pollution, noise, risky bank lending, and so on – would be overprovided.” [38]

Coase [39] argues that in the idealized world of zero transaction costs, the initial assignment of rights is irrelevant since the market will adjust itself to achieve the desired result. However, in a world of positive transaction costs, the initial assignment of rights and liability does matter. Using a Coasean analysis, Sholtz likewise argues that the problem of privacy can be addressed through reallocation of rights and liability.

“Economically, privacy can be understood as a problem of social cost, where the actions of one agent (e.g., a mailing list broker) impart a negative externality on another agent (e.g., an end consumer). Problems in social cost can be understood by modelling the liabilities, transaction costs and property rights assigned to various economic agents within the system, and can be resolved by reallocating property rights and liability to different agents as needed to achieve economic equilibrium.” [40]

Lessons from the application of these theories to the environmental protection area, suggests remedies like environmental tax and emission vouchers. Socially desired results are enforced through environmental assessment, allocating liabilities and imposing fines for non-compliance. These ideas are increasingly used to address the problem of spam, and market mechanisms for personal data [41].

While the collection of online information is predominantly used to facilitate transactions, such information can be re-used for a myriad of different purposes. The threat to privacy is not just the result of inexpensive data aggregation and data mining, or arguments concerning lost sales due to lack of privacy. The detrimental effects of erosion of privacy (e.g. surveillance, unwanted marketing, spam mail, identity theft) are a social cost that is often not qualified. Maintaining the status quo erodes social capital both online and offline. It can be argued that the debate as to whether the market or regulatory mechanism is more suitable for enhancing electronic commerce and online privacy can be addressed through reduction of the direct and indirect cost of complying with and enforcing privacy protection.

5.3.5 The Economics of Privacy Enforcement

With the implementation of EU Directive 95/46/EC in national legislation, the data protection principles in Europe are now well established. However, it has been observed that the enforcement of current data protection legislation is often lax [42]. We address in this section the issues facing data protection authorities in Europe and the difficulty in enforcing privacy protection. We try to explain from an economic perspective why the implementation of mechanisms to sanction for non-compliance is lacking, and the role of PETs strengthening enforcement.

First, the costs organisations incur for non-compliance with existing data protection legislation are often not commensurate with cost of dealing with complaints and investigations. Data protection authorities require significant resources to deal with complaints, inspections, audits, administrative decisions, and court actions. When the burden of proof is on the regulators, data protection authorities

Privacy and Identity Management for Europe

can only afford to react to the most serious complaints, resulting in lax enforcement of data protection legislation.

Second, the risks the organisations incur for non-compliance with data protection legislation can be justified by the lack of awareness of data protection practices, or the state of the art. Organisations can often plead innocence, and not take action until data protection authorities instigate an investigation. The burden is on the data protection authorities to educate the users and recommend changes in business practices for compliance with data protection legislation, hence the lax compliance with data protection legislation.

Third, in the absence of an effective privacy-seal programme or other effective ways of signalling compliance (or quality in general) in a market, organisations are rarely punished in the marketplace when they are not in compliance with data protection legislation or industry best practices. It is costly for individuals to verify whether businesses are complying with the information practices they disclose to customers. When consumers are unable to tell the difference, they are unwilling to pay higher prices with merchants that merely state that they invest in privacy-enhancing technologies and practices, but do not do so. When it is difficult to signal product quality within markets, the result is inferior products and services. Therefore there is a need to investigate assurance mechanisms, which is planned to be done within the PRIME project.

Finally, and most importantly, there is a need to educate consumers in their rights and exert their influence in the market. A well-informed public can have tremendous power to enforce privacy through for example:

1. By choosing service providers that respect privacy, demonstrated through privacy audits and privacy seals that they indeed comply with regulation and best practices;
2. By informing themselves through customer protection associations about which service providers respect privacy and merit trust
3. And by even paying such associations to establish list of such trustworthy or less trustworthy service providers

Because this is not yet happening to a significant extent in the market, one can argue that consumers just do not care enough to take action on their own. It can be argued that economic theory has much to contribute to the design of incentives to make a difference. Economic incentives for compliance and sanctions for non-compliance will create better market conditions for privacy protection in general. Compliance with and enforcement of privacy can also be accomplished through technological means and better business practices since they both have the potential to reduce the cost of compliance and enforcement.

5.3.5.1 Technology as Means to an End

Despite improvements in PETs, their widespread adoption continues to face economic barriers addressed in section 5.3.2. The economic rationales for adopting privacy-enhancing technologies may not be reducing private costs, but overall social costs. Introducing state of the art PETs to automate information processes makes it easier for businesses to ensure compliance with policy defined previously by the organisation. PETs can also help check whether the organisational privacy policy is consistent with national data protection legislation. The audit trails and reporting tools provided by PETs makes it easier to monitor for compliance and resolve disputes when they occur. The use of PETs can therefore facilitate stronger enforcement by removing the economic rationales for non-compliance, and shifting the risk/cost equation in favour of compliance. The adoption of PETs that have already withstood the test of standards setting processes should ensure stronger compliance with data protection legislation. However, technology alone is often insufficient without a sensible privacy policy in the first place. Feigenbaum [43] likewise discusses some of the limits of cryptographic research and technologies like Platform for Privacy Preferences (P3P).

5.3.5.2 *Business Practices as Means to an End*

Business policies and practices also play important roles in guaranteeing individual privacy. U.S. Federal Trade Commission (FTC) advocates fair information practices online and privacy disclosures as the way forward for industry self regulation. The efficacy of industry self-regulation is monitored through surveys like the FTC Privacy 2000 survey, which analysed privacy disclosure statements and primary self-regulatory enforcement initiatives - online privacy seal programs like Truste, BBBOnline Privacy Seal, CPA WebTrust and PWC BetterWeb. In a similar vein, the FTC also identified “enforcement - the use of a reliable mechanism to provide sanctions for non-compliance - as a critical component of any governmental or self-regulatory program to protect privacy online”. In 2000, the FTC which currently does not have authority to enforce privacy violations, recommended additional legislation to achieve adequate level of protection for online consumers. The need for stronger enforcement is present whether one adopts a market-based or regulatory approach. Enforcement of privacy can be accomplished through regulation (enforcement as a public good) and better business practices (enforcement as private good). We believe that privacy enhancing technologies like that being developed in the PRIME architecture and the legal and socio-economic principles developed in the PRIME framework can help reduce the overall cost of compliance and strengthen both private and public enforcement of privacy.

We have listed in this section some of the promising avenues of research. We contend that some but not all of the issues in privacy can be subject to economic analysis. While there are limits to any attempt to reduce a discussion on human rights into economics, it can be argued that economic analysis can yield useful insight into compliance and enforcement of privacy rules and practices. Utilising the growing literature on law and economics allows us to analyse the economic incentives for compliance or non-compliance with privacy rules. We address in this section some of the limits of PETs and the complementary role of business practices in protecting individual privacy. One of the objectives of an economic analysis is to reduce the overall cost of complying with privacy rules, and ultimately the costs of enforcement to ensure compliance. Technology and business practices are therefore complementary solutions to the problem of enforcing privacy protection. This is an area where the combination of information security and economics could yield fruitful results.

