PRivacy **E**nabled **C**apability **I**n Co-**O**perative Systems and **S**afety **A**pplications

Deliverable 11

Guidelines for Privacy Aware Cooperative Application

Project:	PRECIOSA
Project Number:	IST-224201
Deliverable:	D11
Title:	Guidelines for Privacy Aware Cooperative Application
Version:	v1.2
Confidentiality:	Public
Editors:	Antonio Kung, Barbara Raither (Trialog), Martin Kost (UBER)
Date:	3 Marc 2011

SEVENTH FRAMEWORK PROGRAMME

Part of the Seventh Framework Programme
Funded by the EC - DG INFSO

Document History

Version	Status	Author	Date
V0.1	initial input	Antonio Kung (Trialog)	24 Nov 2009
V0.2	Updated input	Antonio Kung (Trialog) Martin Kost (UBER)	3 Feb 2010
V0.3	Structure of document	Antonio Kung (Trialog) Martin Kost (UBER)	7 Apr 2010
V0.4	input to sections: Legal perspective Role of EU data protection agency Privacy by design ICO Privacy Assessment Madrid declaration Telematics applications eSecurity report	Barbara Raither	9 Apr 2010
V0.5	input on privacy definitions, nudges, ICO assessment:	Barbara Raither	10 Aug 2010
V0.6	update Acronyms update References update spelling	Barbara Raither	15 Aug 2010
V0.7	more reference updates	Barbara Raither	18 Aug 2010
V0.8	Restructuring Contribution on engineering process	Antonio Kung, Christoph Freytag, Frank Kargl	20 Aug 2010
v0.9	rewrite of sections: Privacy definitions Role of Data Agencies Privacy by Design ITS applications Privacy Nudges	Barbara Raither	28 Aug 2010
v0.9	Reediting of various sections	Antonio Kung	28 Aug 2010
v0.10 BR	update of 3.3.1 & 3.3.2	Barbara Raither	8 Oct 2010
v0.11 MK	sections 5.2.1 & 5.2.2	Martin Kost	23 Oct 2010
v0.12 BR	proofreading	Barbara Raither	24 Oct 2010
v0.13	For internal review	Barbara Raither	27 Oct 2010
v0.14	Revisions added	Martin Kost, Frank Kargl, Florian Schaub	31 Oct 2010
v0.15	Final formatting	Barbara Raither	2 Nov 2010
v1.0	Final	Barbara Raither	8 Nov 2010
v1.1	Adding a remark to privacy by design	Antonio Kung	19 Nov 2010
v1.2	Updated version further to comments from reviewers Scope of document stated more precisely Privacy-by-design is further detailed. (section 4.1) Consideration on costs (section 5.4 added)	Antonio Kung	3 Mar 2011

Table of Contents

List of Figures

1 Executive Summary

The deliverable D11 *Guidelines for Privacy Aware Cooperative Application* sketches a Privacy by Design (PdD) process for Intelligent Transport System (ITS) applications. It first explains the context of privacy in current ICT-based applications by elaborating on the current situation in the Information and Communication Technology (ICT) industry, on the current understanding of privacy, on the current moves undertaken by data protection authorities on Privacy by Design, and on the specific problem of privacy in ITS applications. It then sketches a proposal for a Privacy by Design process and elaborates on the PRECIOSA-specific technology contributions to that process, based on its Privacy-enforcing Runtime Architecture (PeRA). It finally provides a perspective on elements that should be taken into account in the future. The conclusion is that this deliverable is only a starting point to an important undertaking that goes beyond the ITS community, i.e., it should involve the whole ICT community, namely to define and establish a Privacy by Design process within the fields of software and systems engineering.

This deliverable has taken a more global tone than initially planned, i.e., instead of explaining a specific design process based on PRECIOSA technologies, we try to explain a general universal process which could or could not involve PRECIOSA technologies.

2 Introduction

Research and development in the field of Intelligent Transport Systems focuses on the next generation of technology in transportation. Co-operative Systems is the key term which describes a new method for individual travellers equipped with state-of-the-art technology to collaborate with operators of transport systems and service providers. By introducing Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), and Vehicle-to-X (V2X) communication, new potential is opened up to improve safe and ”green” mobility. Such Co-operative Systems are based on mobile and ad-hoc networking. An inevitable prerequisite for deploying these new systems is the availability of secure and safe communication, since Co-operative Systems handle user location and identification information. Some core functions in Co-operative Systems need to identify traveller movements, for example to draw conclusions about the traffic status. These systems also need to authenticate a user’s identity for tasks such as granting access to services in such systems.

Consequently, questions of privacy are inherently connected to Co-operative ITS, whether it be for public or private services or basic system functions. The requirements of observing location patterns on one hand, but assuring privacy and especially location privacy on the other hand seem contradictory.

Co-operative Systems consist of mobile entities (vehicles) which create, process, and share information. Communication happens in a V2X manner, i.e., between vehicles (V2V) or between vehicles and the associated infrastructure (V2I). In the V2I case, information flows via roadside units (RSU) of cellular networks to backend systems. Vehicles, RSUs, and backend systems process and potentially store large quantities of information, including location oriented information such as position, direction headed, speed, or intended destination.

PRECIOSA focuses on privacy problems created by the availability of location oriented information. Privacy violations can occur either internally or externally. Internal attackers are entities such as operators of the backend system, RSUs, and vehicles. External attackers are, for example, eavesdroppers in the communication system. The problem becomes more severe as the size of collections of location information increases.

One objective of PRECIOSA is to define an approach for privacy evaluation of Co-operative Systems. Deliverable 11 actually goes further than this because it elaborates on what it takes to define a Privacy by Design process.

In the context of ITS applications, sensitive information often reveals the movement patterns of individuals. In many cases, information about people is related to information about their vehicles, at least for a specific time interval. Such information relates a person’s identity directly to his vehicle’s identity. Thus the close link between the identity of a person and a vehicle transfers the identification problem from a person’s identity to that of a vehicle. However, in many applications a vehicle identity is required, at least for parts of a journey. The privacy issue therefore requires an approach that handles both requirements, i.e., to protect the privacy of an individual and to relay information about his vehicle.

2.1 *Intended Audience*

This document is a deliverable of WP5, and an official deliverable to the EC. This document is intended for the ICT community interested in the impact of privacy on their services.

The authors of the deliverable and the PRECIOSA consortium would also like to point out the following:

- As rightly pointed out by the European Commission nominated reviewers of this deliverable, the deliverable does not provide *concrete guidelines for the development of privacy-friendly ITS applications*.
- Instead, the deliverable has focused on providing suggestions on concrete steps that would lead to consensus and the creation of concrete guidelines. This is the reason why the document has been structured so that it could be submitted as a working document in further discussion forum such as the eSecurity forum WG (to deliver concrete guidelines for the development of privacy-friendly ITS applications)

Consequently, D11 has been worked out as a policy oriented contribution.

2.2 *Document Structure*

The deliverable contains three sections:

- The first section describes the context for the content of this deliverable.

  - It first explains the context of privacy today. This includes an introduction to the events that led to this work, a summary of the current situation in terms of legal, industry and technology perspectives, and a section on definitions which frame our understanding of privacy.
  - It then explains the concept of Privacy by Design (PbD) and elaborates on the current moves towards PbD by data protection authorities. The UK data protection initiative is presented, as well as the Madrid privacy declaration.
  - It finally elaborates on the specific issues of privacy in ITS applications. Location-based telematics applications and the case of cooperative systems are covered.
- The second section sketches privacy design guidelines for ITS applications. The various elements of the design of privacy features are explained as well as their integration in the classical life cycle process. The position of the PRECIOSA technology contribution based on the PeRA architecture within this process is described. This section is the core part of the deliverable. It takes a more global tone than initially planned, i.e., instead of explaining a specific design process based on PRECIOSA technologies, we outline a general process which could or could not involve PRECIOSA technologies.
- The last section provides a perspective on work needed in the future concerning user involvement, the engineering process itself, and standardisation and interoperability.

2.3 Relationship to the Other Deliverables

While this deliverable is self contained, other deliverables provide more detailed information on the following topics:

- D1 provides information on privacy issues in cooperative systems
- D7 provides details on the PeRA architecture with a refinement of the mechanisms and use-cases presented in D10.
- D13 provides information on how design and implementation can be validated.

3 Context

3.1 Privacy Today

This section provides first a general introduction to privacy in ITS applications. It then describes the current legal, industrial, and technical situation. Finally, an overview of privacy definitions used in this context is presented.

3.1.1 Introduction

This deliverable is the result of work, discussions, and events related to the issue of privacy for ITS applications, more precisely on applications which assume an infrastructure whereby a vehicle can potentially be permanently tracked.

At the end of 2006, the Article 29 Working Party [1] issued a study on the eCall (emergency call) application [3] which raised concerns on the protection of personal data in location-oriented data applications. This resulted in a recommendation stating that eCall implementations should provide the option of allowing vehicle drivers to disable the operation of the eCall subsystem.

In early 2007, the European Commission organised a workshop which led to a decision to create a working group in the eSafety Forum [5]. Thus the eSecurity Working Group [6] was created in early 2007.

In mid 2008, another workshop was organised by the eSecurity WG and PRECIOSA. It was agreed that an action plan would be presented to the Article 29 WP. The eSecurity WG subsequently proposed the organisation of specific meetings which informally involved members of the Article 29 WP. This was presented to the Article 29 WP in March 2009 and received positive feedback.

In July 2009, the European Data Protection Supervisor (EDPS) issued on opinion on the ITS Directive [38] in which it called for (1) a Privacy by Design approach and (2) a consensus approach allowing for the identification of Best Available Techniques (BAT) for privacy protection.

Consequently, three joint meetings were held by the eSecurity WG and the Article 29 WP, in October 2009, December 2009 and May 2010. They focused on (1) respective presentations for mutual understanding, (2) presentations on use cases for discussion, (3) agreement on further work in the eSecurity WG towards recommendations for Privacy by Design.

Based on the discussions held in these forums, PRECIOSA considers this document to be a first contribution towards this goal.

3.1.2 The Current Situation

*3.1.2.1 **Legal Framework***

European data protection has a legal framework that is defined by two Directives:

- Directive 95/46/EC [33] 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” took as an input the OECD recommendations [39] for 7 principles: notice, purpose, consent, security, disclosure, access, and accountability. Basically, the directive organised the principles into three categories: transparency (a data subject has the right to be informed), purpose (personal data can only be processed for specified and legitimate purpose) and proportionality (the amount of collected data must not be excessive in relation to the purpose).
- Directive 2002/58/EC [32], or the e-Privacy directive, builds on the previous directive by addressing the regulation of digital communication. It deals with such aspects as data retention, cookies, and spam. This directive is currently under revision to cover new issues related to current personal data protection issues.

