D62.4

6.4 Privacy & Social Aspects

Work package: 6.2
Version number: Version 1.0
Dissemination level: PU
Date: 11/07/2014

7th RTD Framework Programme
Directorate General for Communications Networks, Content & Technology
Cooperative Systems for energy efficient and sustainable mobility (FP7-ICT-2011-6.7)
Contract Type: Collaborative project
Grant agreement no.: 318485
# Version Control

## Version history

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Main author</th>
<th>Summary of changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.6</td>
<td>24/03/14</td>
<td>Thierry Jacquin</td>
<td>First review Irene Maxwell - 1.1.2</td>
</tr>
<tr>
<td>0.7</td>
<td>28/03/14</td>
<td>Thierry Jacquin</td>
<td>Jean-Pierre Chanod feedback</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Telecom Italia - Current EU legal status and analysis of Italian regulation</td>
</tr>
<tr>
<td>0.8</td>
<td>04/04/14</td>
<td>Thierry Jacquin</td>
<td>Torino meeting</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Volvo - use case, traffic data example</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ACASA - use case, FAI position + iMobility Forum input</td>
</tr>
<tr>
<td>0.9</td>
<td>22/05/14</td>
<td>Thierry Jacquin</td>
<td>Consolidation and second review (Jean-Pierre Chanod)</td>
</tr>
<tr>
<td>1.0</td>
<td>11/07/14</td>
<td>Thierry Jacquin</td>
<td>Finalized (Mobinet position clarified based on comments from reviewers in 5.4 and conclusion)</td>
</tr>
</tbody>
</table>

## Name and Date

<table>
<thead>
<tr>
<th>Name</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prepared</td>
<td>Thierry Jacquin (XEROX)</td>
</tr>
<tr>
<td>Reviewed</td>
<td>Yanying Li (ERTICO)</td>
</tr>
<tr>
<td>Authorised</td>
<td>Paul Kompfner (ERTICO)</td>
</tr>
</tbody>
</table>

## Circulation

<table>
<thead>
<tr>
<th>Recipient</th>
<th>Date of submission</th>
</tr>
</thead>
<tbody>
<tr>
<td>European Commission</td>
<td>11/07/2014</td>
</tr>
<tr>
<td>Project partners</td>
<td>11/07/2014</td>
</tr>
</tbody>
</table>

## Main Author:

Thierry Jacquin (XEROX)

## Additional contributors:

Guillem Bernatallada (ACASA)

Marcus Enered (Volvo)

Domenico Enrico Bena (TI)

Jean-Pierre Chanod (XEROX)
# Table of contents

Introduction .................................................................................................................. 6

1. Privacy as a fundamental right .............................................................................. 7
   1.1. The current legal status of personal data protection in Europe ..................... 8
   1.2. The General Data Protection Regulation: the new (delayed) Regulation ....... 10
   1.3. The lobbies reaction ...................................................................................... 13
   1.4. Potential side benefits ................................................................................... 14
   1.5. The international stakes ................................................................................. 15

2. Geolocation, a central privacy challenge for ITS .............................................. 17
   2.1. A new kind of raw data .................................................................................. 17
   2.2. The value of geolocation in exchanged data ................................................ 19
      2.2.1. Emerging trend: Sticky policies ............................................................... 19
      2.2.2. Sticky policies in Mobinet context ......................................................... 19

3. Generic privacy aspects with respect to ITS ..................................................... 21
   3.1. Exchanged data and associated concerns ..................................................... 21
      3.1.1. Data Location .......................................................................................... 21
      3.1.2. Communication phase ......................................................................... 22
      3.1.3. Security .................................................................................................. 22
   3.2. Privacy sensitive ITS application and services ............................................. 22
      3.2.1. Location-based services and traffic data ................................................ 22
      3.2.2. Third party eCall as a private Service ................................................... 23
      3.2.3. In-vehicle telematics services ................................................................. 23
      3.2.4. Road User Charging ............................................................................. 24
      3.2.5. Pay as you Drive, Pay as You Drive Insurance ...................................... 25
      3.2.6. Traffic data collection ............................................................................ 26
      3.2.7. Cooperative systems .............................................................................. 26
   3.3. List of privacy-friendly approaches to actively promote .............................. 27
   3.4. Mobinet privacy approach ............................................................................ 27
   3.5. The Preserve project – preparing secure v2x communication systems ...... 28