5.4 *The Necessity of a Multidisciplinary Regulatory Approach to Develop PRIME Solutions*

Regulation and adoption of PETs, such as developed in PRIME, are closely related to each other. When we look upon regulation using a multidisciplinary approach with an economic and social perspective, and thus not only from a purely legal perspective, regulation and adoption are even more interrelated. For instance, a PRIME technology that does not comply with European legislation is unlikely to be bought by European companies or accepted in the European society (legislation perspective); a PRIME business model with too high financial costs involved is unlikely to be adopted by e-service providing organisations or by users in the cases where they need to pay for the delivery of the e-service (economic perspective); and finally a PRIME solution which is socially not acceptable in Europe is unlikely to be implemented by e-service providers (social perspective).

If we use the three disciplinary perspectives at the same time, we may come across scenarios in which PRIME-solutions for instance will be acceptable from a social and economic point of view (e.g. in accordance with European societal norms and values, with low financial costs involved), but not in accordance with legislation. Or we might experience situations in which legislation has changed, which would require other conditions for social and economic acceptance. Also, major societal events like 9/11 may be a driver for (rapid) changes in both legal, economical and social types of regulation, and, with that, change the landscape for the adoption of PRIME-solutions under development.

The complexity of the interdependency of these different types of regulation increases even further, when we take into account the enormous variety of legal, economical and social regulation at the national level within the EU, or even at a regional level (e.g. in Germany or Belgium): social values, economic cost models and national legislation regarding privacy enhanced technologies can be hugely

Privacy and Identity Management for Europe

different in European countries, leading to possible situations in which developed PRIME-solutions may work in some countries, but not in others.

These examples of scenarios make clear that the multidisciplinary regulatory framework within which PRIME-solutions are being developed, will be, as a whole, decisive for the adoption of these solutions in European society. Also, they show the necessity to explore and refine the relationships between the different types of regulation at least at the European level, but possibly at the national administrative level as well, regularly during the PRIME-project. Only then an appropriate approach of privacy-enhancing technologies can be proposed that can be adopted by the European citizens.

6 PRIME Concepts, Models and Metaphors

Basic concepts for PRIME will be subject to further refinement and analysis in the context of the development of ontologies. The terminology is important for the use within the project to facilitate communication between the experts from the concerned fields. Outside the project terminology will serve as a means to establish the PRIME framework as a reference for privacy-enhancing identity management. IDM models for users and metaphors will be of key importance for the user interface design and will be addressed by the HCI activity within PRIME.

6.1 PRIME Concepts and Terminology

PRIME integrates partners from many different disciplines. It is therefore vital that participants from different disciplines can agree on a common terminology and set of concepts to be used throughout the project. This agreement on fundamental terms will also serve as a basis for the development of a more detailed ontology later in the project. The choice of which terms are considered key to the domain is important as well as the definition of those terms and their relationships. While early drafts of this document will not integrate explicit input from stakeholders beyond the research partners, it is nevertheless our aim to align the use of concepts with their understanding by all PRIME stakeholders.

The concepts included in the Appendix A represent definitions and relationships of a list of key privacy and identity management terms that were proposed and discussed by PRIME consortium members. These concepts will be further elaborated into PRIME concepts on which there will be consensus within the consortium and which will be published in PRIME Framework V1. The current list of concepts represents the results of the exercise (see <http://p3p.jrc.it/concepts/concepts.php>) and discussions conducted at the PRIME kick-off seminar in Brunnen and discussions conducted on the prime-concepts mailing list and via comments on drafts to date. The initial list of concepts was chosen by textual analysis of the common concepts used in expert descriptions of privacy and IDM scenarios during the above exercise and in discussions within the framework discussions. The relationships defined by the ranges, domains and allowed attributes are also based on those most commonly used in the descriptions collected.

This method of defining concepts is chosen because it provides not only definitions for concepts but also describes the context of its use, its relationships to other concepts, sources for definitions and definition by example. These are all important in understanding the real meaning-in-context of the concepts. This will also be useful in incorporating the concepts into an eventual top-level ontology.

The terms are divided into three categories:

- *Concepts* are classes which can be abstract (e.g. privacy) or instantiateable (e.g. data);
- *Actions* can be carried out on these and other concepts (e.g. process);
- *Properties* of those concepts (e.g. anonymous).

The aim of this text is to convey not only a definition of each term in isolation, but also its relationships to other terms, and its context within the domain. For each term, we therefore give all or some of:

- *Synonyms* are words with precisely the same meaning;
- *Definitions* (one or more) - these definitions are intended to provide a consensus among all PRIME stakeholders and are not intended to be definitive in any sense;
- *Domains* express who or what can be the subject of an action or property. For example, data controllers can collect data;
- *Ranges* express who or what can be the object of an action or property. For example, “private” can be applied to data but not people;

Privacy and Identity Management for Europe

- *Allowed attributes* express what attributes can be applied to a concept. For example data can be private but not red;
- *Examples of usage*;
- *Subclasses or subproperties*;
- *Notes*.

See 7 for definitions of different concepts, actions and properties.

6.2 *PRIME Models for Users and Metaphors*

6.2.1 Introduction

The following quote from the principles stated in the EC contract for PRIME (Annex 1, p. 7) underlines the importance of developing user interface paradigms that can adequately inform users who are not familiar with IDM terminology and concepts:

“Users need easy and intuitive abstractions of privacy: experience shows that such technology is not directly usable by normal users. Instead, normal users need intuitive metaphors and [user interface] models that hide technicalities like pseudonyms and privacy policies.”

This chapter on Prime Models and Metaphors briefly provides and discusses definitions for the terms conceptual model, mental model and metaphor and discusses the importance of those concepts for HCI design. Moreover, it discusses general design decisions. It then summarises the discussion on proposals for IDM models and metaphors that PRIME participants had at the PRIME kick-off seminar and via a mailing list and at video conferences during the first two months of the project. Furthermore, this chapter explains how it can be tested how various aspects of user interfaces affect users' models of a system.

6.2.2 Discussion of Definitions

6.2.2.1 *Conceptual Models and Mental Models*

In the system-modelling phase, concepts related to the application domain and system domain is put in relation to each other. *Conceptual modelling* is the act where systems developers construct models that are meant to reflect the concepts of the application domain (rather than the data model derived later to implement the desired system). The eventual system should be a correct but also a very detailed implementation of the ideas in the conceptual model.

In the HCI literature one encounters the opinion that the conceptual model is a description of the proposed system which “will be understandable by the user in the manner intended” [44]. It should be noted, however, that this model is consciously developed and is not necessarily the same as the user's model of the final system when it is up and running. A question for PRIME is how users should be made understanding the conceptual model underlying the PRIME prototype. Basing the PRIME prototype on a model of the IDM concepts people already have would not be sufficient because people do not have an elaborate set of IDM concepts.