The directives are implemented nationally with the help of the national data protection authorities. Their mission is to monitor the application of and ensure the respect for data protection legislation. Such organisations are independent, i.e., Member States are required to ensure that their national Data Protection Authorities act in complete independence while exercising the functions entrusted to them [33]. They are allocated resources either directly through their national governments, or through fees that are levied (the case in the UK), or through the fines that they can charge upon infringement. They are also granted powers for intervention, ensuring compliance or punishment.

The Article 29 Working Party [1] is a working group managed by the European Commission with the task of harmonising the position of the various data authorities. One of the activities of the Article 29 WP is to check that issued directives are compliant with the privacy directives.

Finally, the European Data Protection Supervisor (EDPS) [4] is an independent supervisory authority with the role of ensuring that EC institutions and bodies respect their data protection obligations. The EDPS also advises EC institutions and bodies on all matters which have an impact on the protection of personal data. This can apply to proposals for new EU legislation, which was the case in the case of the ITS directive.

*3.1.2.2 **Industry Perspective on Privacy***

While the treatment and implementation of data privacy by the EU Member States is subject to the directives mentioned above and national law, in practice infringement of data protection policy can easily occur. This can be due to lack of awareness or lack of enforcement.

- Awareness of data security is growing. Hardly a day goes by without the press reporting potential or actual problems with data protection. However, lack of understanding is still a major issue, either at management or at the Research & Development level. Small and medium sized organisations are often weak at both levels, such that they deploy ICT-based services which do not meet data protection requirements. In addition, many of these organisations are often not aware that they need to make a declaration to their national data protection agency when they collect personal data. Large organisations generally have good management practices (e.g., they appoint a privacy officer), and they make sure that they comply with legal obligations. Nevertheless, the lack of awareness at the R&D level results in much development being done without privacy in mind. The consequence is that large R&D investments in time and money are spent before privacy validation takes place, making it difficult or impossible to implement a satisfactory solution later on in the development process. We believe an underlying cause of this lack of understanding is the dearth of courses concerning privacy at the educational level. The current curriculum on ICT and computer science rarely, if ever, includes privacy or Privacy by Design as core topics, with the result that only very specialised students learn about privacy and related technologies.
- Lack of enforcement is also the norm today. While many data protection agencies have the right to audit companies and to fine them when infringement takes place, they often do not have enough resources to implement effective enforcement. Furthermore, even when organisational enforcement is in place the process can be error prone. For example, an employee must keep data he processes confidential but may reveal confidential data by accident.
- On a side note, we want to stress that data protection misses a third critical component: prevention. Our ICT infrastructures are not built in a way that puts up any hurdles on breaching data protection. This is in sharp contrast to other areas where the prevention of breaking the law is a regular topic and often a research discipline in itself, e.g., the prevention of crime or fraud. Following this line of thought, the prevention of privacy infringement would lead to ICT systems such as networks that have built-in capabilities to hinder unnecessary data collection or abuse of personal data. PRECIOSA's PeRA could be seen as an early step towards such a goal.

*3.1.2.3 **Technical Perspective on Privacy***

From a technical point of view, data protection capabilities, known as Privacy Enhancing Technologies (PETs), are in general understood by security experts, and are often seen as complex and costly.

We wish to highlights two trends that could have an impact in the (possibly near) future:

- The security community has been working for some time on zero-knowledge technology, which deals with mechanisms that allow properties associated with personal data to be made available without revealing the personal data itself. For instance, if a user is equipped with specific cryptographic credentials, it can be securely proven that a person is above 18 without revealing his birthday. Such security mechanisms are still quite expensive in terms of consumed resources, though there are many cases where practical development has been done.
- There is a growing awareness that privacy can be enhanced at the architecture and R&D process level. This is the case with PRECIOSA, in which the main contributions have been (1) the PeRA architecture and (2) an understanding of what it takes to implement a Privacy by Design process.

3.1.3 Current Privacy Definitions

Privacy has always been difficult to define, in both legal and technical domains. With every advance in communication technology, the task becomes even harder, and the development of digital data storage and transmission is no exception. Alan Westin did some of the first significant work on the problem of consumer data privacy and data protection. In his 1967 book *Privacy and Freedom* [30], he wrote that privacy is “the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.” In the years since, numerous scholars and organisations have provided additions and refinements to the definitions of privacy. The selection of definitions below provided by organisations and experts on privacy offers a sample of relevant definitions.

In addition, the PRECIOSA project created on-line glossaries of privacy terminology [27] and ITS terminology [26] which provide a more extensive collection of definitions.

3.1.3.1 EDPS Data Protection Glossary

The European Data Protection Supervisor provides the following definitions in its Glossary of Data Protection terminology [16]:

Privacy

Privacy is the ability of an individual to be left alone, out of public view, and in control of information about oneself.

One can distinguish the ability to prevent intrusion in one's physical space ("physical privacy", for example with regard to the protection of the private home) and the ability to control the collection and sharing of information about oneself ("informational privacy").

The concept of privacy therefore overlaps, but does not coincide, with the concept of data protection.

The right to privacy is enshrined in the Universal Declaration of Human Rights (Article 12) [11] as well as in the European Convention of Human Rights (Article 8) [7].

Personal data

According to Article 2 (a) of Regulation (EC) No 45/2001 [34]: "Any information relating to an identified or identifiable natural person, referred to as "data subject" - an identifiable person is someone who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity".

The name and the social security number are two examples of personal data which relate directly to a person. But the definition also extends further and also encompasses for instance e-mail addresses and the office phone number of an employee. Other examples of personal data can be found in information on physical disabilities, in medical records and in an employee's evaluation.

Personal data which is processed in relation to the work of the data subject remain personal/individual in the sense that they continue to be protected by the relevant data protection legislation, which strives to protect the privacy and integrity of natural persons. As a consequence, data protection legislation does not address the situation of legal persons (apart from the exceptional cases where information on a legal person also relates to a physical person).

Personal data filing system

According to Article 2 sub (c) of Regulation (EC) No 45/2001 [34], personal data filing system refers to "any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis."

The definition is independent of the size of the filing system, which may vary according to the circumstances. In some cases, such as for instance the case of disciplinary files for a small sized EU-body, the filing system can comprise just a handful of entries.

Processing (of personal data)

According to Article 2 (b) of Regulation (EC) No 45/2001 [34], processing of personal data refers to "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction."

Personal data may be processed in many activities which relate to the professional life of a data subject. Examples from within the EU institutions and bodies include: the procedures relating to staff appraisals and to the billing of an office phone number, lists of participants at a meeting, the handling of disciplinary and medical files, as well as compiling and making available on-line a list of officials and their respective field of responsibilities.

Personal data relating to other natural persons than staff may also be processed. Such examples may concern visitors, contractors, petitioners, etc.

Processor

According to Article 2 (e) of Regulation (EC) No 45/2001 [34], a processor shall mean "a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller."

The essential element is therefore that the processor only acts "on behalf of the controller" and thus only subject to his instructions.

For example, a security company monitoring the entries into an institution's building is not processing personal data of the persons entering a building for its own purpose, but on behalf of the institution concerned.

In some cases, the processor may choose not to process the data himself, but may have recourse to a subcontractor who processes the data on his behalf. In practice, this will depend upon the processor agreement entered into with the controller.

PETs

The acronym 'PETs' stands for "Privacy Enhancing Technologies". It refers to a coherent system of information and communication technology (ICT) measures that protect privacy by eliminating or reducing personal data or by preventing unnecessary and/or undesired processing of personal data, all without losing the functionality of the information system.

The use of PETs can help to design information and communication systems and services in a way that minimizes the collection and use of personal data and facilitates compliance with data protection rules. It should result in making breaches of certain data protection rules more difficult and/or helping to detect them.

PETs can be stand-alone tools requiring positive action by consumers (who must purchase and install them in their computers) or be built into the very architecture of information systems.

3.1.3.2 ICO Privacy Assessment Handbook

The UK’s Information Commissioner’s Office describes four aspects of privacy in its Privacy Assessment Handbook [21].

Privacy of personal information

This is referred to variously as ‘data privacy’ and ‘information privacy’. Individuals generally do not want data about themselves to be automatically available to other individuals and organisations. Even where data is possessed by another party, the individual should be able to exercise a substantial degree of control over that data and its use. The last six decades have seen the application of information technologies in many ways that have had substantial impacts on information privacy.

Privacy of the person

Sometimes referred to as ‘bodily privacy’, this is concerned with the integrity of the individual’s body. At its broadest, it could be interpreted as extending to freedom from torture and right to medical treatment, but these are more commonly seen as separate human rights rather than as aspects of privacy. Issues that are more readily associated with privacy include body searches, compulsory immunisation, blood transfusion without consent, compulsory provision of samples of body fluids and body tissue, and requirements for submission to biometric measurement.

Privacy of personal behaviour

This relates to the observation of what individuals do, and includes such issues as optical surveillance and ‘media privacy’. It could relate to matters such as sexual preferences and habits, political or trade union activities and religious practices. But the notion of 'private space' is vital to all aspects of behaviour and is relevant in 'private places' such as the home and toilet cubicle, and is also relevant in 'public places', where casual observation by the few people in the vicinity is very different from systematic observation, the recording or transmission of images and sounds.

Privacy of personal communications

This could include various means of analysing or recording communications such as mail 'covers', the use of directional microphones and 'bugs' with or without recording apparatus and telephonic interception and recording. In recent years, concerns have arisen about third party access to email messages. Individuals generally desire the freedom to communicate among themselves, using various media, without routine monitoring of their communications by other persons or organisations.

3.1.3.3 Taxonomy of Privacy

In the 2006 article "A Taxonomy of Privacy" [28], Daniel Solove provides a framework for how the legal system can come to a better understanding of privacy. His aim is to develop a taxonomy that focuses more specifically on the different kinds of activities that impinge upon privacy. In his taxonomy, Solove describes the following four basic groups of harmful activities.

Information Collection

Information collection creates disruption based on the process of data gathering. Even if no information is revealed publicly, information collection can create harm. There are two forms of information collection: (1) surveillance and (2) interrogation.

Information Processing

Information processing refers to the use, storage, and manipulation of data that has been collected. Information processing does not involve the collection of data; rather, it concerns how already-collected data is handled. Five forms of information processing are: (1) aggregation, (2) identification, (3) insecurity, (4) secondary use, and (5) exclusion.