4. User awareness ........................................................................................................ 29
   4.1. Risks .............................................................................................................. 30
      4.1.1. Personal risks .......................................................................................... 30
      4.1.2. Business risks ......................................................................................... 31
      4.1.3. Societal risk ............................................................................................ 32
D62.4 Privacy & Social Aspects

4.1.4. Privacy by Design, the current guidelines to manage the identified risks ........33
4.2. Trust and Acceptance ..........................................................................................35
4.3. Social Aspects .....................................................................................................36
  4.3.1. The social impact of Social Networks ..............................................................36
  4.3.2. Current Privacy Issues ....................................................................................37
  4.3.3. Big Data trend and related public clouds initiatives .........................................38
4.4. Data ownership perspectives ..............................................................................38
4.5. User awareness vs. community awareness .........................................................41
5. Responsibilities and Actors ....................................................................................42
  5.1. Public security vs. Democracy ...........................................................................42
  5.2. Technical Security vs. Operational Excellence ..................................................42
    5.2.1. Access Control Lists .....................................................................................42
    5.2.2. Encryption ...................................................................................................43
    5.2.3. Certificates ...................................................................................................44
  5.3. Business performance and Privacy Lifecycle Costs .........................................45
    5.3.1. Privacy-aware applicative design .................................................................45
    5.3.2. Privacy-aware application development ......................................................45
    5.3.3. Privacy-aware application deployment .........................................................46
    5.3.4. Privacy-aware applicative maintenance ......................................................46
    5.3.5. Privacy-aware application governance .........................................................47
  5.4. The Mobinet Privacy Framework: an interpretation of Privacy by Design for agile platforms 47
6. Conclusion .............................................................................................................49
References .................................................................................................................50
# Abbreviations and definitions

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACL</td>
<td>Access control list(s)</td>
</tr>
<tr>
<td>DPA</td>
<td>Data Protection Authority</td>
</tr>
<tr>
<td>GDPR</td>
<td>General Data Protection Regulation</td>
</tr>
<tr>
<td>GFAC</td>
<td>Generalized Framework for Access Control</td>
</tr>
<tr>
<td>IPC</td>
<td>Inter-Process Communication</td>
</tr>
<tr>
<td>OBU</td>
<td>On-Board Unit</td>
</tr>
<tr>
<td>PIA</td>
<td>Privacy Impact Assessment</td>
</tr>
</tbody>
</table>
Introduction

The purpose of this Mobinet Deliverable is first to shed light on emerging line of thoughts regarding personal data protection in the digital world, and then to analyse in depth implications in the context of ITS.

With the widespread circulation and dissemination of data in a hyperconnected world of services, personal data protection expands far beyond the perceptions and concerns traditionally associated with privacy. This new thinking involves multiple areas of expertise (legal, politics, sociology, technology, economics, business) that typically evolve along different perspectives and cycles. This document will make it apparent that, under such conditions, no one has the authority to negotiate a consensus among all the different stakeholders.

One can anticipate that the time needed to elaborate a consensus on privacy in the digital world and to implement acceptable solutions will be huge. Meanwhile, privacy issues will grow at an impressive pace due to new technologies, offerings and practices induced by the internet and even more so with the upcoming internet of things.

The accepted consensus on privacy in Europe today is bound to the Charter of Fundamental Rights of the European Union, which recognizes privacy as a fundamental right. This will be examined in the first Section of this document, with particular attention to the digital dimension. Our core reference will be the General Data Protection Regulation (GDPR) through which the European Commission decided in 2012 to tackle the challenge of defining the future rules for managing private data (European Commission, 2012).