A *mental model* or, synonymously, a *user's model* is the set of notions a person has about how something works. Usability is tied to the extent to which a user's mental model matches and predicts the action of a system. Ideally, a user interface design matches with a user's mental model.

The phase of conceptual modelling is intended to use concepts relevant to the user, whereas users of the final system might form their own ideas (mental model) about how the system works. From the appearance of layout and content of different screen images, and from experience with different functions and by analogy with similar-looking programs, the users will form – sometimes rather unconsciously – notions about what the system is capable of doing, that is, what a user will be able to

get it to do. Naturally, instructions by more experienced users and descriptions found in instruction manuals also influence users' notions.

In some of the HCI literature "conceptual model" is often used for mental models. What is confusing is that the joining of "conceptual" and "model" is understood in two different ways: either as something "conceptual", that is, mental and non-physical; or as a model of concepts (concepts relevant to the application area for a proposed system) while the model itself is a concrete thing, for instance a diagram. To avoid confusion, "conceptual model" should not be used as synonymous to "mental model".

Likewise, "mental model" is just a label of people's "knowledge of how to use the system and, to a lesser extent, how the system works" [44]. For this reason it may be unwise to speak of "designing the mental model". System developers can only indirectly influence the user's model. The model grows with growing experience: "The more someone learns about a system and how it functions, the more his/her mental model develops" (ibid. Reference is here being made to an introductory but comprehensive text book in HCI by Preece et al [44]. It should be noted, though, that this book does not manage to discuss "user's model" and "mental model" on the same pages. Thus, the field is open for confusion even within the frames of a single book on HCI!).

IDM-models for users who are not familiar to IDM can be called "conceptual models for users", or "IDM-models for end-users", or "user interface paradigms", etc., while "user models" is a term which look confusing like "user's model" and should be avoided.

6.2.2.2 *Metaphors*

For user interface design one often speaks of basing it on metaphors. When building an interface on a metaphor, designers use a vocabulary and a graphical language which are supposed to be familiar and perhaps even entertaining to the user. In popular design belief, one gathers images of objects from the application domain and put them on the computer screen in order to let users understand the systems' functions or at least to let them figuring out how to successfully perform tasks.

However, such a design could have several drawbacks because it locks the solutions of interaction paradigms in ways which are not optimal [45]. Moreover, one should realise that nowadays almost every strand of life is computerised. Thus, trying to represent system functions by taking pictures of what reality looks like for users would just fill the computer screen with a lot of pictures of computers.

On the other hand, for the purposes of PRIME, complex concepts have to be illustrated. Such illustrations can take on traits typical of metaphors: in parallel to figurative speech, such illustrations may contain elements borrowed from other sources than the illustrated domain.

Whether one should use the word "metaphor" or simply the word "illustration" is a matter of choice. On the other hand, when it comes to illustrations/symbols on buttons and page headings, the word "icons" should be used, whilst "metaphor" should be used when describing an icon if it is indeed motivated by some sort of metaphoric allusion.

One should further note that graphical metaphors make it possible to refer to individual elements by words, which denotes the things depicted. Thus, a graphical metaphor entails a verbal metaphor. Verbal metaphors could of course be used also without illustrations. To the problem of making terms intelligible to broad user groups comes the problem providing precise formulation so that users are well-informed in legal terms. Can a service provider rightfully claim that the user has given his/her informed consent if the service provider has used metaphoric explanations?

In HCI there was once a strong emphasis on the need for consistent *global metaphors*. A global metaphor is a single, overarching metaphor that provides a framework for all the other metaphors in the system [45]. A metaphor at OS level should be used also in individual programs. There have been arguments against this as noted above because it locks the solutions of interaction paradigms in ways which are not optimal. One can also observe that users seldom have difficulties with metaphor breaches when such cracks take the form of clearly visible and identifiable objects (in the same way that, for instance, the function of a telephone is not incomprehensible in a kitchen precisely because it does not look like a cooking appliance).

Privacy and Identity Management for Europe

Breaches with a global metaphor might be found in illustrations used in various sorts of help functions.

Three broad categories of user-invoked help functions can be discussed:

- There could be general introductions to IDM in form of tutorial material such as provided by PRIME Activity 13 “Education” addressing the need for educational material;
- There could be help buttons in the user interface to aid the user at specific points;
- There could be specific links from words known to be problematic for users, as used by the Karlstad group in previous mock-up designs and testing for privacy protocols on mobile devices.

Explanations in these three types of help functions can elaborate parables necessary for illuminating the concepts. This may include illustrations which, as already noted, may borrow elements from other sources than the illustrated domain (this domain may be rather abstract). There is no reason to strive for a coherent source domain for the illustrations because these are encountered at different instances by the user and the most important requirement is that they function efficiently where they are supposed to appear.

Another argument against global metaphors (or global themes of illustrations) is that illustrations should reflect users’ mental models of each application area. Such illustrations may thus have to be specific for each area to make sense. On the other hand, for the user to be able to carry over experiences of electronic IDM from one area to another, there should be easily identifiable elements representing common functions, but to what extent they have to be standardised and whether such elements should be pictures or words will have to be decided when more elaborated application scenarios have been developed. Cross-linguistic considerations have also been taken into account.

A problem with the consistency of the user interface might occur if users can personalise the user interface metaphors. Personal settings do not show up if one uses someone else’s browser. But this is not specific for the metaphorical part but for all other settings as well and thus has to be dealt with at that level.

A further issue of homogenising the user interface is how to adapt the user interface (whether application- and user-specific or not) to various devices such as computer screens and mobile phone displays. The goal is a user interface model, which will be perceived by users as ‘the same’ across different devices. Ambient technologies (see section 4.6) might need access via standard devices such as mobile phones for people to be able to check privacy protection modes.

6.2.3 Examples for IDM Models and Metaphors

This section provides some examples for IDM models and metaphors, especially graphical metaphors. The discussion is still ongoing and ideas still have to be further elaborated.

Graphical metaphors for IDM, especially for IDM protecting informational privacy, could be used to illustrate different perspectives. They could illustrate how users want their data to be handled, e.g. to choose different levels of privacy preferences. Potentially, they could also be used to illustrate service providers’ demand for personal information. The latter perspective has not been discussed so far within the project. Even for the first perspective there are many alternatives.

6.2.3.1 House Metaphor

Andreas Pfitzmann has presented a classification of “Data Protection Models” that users have:

- Model of Sphere (intimate, private, public);
- Model of Mosaic (pieces are not sensitive, but large sets are);
- Models of Roles (personal data is bound to a context, i.e. role).

and how those models are influencing the user's Internet habitudes, and what metaphors could be used for those data protection models. Especially the Model of Sphere and possible metaphors, such as a house metaphor or virtual residence metaphor (see also [46]) has so far been discussed within the PRIME group.

Graphical metaphors for privacy protection could draw upon the aspect of *hiding* the user's information (choosing the level of protection, i.e. Model of Sphere). A jalousie that could be set to different degrees of transparency could conduct the notions of various degrees of anonymity (an anthropomorphic figure could be placed behind the jalousie to signify the user himself).