Information Dissemination

Harms arising out of the collection of information as well as harms arising from the storage and use of data can occur. "Information dissemination" is one of the broadest groupings of privacy harms. These harms consist of the revelation of personal data or the threat of spreading information. This group includes (1) breach of confidentiality, (2) disclosure, (3) exposure, (4) increased accessibility, (5) blackmail, (6) appropriation, and (7) distortion.

Invasion

The final grouping of privacy harms are labeled as "invasion." Invasion harms differ from the harms of information collection, networking, and dissemination because they do not always involve information. There are two types of invasion: (1) intrusion, and (2) decisional interference.

3.2 Privacy by Design

3.2.1 Concept of Privacy by Design

The concept of Privacy by Design was developed in the 1990's by the Privacy Commissioner of Ontario, Canada, Dr. Ann Cavoukian [13]. The concepts of PbD were developed to address the increasing effects of Information and Communication Technologies, and of large-scale networked data systems.

Privacy by Design refers to the goal and approach of embedding privacy into the design specifications of various technologies by building the principles of Fair Information Practices (FIPs) into the design, operation, and management of information processing technologies and systems. Though originally developed with Information Technology (IT) as its primary area of application, it has since expanded its scope to accountable business practices as well as physical design and infrastructures.

Since privacy cannot be assured only by compliance with regulatory frameworks, privacy assurance must become the default mode of operation. Privacy Enhancing Technologies are only part of the solution. A more substantial approach is required which extends the use of PETs.

In brief, PbD refers to the philosophy and approach of embedding privacy into the design specifications of various technologies. This may be achieved by building the principles of Fair Information Practices into the design, operation, and management of information processing technologies and systems. It encompasses the following elements:

- Recognition that privacy interests and concerns must be addressed proactively;
- Application of core principles expressing universal spheres of privacy protection;
- Early mitigation of privacy concerns when developing information technologies and systems, throughout the entire information life cycle end to end;
- Need for qualified privacy leadership and/or professional input;
- Adoption and integration of Privacy-Enhancing Technologies (PETs);
- Embedding privacy in a positive-sum (not zero-sum) manner so as to enhance both privacy and system functionality;
- Respect for users’ privacy.

The objectives of Privacy by Design are ensuring privacy and personal control over one’s information and, for organisations, gaining a sustainable competitive advantage. These objectives can be reached by practicing the seven foundational principles below, which are defined in [14]:

Proactive not Reactive; Preventative not Remedial

The PbD approach is characterised by proactive rather than reactive measures. It anticipates and prevents privacy invasive events before they happen. PbD does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred – it aims to prevent them from occurring. In short, PbD comes before-the-fact, not after.

Privacy as the Default

We can all be certain of one thing – the default rules. PbD seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice. If an individual does nothing, their privacy still remains intact. No action is required on the part of the individual to protect their privacy – it is built into the system, by default.

Privacy Embedded into Design

PbD is embedded into the design and architecture of IT systems and business practices. It is not bolted on as an add-on, after the fact. The result is that privacy becomes an essential component of the core functionality being delivered. Privacy is integral to the system, without diminishing functionality.

Full Functionality – Positive-Sum, not Zero-Sum

PbD seeks to accommodate all legitimate interests and objectives in a positive-sum “win-win” manner, not through a dated, zero-sum approach, where unnecessary trade-offs are made. PbD avoids the pretense of false dichotomies, such as privacy *vs.* security, demonstrating that it *is* possible to have both.

End-to-End Lifecycle Protection

PbD, having been embedded into the system prior to the first element of information being collected, extends throughout the entire lifecycle of the data involved, from start to finish. This ensures that at the end of the process, all data are securely destroyed in a timely fashion. Thus, PbD ensures cradle to grave lifecycle management of information, end-to-end.

Visibility and Transparency

PbD seeks to assure all stakeholders that whatever the business practice or technology involved, it is in fact, operating according to the stated promises and objectives, subject to independent verification. Its component parts and operations remain visible and transparent to users and providers alike. Remember, trust but verify.

Respect for User Privacy

Above all, PbD requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options.

In October 2010, the International Conference of Data Protection and Privacy Commissioners, which included over 600 representatives of governments, companies, and non-governmental organizations, approved a resolution which recognizes the concept of Privacy by Design. The goal is to ensure that privacy is embedded into new technologies and business practices from the outset as an essential component of privacy protection [10].

3.2.2 The UK Data Protection Initiative on Privacy by Design

The Information Commissioner's Office (ICO) is the independent authority created to uphold information rights in the public interest in the UK [9]. The ICO promotes openness by public bodies and data privacy for individuals. The department that sponsors it within the government is the Ministry of Justice.

The Protection Act, the Freedom of Information Act, the Environmental Information Regulations, and the Privacy and Electronic Communications Regulations are all enforced and overseen by the ICO. In this capacity, it rules on eligible complaints, gives guidance to individuals and organisations, and takes appropriate action when the law is broken.

The ICO supports Privacy by Design. Among the numerous ICO documents related to PbD, in 2008 a report was issued which provides an analysis of the situation and proposes actions that can be taken based on recommendations with the aim of achieving a comprehensive approach to securing privacy protection [19]. An implementation plan was developed which identifies themes and action points arising from this report [20].

The ICO's Privacy Impact Assessment Handbook [21] provides a guide for the process of identifying and assessing privacy risks at an early stage of project development and implementing privacy protection solutions throughout the entire development life cycle. The following points are excerpts from the Handbook.

The reasons an organisation undertakes a Privacy Impact Assessment (PIA) are:

- identifying and managing risks
- avoiding unnecessary costs
- inadequate solutions
- avoiding loss of trust and reputation
- informing the organisation's communications strategy.

Ideally the end results of an effective PIA are:

- the identification of the project's privacy impacts
- appreciation of those impacts from the perspectives of all stakeholders
- an understanding of the acceptability of the project and its features by the organisations and people that will be affected by it
- identification and assessment of less privacy-invasive alternatives
- identification of ways in which negative impacts on privacy can be avoided
- identification of ways to lessen negative impacts on privacy
- where negative impacts on privacy are unavoidable, clarity as to the business need that justifies them
- documentation and publication of the outcomes.

In order to achieve these goals, the Handbook outlines the following guidelines:

- Start early to ensure that project risks are identified and appreciated before the problems become embedded in the design.
- Commence a PIA as part of the project initiation phase (or its equivalent in whichever project method the organisation uses).

- If the project is already under way, start today, so that any major issues are identified with the minimum possible delay.

The Handbook suggests that the most beneficial and cost-effective approach is to conceive of the PIA as:

- a cyclical process
- linked to the project's own life-cycle
- revisited in each new project phase.

An organisation should identify its privacy risks, which can be of various types such as:

- broad personal information issues
- issues around identification of the individual
- function creep
- registration and authentication processes
- surveillance
- location and tracking.

Once an organisation's privacy risks are identified, it can define privacy mitigation avoidance measures to reduce the risk. These can include:

- minimising the collection of personal information to what is strictly necessary
- non-collection of contentious data-items
- active measures to stop or block the use of particular information in decision making (a good example of this is ethnic monitoring forms being filled out anonymously when companies are recruiting)
- active measures to preclude the disclosure of particular data-items, for example screening or hiding of certain services which are being provided to the individual which might disclose other personal information
- non-adoption of biometrics in order to avoid issues about invasiveness of people's physical selves.

Based on these principles, the Handbook goes on to provide practical guidelines with details for implementing the PIA process, as well as checklists for screening the criteria. The main steps of the process are:

- initial assessment
- privacy impact assessment
- privacy law and other legal compliance checking
- Data Protection Act compliance check.

3.2.3 The Madrid Privacy Declaration

The goal of the Madrid Privacy Declaration [29] is to reaffirm international instruments for privacy protection, identify new challenges, and call for concrete actions. More than 100 civil society organisations and privacy experts had signed this declaration by November 2009 at the 31st annual meeting of Privacy and Data Protection Commissioners' conference in Madrid.

The Declaration affirms that privacy is a fundamental human right, and warns that "privacy law and privacy institutions have failed to take full account of new surveillance practices." It urges countries "that have not yet established a comprehensive framework for privacy protection and an independent data protection authority to do so as expeditiously as possible," and recommends a "moratorium on the development or implementation of new systems of mass surveillance."

The document begins with a reminder of the declarations and agreements currently in force in Europe and worldwide, such as the Universal Declaration of Human Rights [11] and the 1995 Data Protection Directive [33]. It then lists some examples of current practices that put personal privacy at risk, such as unaccountable surveillance and internet-based services. The declaration states the following ten actions:

1. Reaffirm support for a global framework of Fair Information Practices that places obligations on those who collect and process personal information and gives rights to those whose personal information is collected;
2. Reaffirm support for independent data protection authorities that make determinations, in the context of a legal framework, transparently and without commercial advantage or political influence;
3. Reaffirm support for genuine Privacy Enhancing Techniques that minimize or eliminate the collection of personally identifiable information and for meaningful Privacy Impact Assessments that require compliance with privacy standards;
4. Urge countries that have not ratified Council of Europe Convention 108 together with the Protocol of 2001 to do so as expeditiously as possible;
5. Urge countries that have not yet established a comprehensive framework for privacy protection and an independent data protection authority to do so as expeditiously as possible;
6. Urge those countries that have established legal frameworks for privacy protection to ensure effective implementation and enforcement, and to cooperate at the international and regional level;
7. Urge countries to ensure that individuals are promptly notified when their personal information is improperly disclosed or used in a manner inconsistent with its collection;
8. Recommend comprehensive research into the adequacy of techniques that de-identify data to determine whether in practice such methods safeguard privacy and anonymity;
9. Call for a moratorium on the development or implementation of new systems of mass surveillance, including facial recognition, whole body imaging, biometric identifiers, and embedded RFID tags, subject to a full and transparent evaluation by independent authorities and democratic debate; and
10. Call for the establishment of a new international framework for privacy protection, with the full participation of civil society that is based on the rule of law, respect for fundamental human rights, and support for democratic institutions.

3.2.4 Conclusion

The advent of the Internet and of ICT has led to initiatives from data protection agencies to promote Privacy by Design. Principles for PdD have been proposed by Ann Cavoukian in Canada. A systematic application has been promoted by ICO, the UK data protection agency, with a suggestion to use publishable privacy assessment documents. In addition, the Madrid joint declaration has been published by the community of data protection agencies.

The ICO approach was discussed within the joint eSecurity/Article 29 WP meetings, and it was concluded that it is a good starting point, but at a very high level, thus lacking an embedding in a technical approach for software or systems engineering, i.e., something that we might call a “Privacy by Design engineering process”. In Section 4, PRECIOSA will make an attempt to sketch a PbD process for ITS applications.