Then this document will dig into this broad topic under the specific angle of ITS.

Section 2 will consider the type of data most relevant to ITS services, that is geolocation. We will review privacy challenges associated with geolocation, based both on EU and US cases.

Section 3 will address the nature of exchanges in ITS, based on services. This will naturally bring to light specific issues related to data ownership.

One area of consensus among the various stakeholders of digital privacy today is the need for user awareness. We will see in Section 4 that this may have multiple interpretations, depending on backgrounds and interests.

Finally, Section 5 will reconsider those points with the aim of identifying the Responsibilities and Actors that could contribute various elements of solution for privacy enforcement. The Section will identify methodological gaps and limitations that make the building of a consensus extremely difficult. We try to identify how filling these gaps will help establish principles and rules for user awareness and data ownership. We will then indicate how Mobinet can contribute a set of propositions, which, considered with alternative endeavours, should put stakeholders in a better position to accelerate the building of a consensus on digital privacy.
1. Privacy as a fundamental right

The Charter of Fundamental Rights of the European Union considers data protection as a fundamental right, distinct from the respect for private and family life. This feature sets the EU Charter apart from other major human rights documents which, for the most part, treat personal data protection as an extension of the right to privacy (European Parliament, 2000).

We will see in this section that such a fundamental right (as all the others considered in the past e.g. slavery abolition), need time and context to impose on society. The following sentence from Viviane Reding, the EU Justice Commissioner, and one of the initiators of the regulation project about personal data protection (European Commission, 2012), highlights this dual character: “[…] some companies and a few governments continue to see data protection as an obstacle rather than as a solution; privacy rights as compliance costs, and not as an asset.” Ms. Reding, expressed her regret after the decision of the Commission to delay the regulation vote to the end of 2014, forced by the number of requests for modification from EU member countries. Meanwhile, the general public reached a level of awareness of surveillance abuse, mainly through the Snowden case. Even in the US, the subject of personal data protection became highly visible and political. In particular, the full scope of contemporary political dialectics on collective security versus individual freedom, but also between public and private investment, and ultimately between jurisdiction and market law is more than present in the landscape of digital privacy.

As such, the debate also encompasses some diplomatic aspects, since the EU regulation would tend to reinsert the notion of territory into the wild ocean of the Internet, just like the Brazilian Civil Rights Framework for the Internet (or Marco Civil da Internet) does in Brazil (D. Doneda, 2014). Countries such as China have decided not to let their citizens navigate such extra-territorial areas. This radical approach seems a bit extreme to most of us, but we should also consider that public authorities are tempted to consider such solutions to reconnect the digital world with territoriality:

"Merkel said in her weekly podcast that she disapproved of companies such as Google and Facebook basing their operations in countries with low levels of data protection while being active in countries such as Germany with high data protection. ‘We’ll talk with France about how we can maintain a high level of data protection,’ Merkel said. ‘Above all, we’ll talk about European providers that offer security for our citizens, so that one shouldn’t have to send emails and other information across the Atlantic. Rather, one could build up a communication network inside Europe.’ Hollande’s office confirmed that the governments had been discussing the matter and said Paris agreed with Berlin’s proposals."

Figure 1 – extract from http://www.reuters.com/article/2014/02/15/us-germany-france-idUSBREA1E0IG20140215

This potential negative perspective explains why it is now time to work in a more positive direction, wherein territoriality can be ignored since personal data would be internationally managed in a responsible and respectful way. There is still time to privilege this option, if we all invest our collective intelligence towards the right goal: preserving the immense potential of a global, shared Internet, a vehicle of knowledge and social interaction, supporting every day new business avenues and collaboration improvements.

To achieve this, we must understand what kind of responsible data management is necessary. As primary source of reflection, we will use all the significant work that has been done to elaborate the draft EU Regulation, as indicated in the introduction. We will revisit some details of the draft Regulation together with some elements of lobby reactions which caused delays and prevented a final decision to
be made by the EU Parliament before the 2014 elections. We will then review some of the expected (and often unconsidered) benefits to be gained when the Regulation is adopted. Finally, we will underline the political stakes hidden behind the ‘fundamental right’ flag.