To illustrate that the user should not only set different degrees of transparency of his/her personally identifiable information but also that different kinds of information may be revealed to different service providers, a house metaphor could be used where the different sorts of information are stored in different rooms where jalousies or shutters are used to conceal them.

If the various rooms of this house are meant to symbolise different pieces of information about oneself, a user could enter the 'values' of the different rooms while any default-setting would perhaps be easily demonstrated by illustrative graphics in the rooms. For different 'roles' (that is, in different situations), different patterns of open and closed shutters would be shown in the user interface.

The question then is whether the rooms metaphor has any good extensions. Should medical information be gathered in the bathroom? In such a case, do we need only one bathroom?

Furthermore, it should be evaluated how this use of a house metaphor reflects degrees of anonymity of a user. IDM is about the identification of persons while the house just stands there, easily located = easily identified as an individual entity. This relates to another pertinent question, namely how does the user recognise her/himself in a graphical metaphor?

For the house metaphor, users could be provided with means to shape the building to some extent to make them regard the house as their personal belongings. On the other hand, this might make them dependent on the same browser to feel 'at home'. If the interior of a house were used instead, "going to" different rooms would more clearly identify where the user is now. However, then there are no shutters to rely on. Instead one could potentially utilize the different functions of the rooms of an ordinary house or flat: bathroom for privacy, living room for information you reveal to close friends, the street outside for information that you allow to be public. However, for the residence metaphor one has to find ways of illustrating the intended *direction* of increased privacy. The bathroom was discussed as the most private place. Some users might misinterpret the bathroom as the place where you show all your personal information, because in a bathroom you may be naked. While in the living room and on the street you will use an increasing amount of clothes – to protect your privacy. Such an interpretation runs directly counter to the one intended. Similarly, the jalousie model with an anthropomorphic 'place-holder' for the user behind the jalousie, as suggested above, could potentially be interpreted as someone watching the user rather than as the user hiding himself.

6.2.3.2 Mask Metaphor

A mask metaphor probably provides a conceptual model that is easier to understand. If there is no-one behind a mask, it is the user who is supposed to be wearing it. The masks could be used for the concept of anonymity as well as for the concept of pseudonyms – the latter by showing masks with detailed faces. There is a possibility to draw upon the kind of stylised or standard characters used in Greek drama and Italian commedia dell'arte. Perhaps masks could be used also in illustrations explaining IDM concepts where one would need to stylise different actors such as "attackers".

John Borking enclosed for discussion a picture with masks that has been used at the Dutch data Protection Authority to explain the identity protector (see Figure 6).

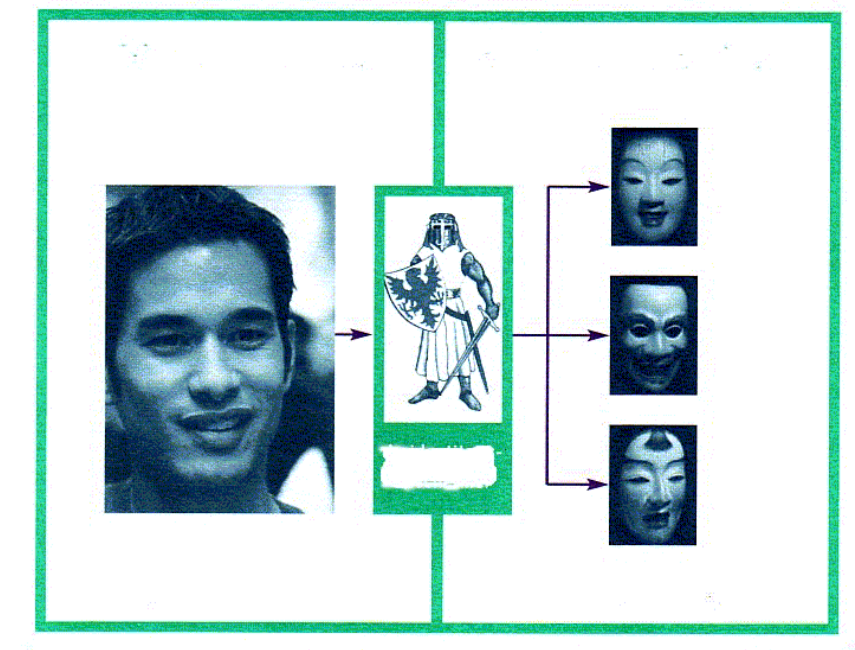


Figure 6 Identity Protector illustrated through masks.

6.2.3.3 Roles

Shutters, rooms, or masks, they all allow the user to do pre-defined settings and then select among the various settings for specific occasions. This can be expressed as defining and selecting different “roles” (thus neglecting for the purpose of simplicity other ways of defining roles).

For user interfaces, icons illustrating different roles can draw on jalousies or masks, but experiments together with users can show how they prefer to put icons on their different roles. They might prefer purely mnemotechnical symbols relevant for each individual role they create but with no coherent semantic structure (i.e., no consistent “metaphor”) relating the symbols to each other. This might however not be a drawback (cf. the section above on “global metaphor”). Thus, allowing the users to select mnemonic icons for specific privacy settings will not make the user interface unusable even if we lose the ability to teach the user via the icon.

Investigating how roles are defined and illustrated in relation to application areas will make the discussion on User Interface (UI) design for IDM more informed.

6.2.3.4 Bank Account

A “Bank Account” is something virtual but yet has a very strong meaning to most people. If you do not want your data to be transmitted to any third parties, you could talk about “depositing it” in an account with a certain company. There are also “holding accounts” where money is kept temporarily before being transferred, which could be used as a metaphor for a company which will hold your data before transferring it to a third party.

6.2.3.5 Graphical User Interfaces built on using Arbitrary Symbols: Colourful Birds

Using more arbitrary symbols than, for instance, the house metaphor discussed above have certain advantages. People have different experience of bathrooms, bank accounts etc. and they will consequently have different intuition about the elements of the metaphor. Moreover, it might not be possible to put all the IDM functions into easily understandable graphical metaphors.

A more abstract conceptual model could be based on the idea of the AT&T Privacy Bird²¹. The Privacy Bird constitutes an interesting example using shape, colour, and sound, and it also highlights the possibility to use a different graphical approach in browsing mode than in the setting mode (where no icons are used). The Privacy Bird software puts a little bird in the tool bar of the Internet browser. This bird shifts colour if web sites' privacy policies deviates from the one preferred by the user. Signalling is also done by displaying a speech bubble adjacent to the bird and by sound.

For PRIME-based systems, a library of birds could be connected to pseudonyms and could be mixed with a palette of colours which are used to show the status/risks of an operation.

6.2.3.6 Multi-layered Metaphors; Town Metaphor

However, it has been noted that metaphors, such as the colourful bird or the bank account metaphor, would not be sufficient, because they are not rich enough to define roles. In choosing roles, there are many ways to proceed.