3.3 Privacy in ITS Applications

3.3.1 Location-Based Telematics Applications

This section provides an analysis of security and privacy of location information in location-based ITS applications based on three services: eCall, road charging, and pay-as-you-drive. These applications are excellent cases for demonstrating privacy risks and the advantages of Privacy by Design.

*3.3.1.1 **eCall***

The eCall (emergency call) initiative is sponsored by the European Union with the goal of bringing rapid help to motorists involved in an accident anywhere in the EU [3]. Immediately after a crash, a car will automatically contact the nearest emergency centre and provide it with the necessary data. The deployment of a harmonised eCall system is a joint industry/public project.

The content of an eCall creates privacy issues because of the potential risk that vehicles could be permanently tracked. The Article 29 Working Party [1] examined this problem and recommended several actions. In brief, if eCall is optional, then a driver should be able to deactivate it, but if it is mandatory, then laws are needed to take into account data protection principles. To protect privacy, strict measures should be taken while collecting and transmitting data. For example, data should be erased after a set time limit, e.g., 24 hours, and to ensure that data is not used to track vehicle speed, it should be modified in such a way that location information is accurate while speed information is blurred.

3.3.1.2 ***Road Charging***

Road charging (also known as road pricing or electronic fee collection) is a system that charges a fee for using an infrastructure like a road, tunnel, or bridge. Tolls can be collected either manually or electronically. Electronic systems may or may not require the installation of On-Board Equipment (OBE), road side infrastructure, or satellite positioning.

Several different implementation strategies have been developed for road charging systems. The following three methods have been tested, and the advantages and disadvantages of each are described.

1. Thin Client

   The OBE collects positioning information from a satellite and on-board sensors. It does a small amount of processing of this information and then transfers it to the back-office system which does the major processing of the data and determines the toll. Since the OBE does not determine whether it is in a toll zone or calculate the fee, all positions need to be transmitted to the back office. The transmission and storage of this amount of personal and location information creates potential privacy problems. In order to make this method privacy friendly, a combination of technical solutions, such as using pseudonyms and PeRA policy enforcement, and laws, such as requirements on data minimisation and processing strictly bound to the purpose, are needed.

2. Thick Client

   The OBE collects position information and performs complex processing on it, including the calculation of the fee. The only data sent to the back-office are the details of the invoice and enough information for the toll operator to verify that the fee calculated by the OBE is correct. Thus the OBE must be more complex, but communication and back-end requirements are lighter. From a privacy perspective, this offers the driver more protection.

3. Smart Client

   This method falls between the previous two in that it distributes the intelligent operations between the OBE and back-office according to the needs of the system. For example, the OBE detects toll objects and sends only information about recognized toll objects to the back-office where the data is analysed and the fee is calculated.

In all three methods, a certain amount of personal and location data are collected, transmitted, and stored. A balance is needed between the demands of the user for privacy and the needs of the toll operator for the calculation of accurate payments.

3.3.1.3 ***Pay-As-You-Drive***

Insurance companies have developed Pay-As-You-Drive (PAYD), also called Pay-Per-Mile, models in order to lower costs for both owners and insurers. Instead of a flat yearly fee, customers are charged by how much and where they drive. For every kilometre travelled by a car, the statistical risk of accident is calculated and translated into a personalised insurance fee.

PAYD insurance calculation implementations involve an inherent threat to a user's privacy. Most of them involve OBE which collects location and time information relevant to billing which is transferred to an insurance company. As with road charging, this creates several risks. The insurance company’s management of huge databases creates the risk of information leakage [18][22]. Moreover, the client’s privacy is at risk since the data allows the insurer to track his movements. This conflicts with the proportionality principle since the data collected provides more information than is necessary to carry out the insurance service.

There are some companies that claim to provide privacy-friendly PAYD schemes by collecting only statistics about the location data, e.g., by using the Thick and Smart methods discussed in the Road Charging section above. However, it is often a third company that provides this information to the transportation infrastructure, so the threat to privacy does not disappear but is only shifted. Even if a third party has no knowledge of a driver’s identity, it has been shown that his home and work address can be easily identified from the location information and linked to him [17][24]. Even the anonymisation of data is not fool proof [25][31], and researchers have not yet found a solution to this problem.

3.3.1.4 Conclusions on Location-Based Telematics Applications

In these three location-based applications, it can be seen that privacy concerns have a major influence on the design of their implementation. Clearly, privacy cannot be an afterthought in designing these systems, a situation which calls for a Privacy by Design approach. In addition, the complexity of security solutions requires agreement on evaluation criteria for testing solutions. Those criteria are needed to help the stakeholders make decisions on implementation choices.

3.3.2 The Case of Cooperative Systems

Cooperative Systems rely on the availability of a communication infrastructure that will allow for direct communication between vehicles (V2V) or between vehicles and beacons on the road infrastructure (V2I). The whole infrastructure as well as related applications can raise privacy issues if not properly designed. In Section 5 of the PRECIOSA deliverable *D1 V2X Privacy Issue Analysis*, a number of use cases are presented which demonstrate the privacy risks in such systems. A representative selection of these cases is presented here, briefly summarising the situation and the privacy risks of each.

- Floating vehicle information and traffic information in online navigation:

  An online navigation system on a mobile device includes real time traffic information, some of which is derived from floating vehicle information that is collected from all users of the product.

  Privacy risks are created during the transmission, storage, and processing of time and location information through unauthorised access due to eavesdropping and insecure storage.
- Floating car data / intersection collision warning:

  When approaching an intersection, a driver is warned if there is a danger of collision.

  Location, time, and warning information that is broadcast from beacons to vehicles can be eavesdropped, and data that is insecurely stored can be accessed by unauthorised entities.
- Calculating a route from the current location to home:

  A driver asks a remote Traffic Control Center for the best route from his current position to home.

  Messages can be captured by unauthorised entities, so that current location and destination as well as personal data are accessed.
- Booking a hotel on the road:

  A driver has requested and received the best route to a destination, and he then requests a hotel reservation service to send him the location of a suitable hotel along that route.

  Messages can be captured by unauthorised entities, so that an adversary obtains information on current and future location and time, home and hotel address, and credit card information.

The conclusions for privacy issues in cooperative systems made in PRECIOSA deliverable D1 are the following:

- As long as possible, communicated data should be kept anonymous. This is particularly relevant for broadcasted data, either V2V or V2I, as the receiver is not predetermined in this case.
- For certain applications, anonymity or pseudonymity is not possible, for example because a service has to be paid or a service requires identification for other purposes. In this case, the communication should be kept confidential between the peers. For example, the connection from a vehicle to a backend server is encrypted.
- Because it may be necessary to store data in various units, e.g., in a vehicle, a backend control center, or a road side unit, access to stored data must be regulated to ensure privacy.

3.3.3 The Growing Privacy Awareness in the ITS Community

The ITS community in Europe and elsewhere is involved in considerable Research & Development activities to make intelligent transport systems a reality. To this end, in 2003 the European Commission established the eSafety Forum [5] as a joint coordination platform involving all the road safety stakeholders.

The general objective of the eSafety Forum is to promote and monitor the implementation of the recommendations identified by the eSafety Working Group, and to support the development, deployment, and use of intelligent, integrated road safety systems. This will lead to increase of smart road safety and eco-driving technologies. They are called "smart" because they are based on the powers of computers and telecom communication.

At the end of 2006, the Article 29 Working Party published a report recommending that the eCall boxes could be disabled by the driver for privacy reasons. Consequently, a workshop on privacy was organised by the European Commission, which lead to the creation of the eSecurity Working Group. This working group produced a report, *"Vulnerabilities in Electronics and Communications in Road Transport"*, which is now publically available [15].

The eSecurity report examines vulnerabilities in two different technological situations. The first part covers independent vehicle-based systems, which comprises in-vehicle products and systems such as electronic components, pre-fitted on-board systems, and after-market additional vehicle electronics. The second part covers interactive systems, i.e., applications which communicate with external systems for ITS services such as road charging and eCall. Both parts present several representative use cases and discuss the current legal conditions and their consequences. Since Part 1 deals with current technology, it describes what measures OEMs are taking to deal with the vulnerabilities. Since Part 2 deals with future technologies, it analyses the envisioned security risks and proposes possible technical protection measures.

The report concludes with the following recommendations:

1. Ensure separation between independent vehicle-based systems and interactive systems. Vehicle-based systems should remain under the responsibility of the OEMs and should not be affected by interactive systems.
2. Investigate liability issues of applications beyond informing systems (systems that have an immediate impact on driving). Further research work is needed to understand and monitor these effects.
3. Harmonise legal measures in place within Member States concerning improvement of electronic security (e.g., regulations on manipulation of mileage). Today inconsistencies among legal framework within the Member States exist.
4. Address security issues raised by specific applications. In particular define evaluation criteria and methods which stakeholders can use in their decision process.
5. Undertake further work to identify further recommendations for a Privacy by Design approach.
6. Maintain further work related to cooperative systems. In particular,
   6.1 Ensure necessary standardisation and harmonisation of security solutions.
   6.2 Validate security and privacy mechanisms for the first generation of cooperative systems in field operational trials.
   6.3 Undertake research activities on security and privacy issues for the next generation of cooperative systems.

3.3.4 Conclusion

Recommendation 5 of the eSecurity Working Group report, which is to identify further recommendations for a Privacy by Design approach, is the motivation for the next section of this deliverable.

4 Privacy by Design Guidelines for ITS Applications

This section provides an initial sketch of a Privacy by Design engineering process for ITS applications. While it represents work carried out by PRECIOSA partners, it also takes into account work and opinions from other parties (e.g., the eSecurity WG) and was influenced to a large extent by the discussions and interchanges between PRECIOSA partners and these parties. Further note that while this work was carried out with a focus on ITS applications, probably most, if not all, of the concepts apply to ICT applications in general.

4.1 Sketch of Overall Process

Figure 1 summarises the Privacy by Design engineering process as proposed by PRECIOSA. The process is meant to extend a classical software engineering process. In this document, we use the classical waterfall model (seen on the left side of the diagram) which we have simplified into 5 stages:

- The application requirements phase
- The design phase
- The implementation phase
- The verification phase
- The operation and maintenance phase.

We have chosen the waterfall approach as it is simple and widely known for the sake of illustrating how a PbD process can be integrated with an existing process. There are many similar and different software and systems engineering approaches and we want to stress that our PbD engineering process can be easily tailored to also fit those other approaches. One of the tangible steps that would have to be taken in order to implement the PbD process, would be customise the PbD description process to each engineering standards.