1.1. The current legal status of personal data protection in Europe

The increasingly widespread use of ICT tools, as well as its continuous technological progress, has sharpened the focus on privacy and made more sensitive the European legislator and the national laws in regulating this issue. In fact, the use of collaborative computer tools is associated with an increasing risk that personal data are disseminated in an indiscriminate and uncontrolled way and that its preservation for the future may be jeopardized. Therefore, European and national legislations have been developed in order to ensure that the processing of data carried out through such tools happens in a lawful manner and in accordance with an explicit and legitimate purpose and also in respect of certain security “computing” measures to prevent unauthorized access to personal data, as well as their loss.

Within this context, and in accordance with current legislation, personal data are protected under their two operational facets:

- procedures for the processing and handling of personal information (from simple storage of such information, to processing and dissemination);
- the means by which personal information is handled (from the traditional ones, e.g. paper files, to more modern ones, e.g. ICT systems).

As indicated earlier, the European legislation should significantly change when the GDPR eventually gets adopted. Meanwhile, the current legal framework applicable in EU is based on two Directives:

- Directive 95/46/EC 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 (European Commission, 1995);

The two Directives on privacy listed above have been implemented by the various Member States, letting them introduce specific rules for each national context, while ensuring the application of the general principles established by the European Directives. As a consequence, the regulatory framework regarding privacy of each individual Member State of the European Union, although united by reference to the principles enshrined in the EU Directives, has some specificity, which should be analyzed in order to have a complete knowledge of the rules applicable for MOBiNET in the national context considered.

For example, the main differences between the European and Italian national guidelines are centered on some aspects, which are listed and described in the following points:

- Use of anonymous data in the data processing by means of ICT tools. With regard to this aspect, the Italian law is more restrictive than the Community regulation. In fact, the national Privacy Code requires the use of the data in anonymous form, in the case of data processing carried out with the help of computer and if the purpose of the treatment allows it. This provision translates in a more complex management of data processing, which requires to make
anonymous the data in a preliminary stage of an activity. **Balance between costs and benefits of security measures** to be taken in the context of data processing. With regard to this aspect, the Italian legislation does not require a preliminary analysis of the security measures in order to assess the costs and benefits and guides the choices of those which are more appropriate to be adopted for the data processing. For the Privacy Code, however, it is necessary that the security measures are proportionate to the type of data processing (e.g. storing, retrieving, etc.) and the nature of the data. Thus, the Italian legislature has, in this context, less restrictive measures than the European one, with the objective to preserve more data security at the expense of the economic implications related to their treatment.

- Specific definition of “health information” and rules for the healthcare domain (out of scope in this document)

Location data are not defined as "sensitive data", unless they can be used as suitable to reveal the health status of individuals. Nevertheless, one can anticipate that most individuals will want to consider the information about their location and the places visited as a personal resource to be guarded and not spread. Managing security and privacy are therefore very important for the services based on positions and location tracking, and the overall design of the Mobinet platform must take this into account.

**National discipline for data security and privacy**

This discipline, that comes in particular by Law 196/2003 or the National Italian “Privacy Code”, provides a set of rules that must be followed for the operation of processes (pre-processing, processing, post-processing) in which it is possible to articulate the management process of personal data.

These general rules, therefore, should also be applied to the processing of personal data carried out by the MOBiNET Platform and provide as follows:

- **pre-processing** of personal data
- **processing / use** of personal data
- **post-processing** of personal data

The **Pre-processing of personal data** groups the activities by which a Company proceeds to duly inform the concerned person about the main features of the processing applied to their personal data, as well as to get their approval to process those. The existing law provides that it is not possible to proceed to process personal data without first having informed the person concerned on how the Company plans to treat and use the data (“release of the information”) and having acquired the permission of the person concerned to do so (“detection of consent”).