One could potentially elaborate a "town" metaphor where multilateral security can be demonstrated. An initial set of requirements may be in conflict with others' requirements, and thus negotiations will also be needed. Also selecting contradicting roles should be possible, and it might be useful to elaborate a "social role" concept.

Different layers of paradigms will be needed:

- One layer allowing conflicts (conflicting wishes, conflicting interests within one user);
- One layer for the concrete system (without conflicts).

A town metaphor with one avatar can be used to show a consistent set of wishes, while inserting a few avatars might be a way to express conflicting interests. PRIME participants from TU Dresden and ICPP are currently working on a proposal for a Town Map with places for avatars defining roles for the user. In a generic town, what places represent what?

6.2.4 Testing to Derive and Develop Models that are Intuitive to Users

How do we infer what mental models people have of identity management in general or of a specific IDM system?

Testing of user interfaces in order to develop them may be carried out in several ways. Testing is here understood to involve prospective users. When it comes to testing the intelligibility of terms used for IDM, lots of information can be gathered even without using computer screens or displays of mobile phones. Questionnaires can provide information on how well people understand words, phrases, texts, and illustrations. Because the concepts behind IDM are not well understood by many users, the terminology will have to be tested as will also explanations of various terms because the user interface should provide explanations of difficult terms and concepts (explanations may contain, or be based on, pictures as discussed earlier).

It should be noted that open questions and interviews are a way not only to evaluate certain terminologies or set of icons, but also a way of getting people to explain things so that their conception of things (their "mental models") can be inferred. More indirect ways of inference are to observe users during IDM use and by analysing task completion in user tests.

Furthermore, post-usability test interviews with the test subjects will provide much information on why they did this or that. In this way designers can get a glimpse into user's "mental models", whilst pure performance tests do not tell us if the user really understood the consequences of how he/she gave away information to various services used in the test. When the designers infer a user's understanding / conception / mental model of a subject, it can be described in words or by diagrams relating concepts to each other just like in conceptual modelling.

²¹ <http://privacybird.com>

7 Conclusions and Outlook

The PRIME Framework V0 presented in this document provides the initial holistic view and knowledge of the PRIME project partners on Privacy and Identity Management. During the first phase of the PRIME project, interdisciplinary discussion groups have been formed to elaborate this initial version of the PRIME Framework.

The Framework V0 defines the vision of the project shared by the project participants, identifies the stakeholders of the project as well as their roles and responsibilities, discusses basic terminology, concepts and HCI models and metaphors for privacy-enhanced identity management, and integrates the legal, socio-economic and application-specific views on privacy-enhancing identity management. Besides, it identifies issues that need to be addressed by the various disciplines within the project. The application specific view is illustrated by a set of application scenarios, where for each scenario the status quo of the application domain is briefly presented, privacy problems and requirements are discussed and the vision of a PRIME-based solution is outlined that takes those requirements into consideration.

This initial holistic view on the project should help to establish common project grounds and to facilitate interdisciplinary exchange and cooperation between project partners and stakeholders.

This initial PRIME Framework describes work in progress and will be further elaborated for the next PRIME Framework versions. In particular, the contributions on terminology and HCI concepts, application scenario descriptions and the chapters on the legal, socio-economic environment of PRIME will be further refined. Whereas the initial Framework presents suggestions for terms and concepts that are still under discussion, the next PRIME Framework V1 will include a refined chapter on PRIME terminology on which there will be consensus within the project consortium. Also all application scenarios listed in Annex 1 of the EC Contract for PRIME should be presented in the next Framework version, i.e. besides the scenarios on LBS and Ambient Intelligence, which are already addressed in this initial Framework document, also application scenarios on e-health, e-learning and flight passenger privacy should be elaborated in cooperation with the application providers. In addition, the technical aspects of PRIME will be further integrated by providing an abstract overview to the initial PRIME architecture that is under development as well as PRIME architecture solutions for all application scenarios.

Appendix A Concepts, Actions and Properties

Publication of this working draft of the concepts does not imply endorsement by the PRIME Membership. This is a draft document and may be updated, replaced or made obsolete by other documents at any time. It is inappropriate to cite this document as other than work in progress.

A.1 Concepts

A.1.1 Access

Definition	Being able to process a piece of data
Domain	Persons, legal persons, applications
Range	Data, own data, personal data
Notes	<p>The term "access" in the sense defined above has two important areas of application within legal documentation on data protection:</p> <ul style="list-style-type: none"> • The ability of a third party to process information about a person against their will – as used in phrases such as "I do not want NastyCorp to have access to my data"; • The ability of a person to alter information held about her/his by another party in order to control its accuracy – as used in phrases such as "I want to be able to access my data after I have submitted it". <p>Note that processing includes viewing, knowing, acting upon or altering data</p>

A.1.2 Anonymity

Definition	<p>I. Anonymity is the state of being not identifiable within a set of subjects, the anonymity set²²</p> <p>II. Anonymity is the degree to which an identifier is not identifiable within a set of names (or pseudonyms), the anonymity set²³</p>
Notes	The anonymity set is the set of all possible subjects

A.1.3 Credential

Definition	<p>I. Evidence or testimonials concerning rights to actions or reputation (credentials can also allow access)</p> <p>II. A minimal assured identity which identifies a person as having a right to an action or reputation</p>
Examples	A token authorising a person to access a sports centre must only identify him as a person who has paid a subscription fee (an anonymity set of several

²² http://freehaven.net/anonbib/papers/Anon_Terminology_v0.14.pdf.

²³ Giles Hogben, based on http://cybersecurity.jrc.it/Datapublication/Ontheontologyofidentification_giles_hogben2.pdf - see notes on "identify".

	<p>hundred) and perhaps who has a minimum state of health as attested by a medical certificate.</p> <p>The new ambassador presented her credentials to the president</p>
Notes	<p>As a credential is essentially a set of assured attributes about a person, it also corresponds to an identity in the sense that it identifies the person as belonging to the group of people who have the right to a certain action.</p> <p>The classical model of authorisation grants access to services through user names and passwords. Attributes that are linked to a user name and a password verify whether the user is authorized. Often however, this data is not actually required to carry out the service. Its request can therefore contradict the principle of data minimisation set out in the EU Data Protection Directive article 6, whereby data should be “adequate, relevant and not excessive in relation to the purposes”. Therefore recent developments in privacy enhancing technologies have emphasised the use of credentials, which are certified, minimal facts required to use a service. E.g. to buy duty free goods in an EU airport shop, the required information is an assurance that I am a bona fide passenger travelling from the EU to the US, not as is current requested all the data contained in a boarding card. In terms of our model, a credential is a minimum set of facts, certified by some trusted means, for the provision of a given service</p>

A.1.4 Data

Definition	<p>I. A collection of assertions from which inferences can be drawn</p> <p>II. A sequence of symbols</p>
Allowed Attributes	Personal, sensitive

A.1.5 Data Subject

Definition	Identified or identifiable natural person (See Directive 95/46/EC)
-------------------	--

A.1.6 Data Controller

Definition	The legal or natural person or entity defined to be responsible for a data processing act
-------------------	---