The Privacy by Design process has three major stages (seen in the red text going down the right side):

- A privacy requirements analysis stage (Stage I)
- A privacy-aware design and implementation stage (Stage II)
- A privacy verification and assurance stage (Stage III)

Note that the Design box in the waterfall model overlaps with the PdD Stages I and II, since certain privacy requirements identified in Stage I should impact the design of the system.

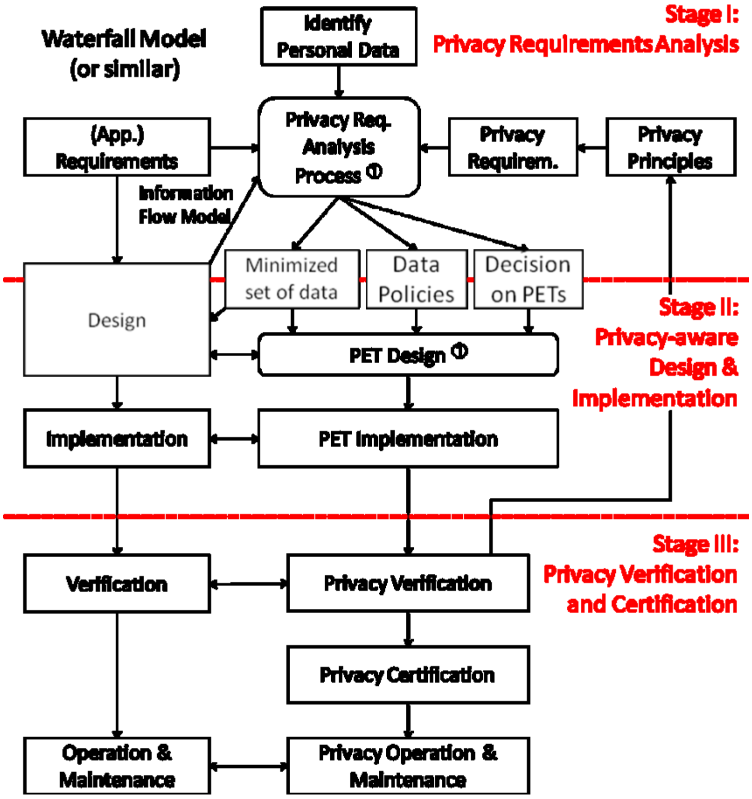

Figure 1: Privacy Engineering Process

The following activities are performed during Stage I:

- Identification of personal data. This assesses the full amount of personal data that this application might process if no data minimization would be applied.
- Identification of privacy principles. This action has a box in the diagram, but it is possible that the privacy principles are already identified and agreed upon ahead of time. For instance, if the OECD guidelines [39] are followed, then the following principles are used: limited collection, data quality, purpose specification, use limitation, security safeguards, openness, individual participation, and accountability.
- Identification of privacy requirements, based on privacy principles.
- Privacy requirements analysis process.

The privacy requirements analysis process is a key activity which is further described in Figure 2. It takes the following input: privacy requirements, identified personal data, application requirements, and a design based information flow model (provided in the early stages of the design phase in the waterfall model). The following activities are carried out:

- Identify the minimum set of personal data needed to handle application requirements
- Add data transformations to achieve a minimized set of data. This will involve mechanisms such as anonymisation, unlinkability, aggregation, obfuscation, changing resolution, etc.
- Specification of restrictive default policies for data.

As a result, the privacy requirements analysis process provides three items as input for Stage II:

- The specification of a Minimised Set of Data (MSD)
- The specification of data policies
- A decision on the privacy enhancing technologies to be used

The privacy requirements analysis process is a key phase because it could involves iterations and therefore modification of architecture approaches. The cost and performance of some PETs could be incompatible with the overall application cost objectives and this could lead to a modification of the minimized set of data. Another tangible step in the PbD process is therefore to **document** the alternatives and provide a rationale on why one architecture has been selected.

Assume a distributed system with A (web server), B (road side unit), C(vehicle).

- If A has lots of computing resources, B has significant computing resources and C limited resources, the minimum set of data from C level is not optimised as C has to reveal more data to C. The minimum set of data from B viewpoint could on the other had be optimal, as a most advanced PET can be integrated in B
- If A has lots of computing resources, B has significant computing resources and C significant computing resources, the minimum set of data from C level could be optimised

Stage II includes design and implementation. In parallel to the application design on the left, we must carry out a PETs design phase which might, for example, include the following activities in Figure 2:

- Designing mechanisms for policy enforcement
- Designing mechanisms for data retention
- Designing or applying other PETs

Taking again the distributed system with A (web server), B (road side unit), C(vehicle).

- If A has lots of computing resources, B has significant computing resources and C limited resources, the architecture involves transmission of data between B and C. Therefore some policy enforcement has to be carried out at B level and and C level
- If A has lots of computing resources, B has significant computing resources and C significant computing resources, the minimum set of data from C level could be optimised. Therefore policy enforcement need to be put in place at C level only.

Following the design and implementation of PETs, we get to Stage III, where verification and testing activities take place. It is important at this point to verify that the level of privacy reached corresponds to the requirements identified in Stage I and fully implements the privacy principles. Verification capabilities can lead to certification, since it can show, for example, that either the process is well applied or that a better level of privacy has been reached. This is followed by the operation and maintenance phase, where it is important to be able to operate and maintain the privacy features that have been deployed. This could involve strengthening policies and/or PETs.

Note that the PETs design phase could leverage existing PETs and their implementation in libraries. We envision that more of these components become readily available as PbD engineering becomes an integral part of software and systems engineering. This will open an opportunity for specialized companies that offer products and support in PbD engineering.

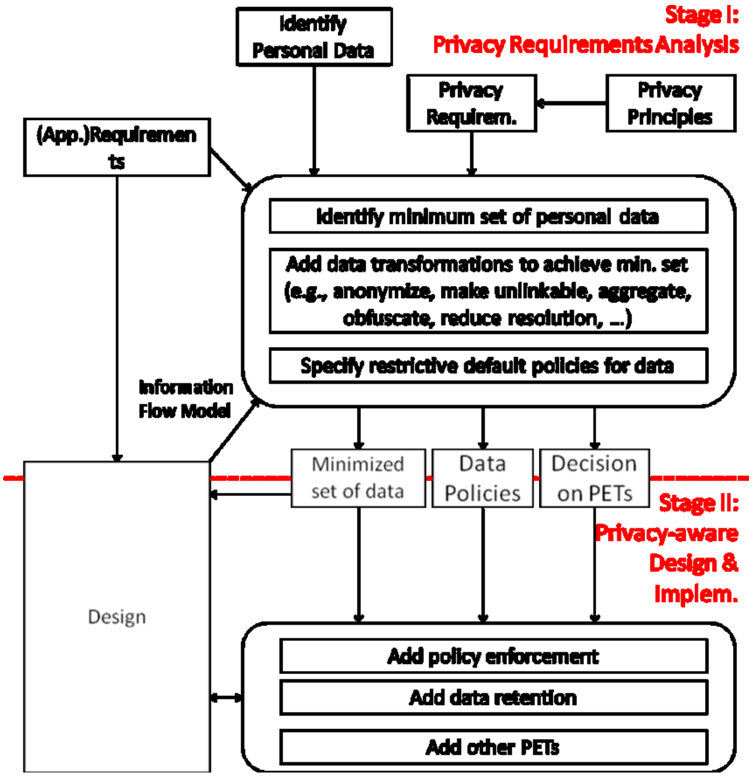
Identify Personal Data
Stage I:
Privacy Requirements Analysis
Privacy Requirem.
Privacy Principles
(App.)Requiremen ts
Identify minimum set of personal data
Add data transformations to achieve min. set (e.g., anonymize, make unlinkable, aggregate, obfuscate, reduce resolution, …)
Specify restrictive default policies for data
Information Flow Model
Minimized set of data
Data Policies
Decision on PETs
Stage II:
Privacy-aware Design & Implem.
Design
Add policy enforcement
Add data retention
Add other PETs

Figure 2: Privacy Requirement Analysis Process

4.2 PRECIOSA Contributions to Privacy

PRECIOSA has carried out work that pioneers the transformation of Privacy by Design concepts as advocated by data protection authorities into its integration and the engineering process. PRECIOSA has also contributed to three areas from a technology viewpoint:

- The focus on PETs related to privacy policy enforcement. In the EDPS‘s definition for PETs [16], it distinguishes between data minimization PETs and “preventing unnecessary and/or undesired processing of personal data”. While more work has been done so far on data minimization, we see potential in the second area, especially policy enforcement, and chose to explore this part in more detail.
- The definition of a run-time architecture, i.e., the PeRA architecture, to provide a distributed perimeter within which privacy policies are enforced. Figures 3, 4, 5, and 6 describe the main features of this architecture.
- The concept of a privacy policy enforcement perimeter is defined. This means that within this perimeter, data that needs protection is associated with allowed operations (policies). These policies cannot be changed or circumvented by any regular means in the system and are thus mandatory. The enforcement of policies is ensured by a Mandatory Privacy Control (MPC) subsystem. This subsystem is itself protected by an MPC integrity protection subsystem.

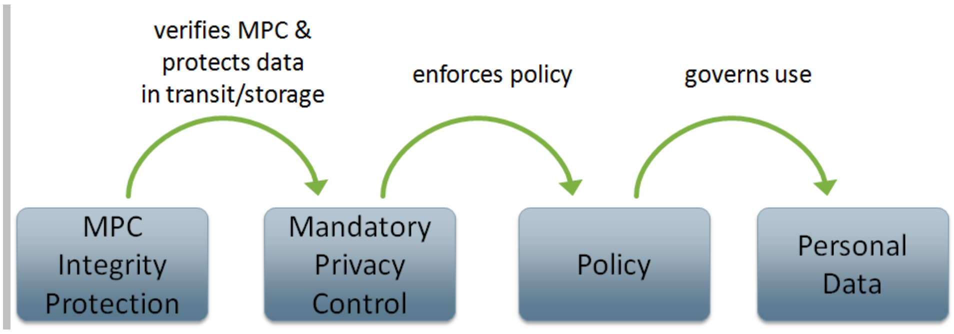
verifies MPC & protects data in transit/storage
enforces policy
governs use
MPC Integrity Protection
Mandatory Privacy Control
Policy
Personal Data

Figure 3: Policy Enforcement Perimeter

The PeRA Architecture consists of two layers: the MPC layer and the underlying MPC Integrity Protection (MIP) layer. The MPC is accessed through a Query-based Application Programming Interface (Query API), which then interacts with the privacy control monitor. This monitor decides whether access is authorised by interacting with the privacy policy manager, and then interacting with the secure local storage and trust manager of the MIP to implement access.