About the process of **use of personal data**, the existing law provides that personal data must be processed "fairly and lawfully ", "collected and recorded for specific, explicit and legitimate purposes" and also defines a set of safety measures to be taken in case of treatment with ICT tools. This process groups the activities by which the Company proceeds to the actual processing of the data (e.g., collection, consultation, dissemination, etc.). These activities shall be made in accordance with certain conditions that define, in a timely manner, the operational procedures and safety measures to be adopted in the execution of data processing. Specifically, this process is embodied in the activities of “Data processing” and “Management of data security”. The national legislation provides, during the processing of data, to adopt safety measures appropriate to avoid the loss / accidental modification of data, as well as the access to them by unauthorized persons.
Figure 2 National discipline for data security and privacy

Data exchanges between the EU and the US are ruled under a negotiated umbrella called Safe Harbour. The process was developed by the US Department of Commerce in consultation with the EU, as a means for US companies to comply with the EU Directive 95/46/EC on the protection of personal data. When companies, for operational reasons need to transfer data from one side to the other, they must inform authorities about the transfer, motivate the exact need of the transfer and detail all the protective actions taken in order to protect the transferred data.

1.2. The General Data Protection Regulation: the new (delayed) Regulation

The current draft EU Regulation (GDPR) plans to constrain all business players in asking their customers their consent for capturing or using personal data. The informed and explicit consent of the data subject for will be requested (and preserved) for any storage and processing of personal data. Service providers will be accountable for any further usage of the captured data. They also will be liable for any processing which would not respect the consent provided by the data subject.

This is very demanding for business, and the question of enforcement and its related cost, follows immediately the expression of such intended obligations. The global cost of enforcement (roughly distributed on administrative, legal, police and technology activities), would have to be shared between the public authorities, the business players and potentially the citizens. What is the ideal split? Not surprisingly, such an important question is difficult to answer as nobody knows the amount of the bill, as the level of investment has yet to be determined.

Whatever distribution of the financial cost (sometimes called proportionality) is adopted, there is an additional cost to be considered: the cost of heaviness. This corresponds to the generally accepted assumption that the more norms and constraints public authorities apply to businesses, the less fluid and
efficient these are to adapt to evolving contexts. No need to say that the current context is constantly evolving, and for this reason this longer-term cost threatens particularly the entrepreneurial leaders and their political counterparts. The competitiveness of Europe is such a structuring subject of debate in Europe with respect to the global economy that it is very difficult to re-introduce this debate for the next wave of the globalization. Many anticipate the future use of Internet capacities will support not only the commercial or service-oriented operations of today, but also very soon the design and production of goods. When such a prediction realizes, we can foresee a drastic change in the nature of global competition, based on an intense communication process of operational data, centred on the needs of individual customers. Then, all the industrial data connected to this customer can be considered private, and will need to be treated as such in Europe. Thus, the competitive challenge will not be restricted to the basic e-commerce mechanisms known today: all the layers of economic activities involved in the production lifecycle will be impacted and under competitive pressure from a data exchange perspective.

As we will develop hereafter, other voices present this risk as an opportunity. There is still time to provide acceptable solutions, in order to be among the rare potential providers for such future strategic data exchange infrastructures. From an institutional point of view, some countries (e.g. UK) tend to privilege the consideration of short-term risks, fearing the direct economic consequences of obligating European businesses to compete while handicapped by stricter privacy obligations. Nevertheless, the long-term trends identified above remain huge opportunities but, as usual, the investment motivations will be harder to define for those who would like to bet on this anticipated future.