A.1.7 Identifier

Definition	<p>I. A symbol or a set of symbols which refers to a concept allowing to distinguish it from others (reference is defined by the semantic model theory used)</p> <p>II. A name which is imposed by a third party</p>
Synonyms	Name, label, nym
Sub-classes	Pseudonym, synonym, alias, unique identifier (to be defined in later draft)

A.1.8 Identity

Definition	<p>I. A set of assertions which identifies an identifier (a name) among others in a set. Although this seems circular, note that we give a specific (non circular) definition to the term "identifier".</p> <p>II. External presentation of a self</p>
Synonyms	Persona
Possible Actions	Steal, fake, create, falsify (add untrue facts)
Subclasses	Unique identity, digital identity
Example	<p>-With the following prior knowledge: F1:"Mickey Mouse owns a Harley Davidson"; F2:"John Smith doesn't own a motorbike"; F3: "X doesn't own a motorbike".</p> <p>The assertion: F3:"A Harley Davidson is a motorbike".</p> <p>This constitutes an IDENTITY of X among X, Mickey Mouse and John Smith (because it identifies it)</p>
Notes	The concept of THE identity of a person not so useful as a concept because everyone has an infinite number of identities

A.1.9 Identity Management

Definition	Identity management subsumes all functionality that supports the use of multiple identities, by the identity owners (user-side IDM) and by those parties with whom the owners interact (services-side IDM)
-------------------	--

A.1.10 Information

Definition	<p>I. Something that allows us to reduce the number of states a system may be in (Shannon)</p> <p>II. Often used synonymously with Data</p> <p>III. A set of assertions</p>
Possible Actions	Reveal, sell ,misuse ,alter, aggregate ,link, bind, abuse, leak, flow, transfer, share, reveal, disclose, retrieve, delete, merge, aggregate
Allowed Attributes	Personal, aggregate, sensitive, integrity, intimate, true, false, complete, incomplete, missing, misleading, public, general, hidden, specific
Notes	The difference between Data and Information is perhaps that Data is the physical manifestation of Information. Data does not provide information unless it is interpreted

A.1.11 Personally Identifiable Information

Definition	Any set of assertions which identifies a person to any degree
Notes	Sometimes referred to with the acronym PII

A.1.12 Privacy

A.1.12.1 Informational Privacy

Definition	Control over what information is known about a human person Privacy is the power to selectively reveal oneself to the world." Eric Hughes, A Cypherpunk's Manifesto Control of a personal identity
-------------------	--

A.1.12.2 Spatial Privacy

Definition	Control over what is presented to your senses (subject to a set of rights) Example: Things which violate spatial privacy are anything from Spam to a neighbour cooking curry at night. Notes: Personal space in this context is not yet a well-defined notion legally speaking (it is hoped that Prime will shed some light on this). Clearly however, every person should have certain rights over what is presented to their senses. For example if a satellite TV company were to install a TV which cannot be switched off and which plays non-stop advertising in a person's home, this would be considered a definite violation of personal informational space, even though there would be no physical violation. More contentious issues concern advertising in more public places. For example, should it be considered a violation of personal informational space to put TVs with advertising on them in queues for essential services such as benefits, or healthcare? Another example, which is already happening, is the use of television screens to advertise to "captive audiences" in hospital beds. The other end of the spectrum would be if a person enters someone else's home, they clearly have no right for example to claim that music or advertising should not be played if it is chosen by the owner of the home. This links to the control of personal information where personal space is being invaded with content which has been tailored to target a given person, using previously collected personal information
-------------------	---

A.1.13 Private Space

Definition	Legally defined but flexible space where a person has special rights e.g. to remain unsensed, uninvaded, and to perform certain actions they could not perform outside that space
Synonyms	Private sphere, home?
Examples	The home where people can have sex, have the right to silence, freedom from advertising. The car - where law enforcement can photograph you, you can't be naked, etc.
Possible Actions	Invade, protect, eavesdrop
Notes	A physical human person's private space could be seen as that space extending around the person's body where sensory events are sensed by that person alone. This definition could be extended to cover groups of persons

A.1.14 Profile

Definition	Collection of assertions (true or untrue facts) including behaviours collected with the intention of identifying a person or group of persons
Synonyms	Trace, partial identity
Possible Actions	Link, build, own, reveal, combine

A.1.15 Pseudonym

Definition	<ul style="list-style-type: none"> I. An identifier of a person or set of persons II. An identifier of a person or set of persons, chosen by the person or group III. An identifier of a subject or set of subjects which is used in contexts where a person does not wish its identity with official names to be known
Notes	There has been a discussion on whether a pseudonym can mean any type of identifier. The problem is the connotation this holds due to its linguistic roots

A.1.16 Trust

Definition	<ul style="list-style-type: none"> I. Positive expectation of future behaviour based on past experience II. Intention to accept vulnerability based upon positive expectations of the intentions or behaviour of another
Synonyms	Confidence
Domain	Legal persons
Range	Legal persons, applications, entities including 3rd parties, systems/machines
Example	<p>Alice trusts Bob to pay him \$10 when he/she has received the goods.</p> <p>Alice trusts Bob to give her a nice surprise on her birthday</p> <p>Alice trusts Bob not to crash her car</p>
Notes	<p>Trust does not necessarily have to do with predictability as an artist for example may be trusted to come up with something original, however something can fulfil expectations (e.g. originality) without being predictable.</p> <p>When ‘trust’ is applied in an online business context, these expectations include: a technological basis, a contractual side and customers’ image built up via previous interactions with a company, brand image, publicity, etc.</p> <p>Entities typically trust – or do not trust- each other to fulfil selected obligations or for a particular purpose rather than for everything</p>

A.2 Actions

A.2.1 Authenticate

Definition	To establish confidence in the truth of some claim
Notes	The claim could be any declarative statement about an identity or about its attributes – for example: “this individual’s name is Neil Morrison” or “this web

	<p>surfer with pseudonym name@web.com is over 18 years old".</p> <p>It may or may not be possible to link an authenticated identity to a person; i.e. to identify him/her. For example, verification of the password associated with an account provided by a pseudonym service authenticates an identity (loginname@pseudoweb.com) that may not be possible to link to a specific individual</p>
--	---

A.2.2 Authorise

Definition	To allow an entity to access a service or resource
Notes	Usually conditions are attached to the authorisation which require the identification of the entity requesting access, either uniquely or within a group with a set of credentials

A.2.3 Disclose

Definition	To permit access to data
Synonyms	Reveal

A.2.4 Discriminate

Definition	To change a behaviour which concerns an individual based on information known about them
-------------------	--

A.2.5 Exploit

Definition	To use something beyond the purpose it is intended for
-------------------	--