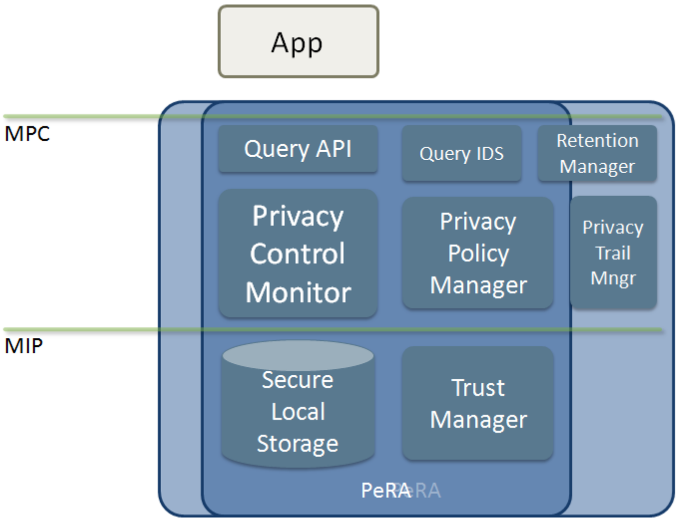

Figure 4: PeRA Architecture

The PeRA architecture can be used in distributed configurations, i.e., the policy enforcement perimeter spans several nodes. In that case, an importer/exporter component provides communication capabilities.

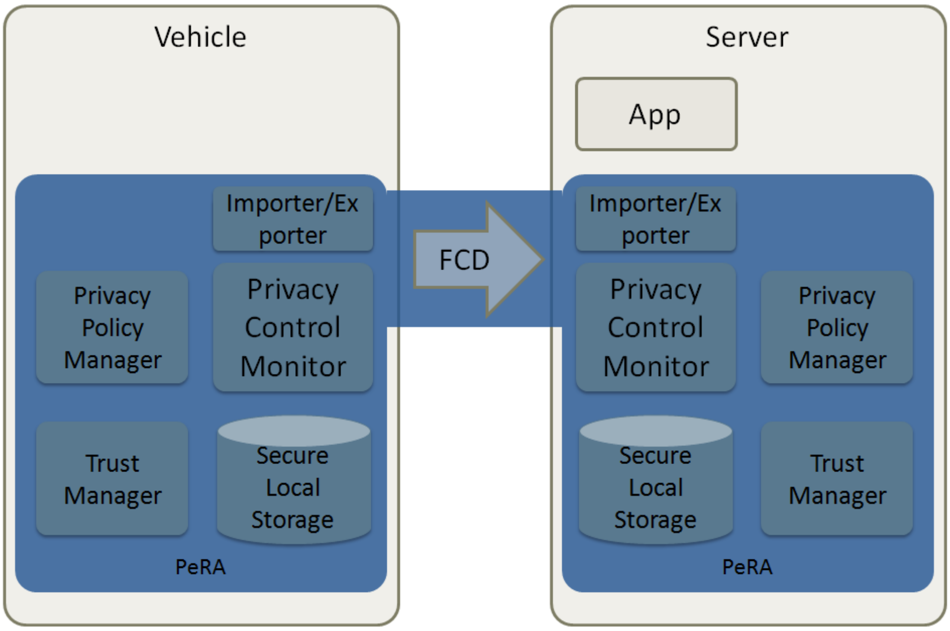

Figure 5: PeRA Architecture in a Distributed Configuration

Finally, the PeRA architecture also supports the notion of an application sandbox, termed Controlled Application Environment (CAE). The CAE can contain specific application code which is considered part of the policy enforcement perimeter. It can access more personal data than applications that are external to the perimeter, but the CAE imposes much tighter control on application capabilities. For example, such an application cannot communicate directly with external entities.

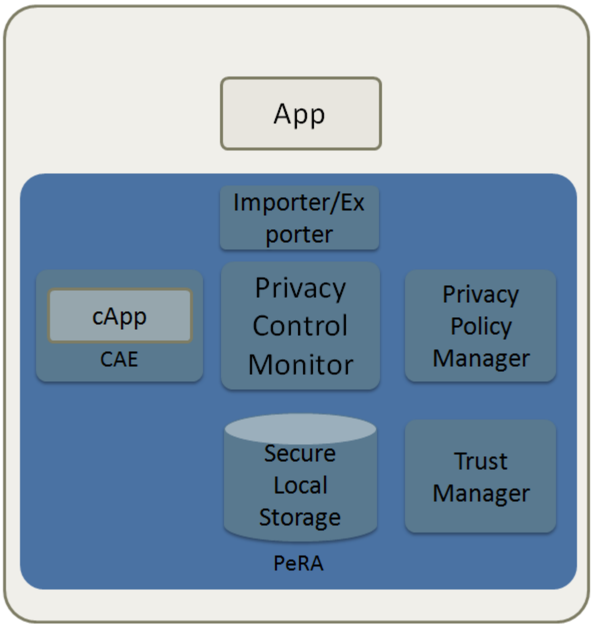

Figure 6: Sandboxes in PeRA Architecture

Different clusters of applications could have different perimeters, i.e., several instances of the PeRA architecture could be deployed.

The PRECIOSA deliverables D7 and D10 contain more detailed descriptions of the PeRA architecture and its mechanisms. The PeRA architecture has stirred considerable discussion in the eSecurity Working Group and during the PRECIOSA Workshop on Privacy in ITS Applications as it is a very different approach to PETs.

4.3 *Example: Road Charging*

We now illustrate how a road charging application could be designed using the Privacy by Design process described above.

4.3.1 Stage I: Privacy Requirements Analysis

During the privacy requirements analysis stage, application requirements and privacy requirements need to be assessed to derive a minimised set of personal data to be used by the application. Simplified requirements could be the following:

1. Application requirements:
   - Constantly record information about vehicle route
   - Ensure accuracy of recorded information
   - Bill driver/vehicle based on recorded route information
   - Keep information for invoice verification
2. Privacy requirements:
   - Keep driven route private from road toll collector
   - Only keep route specific information during invoicing litigation period

Based on such requirements the minimised data set could consist of:

- Customer ID (required to associate vehicle with a customer account and billing information)
- Proof of driven route
- Cost for driven route

Resulting privacy policies for this data set could be:

- Detailed data concerning the vehicle route is only kept inside the vehicle's On-Board Equipment (OBE).
- Proof information about the route is only stored by the OBE for an amount of time needed for invoice verification.
- Data sent outside the OBE are aggregated data on the cost for a vehicle to drive in a given area operated by a toll charger and the customer ID. This aggregated data is authenticated by the OBE to prevent tampering.

4.3.2 Stage II: Privacy-aware Design and Implementation

- Different PETs exist that can be used for this example application. In the following, we give a quick overview how the PRECIOSA PeRA could be employed for road charging. A potential alternative solution would be the recently proposed [12]. The PeRA architecture can be used within the OBE to control that recorded route information can only be accessed by a cost calculation routine running inside the OBE, the raw data would be inaccessible to any other software or system components inside or outside the OBE. The routine's capabilities would be restricted and controlled by the PeRA.
- Cost calculations result in a report only containing the final costs, which has to be reported to the road operator. The PeRA ensures that only aggregated information which complies with the specified privacy policies leaves the OBE. Further, end-to-end transport encryption is enforced and reports are authenticated with the OBU's credentials.
- With data transformations, aggregated proofs can be generated and stored inside the OBE for invoicing instead of detailed location measurements. The PeRA can authenticate such proofs by ensuring the integrity of any components processing the data.
- After the invoicing litigation period, the PeRA ensures destruction of the proof data.

4.3.3 Stage III: Privacy Verification and Assurance

- During the privacy verification and certification stage, the data collected locally in the OBE and transmitted remotely is validated first at the specification level, i.e., through the ontology based privacy analysis based P3L, possibly integrated into some sort of common criteria evaluation, and then at the implementation level, i.e., through some sort of conformance testing. PRECIOSA deliverable D13 provides information on how this can be done when a PeRA architecture is involved.

5 Vision for the Future

We now provide a brief perspective on a number of issues that were discussed during the project. These issues are all elements that must be addressed in order to implement a Privacy by Design engineering process for future applications. While PRECIOSA focuses on ITS applications, this perspective is valid for other ICT-based applications as well. The following issues are covered:

- User involvement
- Engineering process
- Standardisation and interoperability.

5.1 User Involvement

To our knowledge, work related to user involvement in privacy issues consists mainly of providing an Internet user with information and feedback on privacy actions that affect him personally. An example of such work is that of Lorrie Cranor, who started with the Platform for Personal Privacy Preferences (P3P) and is now focusing on Privacy Nudges.

5.1.1 Example of Privacy Nudges

The current approach to protecting privacy on the Internet, which started in the 1990s, is known as “notice-and-choice”. This consists of a web site posting a notice of its privacy policy so the users can then make a choice about the level of privacy they prefer. However, it has been found that users rarely read these statements, and if they do they often find them complex and confusing. Often they don’t have a meaningful choice about the use of their personal information such as birth dates, credit card numbers, and web browsing history. Policy and privacy experts agree that increasing Internet data harvesting has outdated the old approach of using lengthy written notices to safeguard privacy.

There is now a move to replace the notice-and-choice model with "rules-and-tools". Rules would be, for example, government regulations that limit how personal information can be used. Tools would be digital reminders, such as an on-screen alert that enhance a user’s perception that an action he is taking has privacy implications. Such reminders are known as “nudges”, since they gently push the user to notice a situation and react. For example, a user putting her birth date on a social networking site hoping for birthday greetings would receive a nudge on her screen before she confirms the action which points out that this information can also be used for targeted marketing and identity theft.

At Carnegie Mellon’s Cylab Usable Security and Privacy Lab (CUPS), research is being carried out on innovative ways to help people protect their privacy and security. One of them is the project Nudging Users Toward Privacy [2]. Since there are many ways that Internet users can inadvertently give up their privacy, the goal is to develop software tools that help reverse this trend by creating privacy nudges that prompt users to recognize actions that have privacy implications. This is a multi-disciplinary effort that uses computer science techniques such as machine learning, natural language processing, and text analysis, as well as results from non-CS disciplines such as economics and behavioural sciences.

The project will study, design, and test systems that can anticipate and even exploit cognitive and behavioral biases that can impede a user’s privacy and security decision making. The goal is to develop a scientific body of knowledge, as well as test the design of privacy technologies that can nudge users without restricting their choices.

The work will conduct foundational studies to understand user privacy needs, preferences, and behaviors, develop nudging technologies to support and ameliorate privacy decision making in the domain, and evaluate the effectiveness of these technologies in countering users’ tendencies while increasing their overall welfare and satisfaction. This will lead to a novel approach to the design of privacy technologies and policies, based on both ongoing work on usable privacy and security as well as lessons from behavioral decision research, with the addition of soft paternalism.