One could also signal that the current draft Regulation also suffers from the fact that very few technical means are foreseen to help in implementing privacy enforcement from a technology perspective. An evidence of this technical gap can be seen in the modification of article 23, stipulating originally that some help would be provided to comply, before eliminating references to cost effectiveness and eventually focusing on the sole intent behind the obligations:
The comparison between the two versions of Article 23, somehow highlights the lack of maturity of the domain. They also show the sense of emergency to solve this issue. In one hand, how could technological support be part of a regulation? On the other hand, is it conceivable to renounce this regulatory intention because of the impossibility to maintain it, due to the scarcity of technical support means? This advocates for urging the software community to provide affordable perspectives in a reasonable short term. This crucial need is acknowledged, not to say amplified, by the European administration itself, through the following statement, captured from section 4.3 in a report produced by Rand Europe for the EU Commission Europe’s policy options for a dynamic and trustworthy development of the Internet of Things’, and in reference to the EU draft regulation on data protection:

As a final remark, we need to report one more issue related to the Regulation, based on a proposed rule, namely the ‘one-stop-shop’ rule. This point is strongly related with the current status presented in the
previous section. The ‘one-stop-shop’ rule aims at facilitating the compliance for companies located all over Europe, so that they would have a single Data Protection Authority (DPA) for all Europe for the new regulation enforcement. The goal is to exempt service providers to be controlled by every DPA of every country they operate in and instead to interact with a single one. This one-stop-shop rule seems to be a very hard negotiation point between EU members, since national authorities could be tempted to compete with each other, attracting operational activities with lower data protection obligations, as they already do with taxes. This internal impossibility to reach a consensus could be another element responsible for the delay from the pure procedural perspective.

1.3. The lobbies reaction

Due to the obvious lack of technical means, and to the current economic situation of Europe, many voices are arguing that the new Regulation should not be enforced at this very moment. But others claim that, when fundamental human rights are not tackled properly, the economy and business adaptation are also considerably slowed down. Thomas Jefferson point of view (THE THOMAS JEFFERSON MEMORIAL ASSCIATION, 1905) does not strictly reflect this view point, but a kind of counterpart of it: It is for the people against the introduction of a new right to demonstrate that there is no need for this right. Nobody should pay the price of their opposition to the right.

In the above excerpt of http://www.constitution.org/tj/jeff16.htm, the considered right is land ownership. Should anyone be the owner of a land for being the first to cultivate it? This crucial American question was controversial for legacy land owners who argued against this new right, on the ground that they provided significant employment to cultivate their land and that jobs would disappear should the new right apply. Jefferson’s counter-argument was basically: land owners' position cannot be defended if they are not able to employ all the people who would be in a position to support themselves thanks to the new right.
We could attempt an analogy with the EU regulation as follows: if the European service providers are not in a situation to compete now, without the privacy Regulation handicap, then what is there to be lost with introducing this new right? This is not a matter of speculating about future competition to come with the Internet of Things that should lead the vision, but rather facing the reality about the current situation. We must admit that Europe is very late in the Internet based business, and should take advantage of this for establishing new rules and so, new frontiers, based on data ownership, as Jefferson did with work on the land.

In a sense, whatever political point of view one adopts, the essential technological challenge is to lower the global bill of the enforcement of personal data protection. Only such an approach can guarantee that fundamental human rights associated with personal data protection (with an exponential increasing importance) be affordable for modern societies. There is a duty for technology to provide the conditions of enforcement at a reasonable cost, within a reasonable timeframe, prior to deciding where the contribution for such a cost would come from. That it be short term is also crucial, since current technological trends are amplifying the effort required to protect personal data. Every hour, an impressive number of new devices connect to the Internet, and feed it with unprotected personal data such as pictures, emails, identities and geolocations. The more time the technology will take to solve the problem, the heavier the implementation of a solution will be, and the weaker our democracies will become.

1.4. Potential side benefits

Furthermore, if this first essential challenge were addressed for the sake of fundamental human rights and democracy sustainability, some huge positive side effects for western economies could be anticipated. Amongst these potential promises, the first which comes to mind is the ability to associate quality and hence value to exchanged data, subsequently entering the data monetizing space in a sound way. Some initiatives are going in this direction, such as the study (ENISA, 2012) on monetizing privacy by the European Union Agency for Network and Information Security (ENISA):

![ENISA releases two new reports on privacy economics and case studies of online practices in collecting and storing personal data in the EU](image)

ENISA launches two reports with recommendations on personal data protection.