A.2.6 Identify

Definition	To use a set of assertions to infer that two or more identifiers are identical
Synonyms	Pick out, discriminate?, individuate
Domain	Any intelligent entity
Range	Anything
Example	Identifying someone in an identity parade
Notes	<p>Formally, there are 3 separate layers to semantics, and hence to the process of identification. The first layer is the layer of names and identifiers. For example, food, cibo and essen are all names. Then the second layer is that of concepts. Each identifier is attached by a mechanism known as reference, to a concept. For example, the word, food and the Italian word, cibo each "refer" to the same idea in our minds which makes us salivate whether there is real food in front of us or not. This is the notion of identity – when two names refer to the same concept.</p> <p>This idea is often met with the reaction that identification is the identification of real world entities. In fact there is often a one to one connection between names, concepts and real-world objects (the interpretation) but there is never a real-world object without an intermediary concept. In the online world of personae, this is particularly important because several names such as "vlad_impaler", "fish_001" may refer to the same collection of electronic data</p>

	in the form of chat-room statements, cellphone calls, etc..., but several conceptual collections of electronic data etc... may be produced by the same real-world person. Hence it is important to distinguish between online personae and real-world instances of these personae.
--	--

A.2.7 Impinge

Definition	Impinge ON - to enter a person's senses against their will
Synonyms	Invade
Allowed Range	Private space

A.2.8 Link

Definition	To establish that the references of two or more identifiers are identical ²⁴
-------------------	---

A.2.9 Process

Definition	To view, know, act upon or alter data
Synonyms	Collect
Range	Data

A.2.10 Trace

Definition	To establish facts about the history of a individual
-------------------	--

A.2.11 Track

Definition	To establish the physical path followed by a person or object
-------------------	---

A.3 Properties

A.3.1 Anonymous

Definition	Not identifiable within a group
-------------------	---------------------------------

A.3.2 Informed

Definition	Aware of some important information
-------------------	-------------------------------------

A.3.3 Identified

Definition	IDENTIFICATION for a given Identifier, P, occurs when, based on a new set of FACTs the number of identifiers in the anonymity set that P could be identical to decreases
Synonyms	Linked

²⁴ See http://cybersecurity.jrc.it/Datapublication/Ontheontologyofidentification_giles_hogben2.pdf.

Examples	<p>Given a fingerprint blob (binary data), attached to the arbitrary identifier XX1, if this blob matches J Smith's fingerprint file, then XX1 is identified among all human beings as being identical to J Smith</p> <p>Given a DNA blob (binary data) attached to the arbitrary identifier XX2, if this blob matches John Smith's DNA blob where John Smith is a twin, then XX1 is identified half as much as in the previous example because XX1 could be any of two of the set of all human beings</p>
Notes	Unique identification is when the identifier could only be identical to one of the anonymity set

A.3.4 Identical

Definition	Having all possible properties in common
Notes	Formally this can be expressed by Leibniz' Rule: $N1 == N2$ iff $(\text{forAll}F)(F(N1) \leftrightarrow F(N2))$

A.3.5 Minimised

Definition	Containing no more information than necessary for a given purpose
Range	Data, information

A.3.6 Pseudonymous

Definition	Having a certain degree of unlinkability, i.e. not uniquely identified
-------------------	--

A.3.7 Relevant

Definition	May have implications for a certain purpose
Range	Purpose

A.3.8 Sensitive

Definition	<ol style="list-style-type: none"> I. May be used to infringe a service requester's fundamental rights II. Belonging to a special category of personal data that touches upon the private sphere of an individual III. Belonging to a special category of personal data which individuals on average prefer to be known only to a few selected others
Range	Data, Information

A.3.9 Transparent

Definition	Easily understood by the persons it is aimed at and unambiguous
Range	Policy

A.3.10 Trusted

Definition	Expected to behave in the expected manner for the intended purpose
-------------------	--

Range	System, person, application
Notes	"Trusted" describes the dynamic, subjective aspect of trustability (e.g. the software state of a platform, whether it has been corrupted by a virus, etc.)

A.3.11 Trustworthy

Definition	Capable of behaving correctly i.e. trustworthy in a commonly agreed sense
Synonyms	Trustable
Range	System, person, application
Notes	Trustworthy describes the social side of trust. For example, you would want to use social mechanisms (via certification, etc.) to be able to determine whether a system should be trusted (e.g. are the correct protocols in place, is the hardware operating as expected, etc.?)

A.3.12 Unlinkable

Definition	Unlinkability of two or more items (e.g., subjects, messages, events, actions, etc) means that within a given system, these items are no more and no less related than they are related concerning the a-priori knowledge ²⁵
-------------------	---

A.3.13 Unobservable

Definition	In a maximum state of anonymity (Discussion Group) Unobservability is the state of IOIs (items of interest) being indistinguishable from any IOI at all. This means that messages are not discernible from "random noise" ²⁶ .
Subproperties	Sender unobservable: then means that it is not noticeable whether any sender within the unobservability set sends. Recipient unobservable then means that it is not noticeable whether any recipient within the unobservability set receives

²⁵ http://freehaven.net/anonbib/papers/Anon_Terminology_v0.14.pdf.

²⁶ http://freehaven.net/anonbib/papers/Anon_Terminology_v0.14.pdf.