The goal of helping users avoid mistakes, decrease regrettable choices, and achieve more rapidly the desired balance between sharing and protecting personal information in these areas has clear societal importance. In addition, this research should advance the scientific understanding of what makes privacy decisions difficult, what influences user behavior, and how to build systems that influence such behavior in a desirable manner.

The results of this project can advance the work of privacy and security technology by providing insights and methods that go beyond better interfaces in order to revisit the strategies and assumptions underlying those systems. Moreover, by exposing conditions under which technology alone may not be sufficient to assist such decision-making, this research can advance the work of policy makers. This approach can be extended to the field of information security, since security decisions, at both individual and corporate levels, are affected by biases similar to those that affect privacy decision making.

5.1.2 Assessment

Work related to user involvement includes not only the detection of issues and gently alerting the user, but also methods for creating trust. The user should be given evidence that privacy management features are effectively put in place.

5.2 Engineering Process

Before coming to a really comprehensive PbD Engineering Process, many issues need to be solved and many potential features could help resolve those issues. This Section briefly describes privacy detection at design level, privacy evaluation, and the promise of model-based engineering that we consider interesting paths to explore.

5.2.1 Privacy Analysis

Privacy analysis should allow for the evaluation of privacy protection properties at design time. Several different stakeholders perform privacy analysis. Consequently, every type of stakeholder has its own perspective, purposes, and privacy criteria. The purposes of the privacy analysis may include setting up privacy requirements to define privacy conformance system behaviour, evaluating systems to detect privacy leakages, to calculate metric values which serve as indicators for describing the privacy risk of using such systems, and checking whether an entity's behaviour conforms to a given set of privacy requirements.

According to the Privacy Impact Assessment (PIA) [21], the purpose of the privacy analysis process is to create privacy-aware design specifications. The PIA process takes the perspective of legal authorities and project managers. The results of PIA are privacy requirements that take into account privacy regulations, privacy laws, and project requirements adapted to the application domain. These results are described at a conceptual level which does not reflect technical interdependencies.

Formal methods for privacy analysis are mostly based on languages which describe technical systems. The purpose is to provide a formal defined vocabulary to avoid ambiguity, to make domain assumptions explicit, to prove properties of a solution, and to explore the design space. Different languages (mostly logic based) and mechanisms (e.g., model checking or system simulations) exist which can be used to provide (semi) automatic evaluation and verification of systems. Technical privacy requirements involve system-specific properties but often fail to integrate high-level privacy requirements that include privacy regulations or stakeholders' interests.

Current research activities focus on improving existing mechanisms of privacy analysis, and some of them try to integrate the different perspectives into a holistic approach. Such approaches try to create a privacy recognition cycle which in one direction injects privacy criteria into a system, while the opposite direction evaluates system behaviour and properties to calculate privacy indicators, as seen in Figure 7.

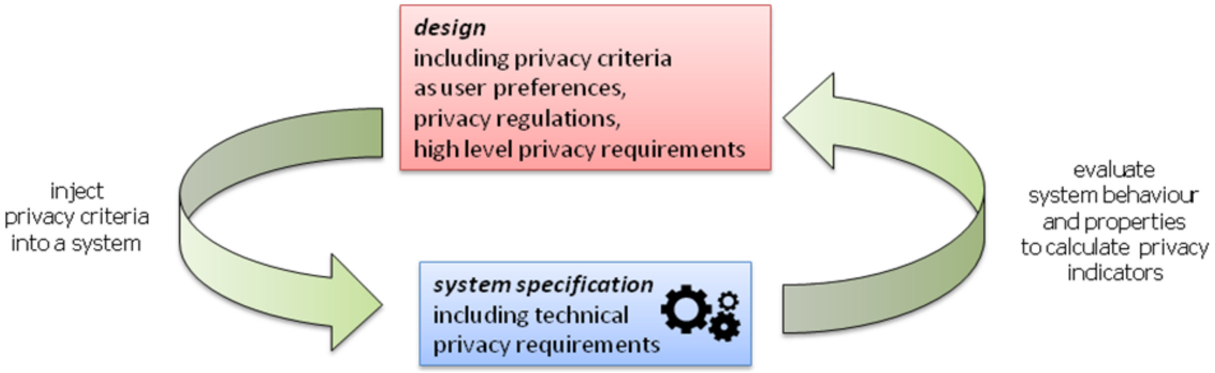

Figure 7: Privacy Recognition Cycle

To adequately implement privacy criteria of different stakeholders, high level privacy criteria (described in the language of stakeholders as data subject and data controller) must be translated into technical requirements which can be analysed and implemented by formal methods and tools such as PETs. Currently, the process of translating high level requirements (such as the results of a Privacy Impact Assessment) into technical requirements is poorly understood. There exist several challenges to translate descriptions from one language into another because the languages address different purposes and thus have different techniques of expression and focus on different aspects. Thus, while performing the translation process, some details of the original description are often lost. Such effects must be taken into consideration with the guarantee that they do not affect the intended purposes. To address these challenges, promising approaches create a shared understanding of the privacy domain by creating standard definitions in form of models and ontologies. We may use these standards to extend the existing analyses by integrating requirement engineering mechanisms, best practices, design patterns, and other well-understood techniques.

5.2.2 Privacy Evaluation

Privacy evaluation must take place at least at three levels:

- A user-centric vision must be provided which will allow the end user to have an understanding of possible privacy profiles and to evaluate whether it matches his own preferences. This will involve initiatives for creating public awareness and initiatives for defining and standardising profiles, with the notion of default values in order not to harass users with too many on-the-spot warnings.
- An engineering-centric vision where existing ICT-based systems can be evaluated. This involves evaluating the process, i.e., verifying that systems are designed with the right methodology. Further privacy protection profiles could also be defined, and evaluation could ensure that a given implementation conforms to well-established profiles. A specific problem that needs to be addressed is incremental evaluation, i.e., how to evaluate individual subsystems and then evaluate the integration of these systems.
- A business stakeholder vision where the roles of the data controller and the data processors must be clearly analysed and evaluated. The problem here is the transfer of liability between stakeholders.
- On top of this is the problem of privacy metrics. There is no general consensus how the level of privacy experienced by a person should be quantified and measured. This would be a pre-requisite for comparing different approaches and evaluating if investments in privacy protection are well spent.

5.2.3 Model Based Engineering Vision

This section is based on the work presented at the PRECIOSA Workshop on Privacy in ITS Applications [23]. Model-driven engineering is the current trend towards a better design approach in general software and systems engineering. We aim at applying this advancement to privacy design.

In brief, models are specifications, often in graphical format, which provide an understandable abstract view of specific aspects of complex systems. With models, engineers can focus on or ignore details in line with their interests. In general, everything can be specified by models.

The whole challenge of model-based engineering is to come up with a collection of models which accurately describe the various parts of the process while maintaining consistency between the models, as various models are often related. For instance, a model describing an ITS application (e.g., using the e-Frame language[8]) would have to be consistent with the chosen privacy model.

In model-driven engineering, this is addressed through model transformation techniques. For example, a well-known transformation establishes the bridge between a platform independent level, e.g., the importer/exporter subsystem in the PeRA architecture, and a platform specific level, e.g., V2X communication in the 5.9 GHz band.

The advantage of a Model-Driven Engineering (MDE) approach for privacy is that it ensures horizontal separation of concerns while providing a specific view and representation and allowing for smooth integration of Privacy by Design. Figure 8 shows how this could impact the overall process:

- Privacy analysis could involve a formal verification process, leading to some proof-related artefacts. An artefact is an artificial product or effect observed in a natural system, especially one introduced by the technology used in scientific investigation. For instance, a relevant artefact for embedded systems is time or a resource constraint.
- An engineer could carry out the Privacy by Design process sketched above, leading to PbD artefacts.
- An ITS application engineer could apply his own application development process.
- Vertically, MDE would ensure the integration consistency of the artefacts.

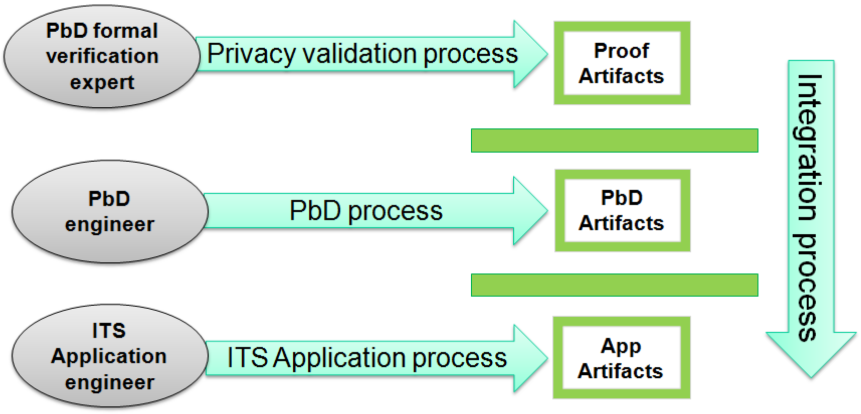

Figure 8: Model-Driven Engineering Vision

5.3 Standardisation and Interoperability

The hurdles of standardisation and interoperability are perhaps the most critical ones. Some of the specific issues are briefly discussed in the following sections.

5.3.1 Interoperability

Interoperability of ICT-based applications and in particular of ITS applications is widely held to be one of the major issues in the digital agenda. In the case of ITS, an initiative for a common language is being carried out through the ITS Frame initiative [8]. The impact of privacy has been discussed with the ITS Frame stakeholders. PRECIOSA members proposed that ITS Frame should be extended to include a user-oriented vision. For instance, the notions of user-defined privacy level and of user preferences would need to be standardised and consequently integrated in the ITS Frame architecture. Technically, the ITS application ontology would need to be extended with a privacy ontology. ITS Frame technicians argued that this would not be a proper way to proceed because from an ITS application point of view, privacy is a non-functional requirement and thus it must be separated. However, it was recognised that from a privacy viewpoint, the privacy ontology is fully functional.

As a result, it was agreed that a parallel ontology would need to be defined by specific stakeholders, but coordination would be needed so that the two “languages”, an ITS language and a privacy language, can be used jointly. Technically this would be solved with some type of transformation bridge connecting the two ontologies. This could be solved through a model-based approach, as explained in the previous section.

Another issue that is not specific to privacy is the bridging from the functional level to the implementation level, and how to ensure that an agreed specification at the functional level is reproduced at the implementation level. This again could be technically enforced through the model-based engineering approach.