Privacy is recognised within the EU as a fundamental right, but what is the current economic reality? Are online customers willing to pay for privacy? Do individuals value their privacy enough to pay more to service providers that protect their information better? The ‘Study on monetising privacy: An economic model for pricing personal information’ is the world’s biggest study of privacy economics and connects the dots between the interaction of personalisation, privacy concerns and competition between online service providers.

This very interesting approach cannot be an incentive to privacy, but should be the consequence of an efficient safeguarding of personal data. Else, the average quality of traded ‘personal’ data will be very poor. One particular aspect of the big data is that it is big. The speculative aspect is then focused on the size aspect, and this should not change, due to constant new occurrences of data generating technologies. This means that the market driver, the key element of pricing will remain the volume, and nobody can predict the necessary incentives to boost qualitative approaches in such an ever-growing market. One incentive could be personal data protection itself. The time spent to consent explicitly to expose some private information to specific and trusted services indicates data quality.

From the user point of view, there are two ways to keep some privacy with online services. The first one is to only use trusted services in their nominal behaviour. The second is to build a fake identity, and
disconnect the registered user of the service from the living individual as much as possible. This tactical approach is already used and leads to a huge number of fake or dirty personal data. Of course, the ‘virtual’ individuals do not spend much time in managing their privacy when services would provide such means. As a result, the measure of the time spent to manage private aspects by the user herself could indicate the level of authenticity or actuality of the data provided. Based on such a criterion, and possibly only then, the monetizing phase could happen.

From a more short-term and practical perspective, the big data trend also plans to statistically model some categories of users based on their behavioural similarities within the service scope. This is often realized with classification or clustering algorithms. These algorithms of categorisation and clustering are mainly based on the notion of a computed distance and some thresholds to decide if an instance enters a group or not. The evaluation of this distance is based on the instance characteristics, or features. The more precise these features are, the more accurate the categorization is. Also, the learning phase of the models used at the time of the association highly depends on the features quality. Also, higher precision on the input data will certainly give the possibility to integrate some marginal instances more easily. In other words, mean is no more a norm, and diversity could be part of the assisted knowledge. Some other advantages could be a more trusted relationship between the citizen and the institutional bodies, or between customers and providers. Ultimately, and specially in anticipation of the emergence of the Internet of Things, tailoring an optimal adaptation for individuals to a pervasive wired environment, together with a greater individual freedom depends a lot on our ability to deliver technology sustaining this due balance at a very low cost.

1.5. The international stakes

As mentioned above, the Regulation draft is also an attempt at redefining and prefiguring future national supremacies based on data capture, and digested knowledge. Defining clearly who is responsible for controlling data referring to European subjects is a matter of the highest economic and strategic importance for the next decades. Within this US/Europe/Asia diplomatic ballet, one can also see the public/private battle. It has always been the privilege of public authorities to manipulate citizens’ data, for personal or collective usage. A new era is appearing now where private companies can analyse public phenomenon better than the authorities in charge of such a phenomenon. A typical example is the crisis response tool provided by Google, which aims at making available critical information around natural disasters and humanitarian crises. Google’s contributions can include: updated satellite imagery, charitable donations to organizations on-the-ground, outreach through Google web properties, and engineering products and information services, such as Google Person Finder and Landing Pages, designed to organize and coordinate critical response information.

This very efficient tool puts Google in the position of first player in case of emergency, leaving the traditional public and even NGO actors in the background of the scene. A lot of ethical problems appear in such situations. We are at the very beginning of an era where private actors may put in place more powerful means than public authorities, to help citizens in crisis situations. This constitutes an obvious problem for governments. The following anecdote shows this may happen not only in time of crisis, but even in some day-to-day situation, due to the infrastructure size such private companies can align in front of governmental digital infrastructures:

With such examples, we understand that it is a question of re-gaining control on all the business actors involved in data capture, which is the essential target of the Regulation. This is not only a question of letting our democracies run their digital world with their own rules, but also a question of letting many actors compete in a sane market, independently from the size of their own infrastructure. It has always been the power and duty of public authorities to provide infrastructure such as highways, energy and health to their citizens, putting them in the position to develop the territorial economy. We clearly understand that European countries need to put themselves in the same situation with respect to the digital economy, knowing that all the infrastructure investments have already been realized abroad.