References

- [1] Merriam Webster Online Dictionary; <http://www.m-w.com>.
- [2] Sinclair, J. (ed.), Collins, C., "English Dictionary for Advanced Learners", HarperCollins Publisher, 2001.
- [3] Chaum, D, Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms, Communications of the ACM, 24 (2), pp. 84-88, 1981.
- [4] Chaum, D, Security without Identification: Transaction Systems to Make Big Brother Obsolete, Communications of the ACM, 28 (10), pp.1030-1044, 1985.
- [5] Pfitzmann, B., Waidner, M., Pfitzmann, A., Rechtssicherheit trotz Anonymität in offenen digitalen Systemen; Computer und Recht 3/10, pp. 11, 12, 712-717, 796-803, 898-904, 1987.
- [6] Lacoste, G.; Pfitzmann, B.; Steiner, M.; Waidner, M., SEMPER - Secure Electronic Marketplace for Europe, LNCS 1854, Springer-Verlag, Berlin, 2000, <http://www.semper.org>.
- [7] Registratiekamer & Information and Privacy Commissioner/Ontario, Privacy-Enhancing Technologies: The Path to Anonymity, Volumes I, Achtergrondstudies en Verkenningen 5B, Rijswijk, 1995.
- [8] Registratiekamer, Privacy-Enhancing Technologies: The Path to Anonymity, Volumes II, Achtergrondstudies en Verkenningen 5B, Rijswijk, 1995.
- [9] Rannenberg, K., Multilateral Security- A Concept and Examples for Balanced Security, pp. 151-162 in: Proceedings of the 9th ACM New Security Paradigms Workshop 2000, Cork, Ireland; ACM Press, September 19-21 2000.
- [10] The Open Group, Identity Management White Paper by Skip Slone & The Open Group Identity Management Work Area, <http://www.opengroup.org/products/publications/catalog/w041.htm>.
- [11] Identity Management Systems, (IMS), Identification and Comparison Study, Independent Centre for Privacy Protection (ICPP) and Studio Notarile Genghini (SNG), http://www.datenschutzzentrum.de/idmanage/study/ICPP_SNG_IMS-Study.pdf.
- [12] European Association for the Co-ordination of Consumer Representation in Standardisation; ANEC 2003, August 2003; <http://www.anec.org/attachments/it008-03rev.pdf>.
- [13] Camponovo, G., Mobile Commerce Business Models, in: eBusiness Models: International workshop on business models Lausanne, Switzerland, 4-5 October 2002.
- [14] Telia FriendFinder, <http://trainingcenter.telia.se/articles/00/00/5c/47/01/>.
- [15] Rannenberg, K., How much negotiation and details can users handle? Experiences with security negotiation and the granularity of access control in communications, Computer Security - ESORICS 2000, Proceedings of the 6th European symposium on Research in computer Security, Toulouse/France, October 2000.
- [16] Figge, Stefan, Gregor Schrott, 3G "ad" Work - 3G'S Breakthrough with mobile Advertising. In: Proceedings of the 8th International Workshop on Mobile Multimedia Communications; Munich, 2003.
- [17] Barker, Garry, I spy with my little mobile, The Age, <http://www.theage.com.au/articles/2003/12/05/1070351787829.html>, December 2003.
- [18] Fritsch, L.; Rannenberg, K., Informationstechnische Voraussetzungen von E-Government am Beispiel des Katastrophenschutzes mittels Mobilkommunikation ;in: Tagungsband zur Jahrestagung 2002 der Deutschen Gesellschaft für Recht und Informatik, Otto-Schmidt-Verlag; Köln, 2001.
- [19] Big Brother Award 2002, <http://www.bigbrotherawards.de/en/2002/>.
- [20] Viseu, A., Clement, A., Aspinall, J., Situating Privacy Online: Complex Perceptions and Everyday Practices, Information, Communication & Society, Vol.7, No.1, Taylor & Francis Ltd., pp.92-114, March 2004,
- [21] Smink, G.C., Hamstra, A.M, van Dijk, H.M, Privacybeleving van burgers in de informatiemaatschappij, report commissioned by the Dutch Platform for Science and Ethics, The Hague, 1999.
- [22] Gellman, R., Does Privacy Law Work?, Agre, P.E., Rotenberg, M., (eds.) Technology and Privacy: The New Landscape, 2001 (Third Printing), The MIT Press, Cambridge, MA/London, pp.193-218, 2001.
- [23] Bennet, C.J., Raab, CD., The Governance of Privacy: Policy Instruments in Global Perspective, Ashgate, Aldershot, 2003.

- [24] Schoeman, F.D. (ed.), *Philosophical Dimensions of Privacy: An Anthology*, Cambridge University Press, Cambridge, UK, 1984.
- [25] Lyon, D., *Surveillance Society: Monitoring Everyday Life*, Open University Press, Buckingham, UK, 2001.
- [26] Vedder, A.H., Blok, P., *Privacy en ICT*, A.M.B. Lips, Bekkers, V.J.J.M., Zuurmond, A. (eds.), *ICT en Openbaar Bestuur. Implicaties en uitdagingen van technologische toepassingen voor de overheid*, Lemma, Utrecht, 2004, forthcoming.
- [27] Solove, D.J., *Conceptualizing Privacy*, *California Law Review*, Vol. 90, No.4, pp.1087-1155, 2002.
- [28] Burkert, H., *Privacy-Enhancing Technologies: Typology, Critique, Vision*, Agre P.E., Rotenberg, M. (eds.) *Technology and Privacy: The New Landscape*, 2001 (Third Printing), The MIT Press, Cambridge, MA/London, pp.125-142, 2001.
- [29] Prins, J.E.J., de Vries, M., *ID or not to be? Naar een doordacht stelsel voor digitale identificatie*, Rathenau Institute, The Hague, Werkdocument 91, April 2003.
- [30] Godin, S., *Permission Marketing - Turning Strangers Into Friends And Friends Into Customers*, Simon & Schuster, 1999.
- [31] Gauthronet S, Drouard E., *Commission of the European Communities (2002) Unsolicited Commercial Communications and Data Protection*. ETD/99/B5-3000/E/96, January 2001.
- [32] U.S. Federal Trade Commission, *Privacy Online: Fair Information Practices in the Electronic Marketplace: A Federal Trade Commission Report to Congress*, May 2000.
- [33] Hahn, R., *The Benefits and Costs Of Online Privacy Legislation*, AEI-Brookings Joint Center Working Paper No. 01-14, October 2001, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=292649.
- [34] Gellman, R., *Privacy, Consumers, and Costs: How the Lack of Privacy Costs Consumers and Why Business Studies of Privacy Costs are Biased and Incomplete*, *Digital Media Forum Report*, March 2002, <http://www.epic.org/reports/dmfprivacy.pdf>.
- [35] Miyoshi, K., Chih-ming H., *Calculating the Cost of Privacy*, Final Report for MGT 565B, Digital Strategy Project, Owen Graduate School of Management, Vanderbilt University, http://elab.vanderbilt.edu/research/papers/pdf/student_projects/Calculating%20the%20Cost%20of%20Privacy%20-%20Final%20Report.pdf.
- [36] Backhouse, J, Hsu, C, Baptista and J, Tseng J. C., "The key to trust? Signalling quality in the PKI market", 11th European Conference on Information Systems, Naples, Italy, 19-21 June, 2003.
- [37] Backhouse, J, Hsu, C, Tseng J. C. and Baptista J, (forthcoming) "A Question of Trust – An economic perspective on Quality Standards in the Certification Services Market", *Communications of the ACM*.
- [38] Kaul, I., *Governing Global Public Goods In A Multi-Actor World: The Role Of The United Nations*, Thakur, R., Newman, E. (eds), *New Millennium, New Perspectives: The United Nations, Security and Governance*, United Nations University, New York, pp. 296-315, 2000.
- [39] Coase, R.H., *The problem of social cost*. *Journal of Law and Economics* Vol. 3, pp. 1-44, October 1960.
- [40] Sholtz, P., *Transaction Costs and the Social Cost of Online Privacy*, *First Monday* Volume 6, Number 5, 7 May 2001.
- [41] Laudon, K.C., *Markets and Privacy*, *Communications of the ACM*, Vol. 39, No. 9, September 1996.
- [42] Bergkamp, L., *EU Data Protection - The Privacy Fallacy: Adverse Effects of Europe's Data Protection Policy In An Information-Driven Economy*, *Computer Law & Security Report* Vol. 18 no. 1, 2002.
- [43] Feigenbaum, J., Freedman, M., Sander, T., Shostack, M., *Economic Barriers to the Deployment of Existing Privacy Technology*, *Workshop on Economics and Information Security*, Berkeley CA, May 2002.
- [44] Preece, J, Rogers, Y., Sharp, H., *Interaction Design. Beyond Human-Computer Interaction*, Wiley, 2002.
- [45] Cooper, A., Reimann, *About Face 2.0. The Essentials of Interface Design*, Wiley, 2003.
- [46] Hansen, M., Berlich, P., *Identity Management Systems: Gateway and Guardian for Virtual Residences*, EMTEL 2003.