5.3.2 Process for Consensus Building

Consensus building is needed when potential conflicts of interest arise in an industry. This was the case for pollution prevention and the IPPC directive [35], where chemical business stakeholders had to reach consensus with environmentalist stakeholders. This was solved through the Sevilla process [37] where working groups with the help of the European Commission (a staff of 20 permanent persons in Sevilla) worked jointly towards common reference documents on Best Available Techniques for pollution prevention. The challenge for the consensus builders is to combine the notion of “best” and the notion of “available”. This approach has been mentioned by the EDPS in their opinion of the ITS directive [38].

The same level of conflict occurs between eSafety stakeholders, for example when deploying ITS applications to improve safety on the road while at the same time ensuring that personal data are well protected.

5.4 Comments on Cost Effectiveness

The motivation of integrating PbD in the future will be manyfold:

- Stakeholders investing on an ITS application or its associated infrastructure wish to ensure that they comply with regulations

- Privacy could be a sufficiently important consumer concern that solutions to handle it could become a selling argrument.

We believe that in the coming years, supporting PbD will be considered as a burden rather than as a feature. Therefore the decision on a minimum set of data and the associated PETs could be the result of conflicting discussions between stakeholders focusing on the ITS application value and stakeholders focusing on the Privacy value. Consensus is needed to reach a position in the middle where an application can be deployed with sufficient value while being based on accepted privacy protection mechanism.

To conclude, we believe that additional engineering cost of integrating PbD is not an issue. On the other hand, the additional deployment cost to integrate a PET is an issue. As long as the support of PET is considered as additional cost, it is important that this additional cost is limited. For instance adding 10% additional cost to an in-vehicle box, will probably be acceptable. On the other hand, tripling the cost of an in-vehicle box will not be acceptable.

6 Conclusion

This document provided a broad overview of privacy approaches and guidelines in the non ITS world and discussed how they could be transferred to ITS scenarios. Beyond that, it identified that the currently often discussed Privacy-by-Design approach needs to be backed up by a technical PbD engineering process and sketched a methodology for such an approach. This methodology needs further refinement and work and Section 5 gives some directions for future efforts.

This deliverable will be an input to the eSecurity Working Group for work that will lead to further results along these concepts and new recommendations on Privacy by Design. At this point, we have identified the following high-level recommendations:

- Create Privacy by Design as a discipline. This involves (1) defining the process and related tools, e.g., a model-drive approach, and (2) changing the education curriculum. The launch of a dedicated Network of Excellence is planned that will address these issues in a broader setting beyond ITS privacy.
- Create a consensus scheme, for instance based on the Best Available Techniques [37] approaches used in the IPPC directive [35].

7 Acronyms

Acronym	Meaning
API	Application Programming Interface
BAT	Best Available Techniques
CAE	Controlled Application Environment
eCall	Emergency Call
EC	European Community
EDPS	European Data Protection Supervisor
EU	European Union
FIPs	Fair Information Practices
ICO	Information Commissioner's Office
ICT	Information and Communication Technology
IPPC	Integrated Pollution Prevention and Control
IT	Information Technology
ITS	Intelligent Transport Systems
MDE	Model-Driven Engineering
MIP	MPC Integrity Protection
MPC	Mandatory Privacy Control
MSD	Minimum Set of Data
OBE	On-Board Equipment
OECD	Organisation for Economic Co-operation and Development
PAYD	Pay As You Drive
PIA	Privacy Impact Assessment
PbD	Privacy by Design
PeRA	Privacy-enforcing Runtime Architecture
PET	Privacy Enhancing Technology
PIA	Privacy Impact Assessment
PPP	Personal Privacy Preferences PPP
RFID	Radio Frequency Identification
RSU	Road Side Unit
V2I	Vehicle to Infrastructure communication
V2V	Vehicle to Vehicle communication
V2X	Vehicle to any communication
WG	Working Group
WP	Working Party

8 References

Working Groups, Organisations

[1] Article 29 Working Party, http://ec.europa.eu/justice/policies/privacy/workinggroup/index_en.htm

[2] Carnegie Mellon Cylab, Project Nudging Users Towards Privacy, http://www.cylab.cmu.edu/index.html

[3] eCall http://ec.europa.eu/information_society/activities/esafety/ecall/index_en.htm

[4] EDPS Data Protection Supervisor, http://www.edps.europa.eu/EDPSWEB/edps/site/mySite/pid/30

[5] eSafety Forum, http://ec.europa.eu/information_society/activities/esafety/index_en.htm

[6] eSecurity Working Group, http://ec.europa.eu/information_society/activities/esafety/forum/esecurity/index_en.htm

[7] European Convention for the Protection of Human Rights and Fundamental Freedoms, http://conventions.coe.int/Treaty/en/Treaties/Html/005.htm

[8] European ITS Framework Architecture, http://www.frame-online.net/

[9] Information Commissioner's Office (ICO), UK, http://www.ico.gov.uk/

[10] Resolution on Privacy by Design Resolution, 32nd International Conference of Data Protection and Privacy Commissioners, http://www.ipc.on.ca/english/Resources/News-Releases/News-Releases-Summary/?id=992

[11] United Nations, The Universal Declaration of Human Rights, http://www.un.org/en/documents/udhr/index.shtml

Publications

[12] Balasch, J., Rial, A., Troncoso, C., Geuens, C., Preneel, B., Verbauwhede, I.; PrETP: Privacy-Preserving Electronic Toll Pricing; In USENIX Security Symposium, 2010, http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.172.8067

[13] Cavoukian, Ann, Information and Privacy Commissioner of Ontario, Canada, Privacy by Design, http://www.privacybydesign.ca

[14] Cavoukian, Ann, Information and Privacy Commissioner of Ontario, Canada, "The 7 Foundational Principles", http://www.ipc.on.ca/images/Resources/7foundationalprinciples.pdf

[15] eSecurity Working Group, "Vulnerabilities in Electronics and Communications in Road Transport: Discussion and Recommendations", http://www.esafetysupport.org/download/working_groups/eSecurity/finalreport/v1/esecurity_vulnerabilitiesinroadtransport_v1.pdf

[16] European Data Protection Supervisor: Data Protection Glossary, http://www.edps.europa.eu/EDPSWEB/edps/site/mySite/pid/84#personal_data

[17] Golle, P. and Partridge, K., "On the Anonymity of Home/Work Location Pairs", in Pervasive 2009 http://crypto.stanford.edu/~pgolle/papers/commute.pdf

[18] Heffernan, B. and Kennedy, E., Alert as 170,000 Blood Donor Files Are Stolen, Nov 2008, http://www.independent.ie/national-news/alert-as-170000-blood-donor-files-are-stolen-1294079.html

[19] Information Commissioner's Office, Privacy by Design Report, ICO, November 2008, http://www.ico.gov.uk/upload/documents/pdb_report_html/privacy_by_design_report_v2.pdf

[20] Information Commissioner's Office, Privacy by Design Implementation Plan, ICO, November 2008 http://www.ico.gov.uk/upload/documents/pdb_report_html/pbd_ico_implementation_plan.pdf

[21] Information Commissioner's Office, Privacy Impact Assessment Handbook v2, ICO, 2009 http://www.ico.gov.uk/upload/documents/pia_handbook_html_v2/index.html

[22] InfoSecurity Magazine, "Norwich Union Life fined £1.26m", Dec 2007. http://www.infosecurity-magazine.com/view/1141/norwich-union-life-fined-126m

[23] Jouvray, Christophe, “The Promise of Model Driven Engineering for protecting private data in ITS”, PRECIOSA workshop. Berlin. Jul 2010. http://www.preciosa-project.org/index.php/workshop-abstracts-cvs

[24] Krumm, J., “Inference attacks on location tracks,” in Pervasive, 2007, pp. 127–143

[25] Ma, Z., Kargl, F., and Weber, M., “Measuring Long-term Location Privacy in Vehicular Communication Systems”, Elsevier Computer Communications, vol. 33, no. 12, 07/2010, http://www.kargl.net/research/publications/view/124

[26] PRECIOSA project glossary of ITS terminology http://www.preciosa-project.org/index.php/its-terminology

[27] PRECIOSA project glossary of privacy terminology http://www.preciosa-project.org/index.php/privacy-terminology

[28] Solove, Daniel, A Taxonomy of Privacy, University of Pennsylvania Law Review, January 2006, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=667622

[29] The Public Voice, Madrid Privacy Declaration, 3 November 2009, http://thepublicvoice.org/madrid-declaration

[30] Westin, Alan F., Privacy and Freedom, The Bodley Head, New York: Atheneum, 1967, http://ann.sagepub.com/content/377/1/196.full.pdf+html

[31] Wiedersheim, B., Kargl, F. Ma, Z., and Papadimitratos, P., “Privacy in Inter-Vehicular Networks: Why Simple Pseudonym Change Is Not Enough”, The Seventh International Conference on Wireless On-demand Network Systems and Services (WONS 2010), Kranska Gora, Slovenia, 02/2010, http://www.kargl.net/research/publications/view/122

Directives, Regulations

[32] Directive 2002/58/EC, Article 15 Concerning the processing of personal data and the protection of privacy in the electronic communications sector: http://www.aedh.eu/Directive-2002-58-EC.html

[33] 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, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

[34] Regulation 45/2001 of the European Data Protection Supervisor http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/DataProt/Legislation/Reg_45-2001_EN.pdf

[35] Directive 2008/1/EC concerning Integrated Pollution Prevention and Control. 15 January 2008, http://ec.europa.eu/environment/air/pollutants/stationary/ippc/index.htm

[36] Directive 2010/40/EU of the European Parliament and of the Council of 7 July 2010 on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:207:0001:0013:EN:PDF

[37] Harald Schoenberger, European Commission. Integrated pollution prevention and control in large industrial installations on the basis of best available techniques – The Sevilla Process. Journal of Cleaner Production. Vol 17 (2009). pp1526–1529. http://www.sciencedirect.com/science?_ob=ArticleURL&_udi=B6VFX-4WHFD48-1&_user=10&_coverDate=11%2F30%2F2009&_rdoc=1&_fmt=high&_orig=search&_origin=search&_sort=d&_docanchor=&view=c&_searchStrId=1507856422&_rerunOrigin=google&_acct=C000050221&_version=1&_urlVersion=0&_userid=10&md5=b7a74d38cb67a2b588ebf4f434c26c3a&searchtype=a

[38] Opinion of the European Data Protection Supervisor on the Communication from the Commission on an Action Plan for the Deployment of Intelligent Transport Systems in Europe http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2009/09-07-22_Intelligent_Transport_Systems_EN.pdf

[39] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html