This wide context having been provided, demonstrating that behind the exposed principle of ‘Privacy as a fundamental right’ a number of essential strengths are to be considered from a strategic and diplomatic view, we can then consider privacy and personal data protection from a more practical aspect. We will now consider privacy in a kind of bottom up approach, focusing this time on ITS systems and their privacy related issues, since this is the business domain of Mobinet.
2. Geolocation, a central privacy challenge for ITS

Geolocation data represent a new type of data in the software area. They mainly appeared with mobile phones but the exponential usage of these together with the amplification associated with the upcoming Internet of Things give them a very specific status. In the particular case of Mobinet, we will see that the potential exchange of geolocation data between service providers requires a very precise consideration from the privacy perspective.

2.1. A new kind of raw data

The particularity of geolocation data is that they reveal an aspect of our physicality that was absolutely ignored by previous systems. This new type of data, in the context of software applications, must be considered as private as soon as the emitting device can be associated with a specific person, directly or indirectly. This is true in Europe by application of the directive of 95. In the US, the situation is less obvious, mostly run by jurisprudential history. The US Government site gps.gov provides information about GPS location privacy, including a number of judgements about the authorization for policemen to use GPS traces, depending on the warrant provided by justice (http://www.gps.gov/policy/privacy/)

Facing such recurrent and sometimes inconsistent decisions, the US government is putting in place a bill, namely the Geolocation Privacy and Surveillance act (US Senat - Chaffetz and Wyden, 2012), aiming at defining a legal framework to clarify how personal location information may be used by law enforcement, companies, employers, and others, based on the Supreme Court decision of January 2012 according to which ‘law enforcement must obtain a warrant before physically attaching a GPS tracking device to a suspect’s vehicle’. The Geolocation Privacy and Surveillance act is trying to enlarge this vision in a broader frame, but ‘It is not intended to influence or express opinions on any ongoing legal deliberations’.

The US press is also recurrently addressing this topic with respect to new tracking devices and the potential usage law enforcement could make with such tracking, including sharing of geolocation as indicated in the following excerpt. This is particularly interesting to us, as the notion of sharing is inherent to a collaborative platform such as Mobinet.
In Europe, public opinion seems to be particularly passive with respect to this tracking ability provided by new devices and apps. For example, the legal debate about the French GPS Act proposal does not generate any public debate (cf. http://www.affiches-parisiennes.com/la-geolocalisation-dans-tous-ses-etats-3968.html). This is seen as a pure technical aspect of modern life style. The fact that providers are located outside of the European power is certainly one of the reasons. Another one being the increasing acceptance of surveillance in western collective unconsciousness.

The notion of context and purpose of usage become more and more difficult to manage given the raw and minimal format of geolocation data, and the easy correlation they provide with single individuals. A proposed minimal solution is to make these traces less precise, but precise enough to take benefit of certain services. The proposal is to configure GPS devices in order to add a random shift maximized by a given distance. This works for a single track, but in case of the occurrence of regular routes, the simple overlap of those and the selection of the intersected area will show the real one with very few instances of fuzzy traces. This example highlights another aspect of the geolocation data: these are highly persistent and easy to understand, by a simple projection on a map or by correlation with others. This correlation possibility is particularly important in an exchange platform such as Mobinet. This is why we will consider the exchange of such data with a particular care.
2.2. The value of geolocation in exchanged data

Geolocation data are very easy to exchange and used across application/services boundaries. This cross-usage does not require a complex data model at the basis of the communication. A single North-East coordinate system, associated with any kind of object, provides the position of this object to any processing service which would know which object is concerned. In Europe, this becomes a matter of privacy whenever the designated object is a physical person, or even when the designated object could be matched with another track that could be associated with a given person with an acceptable level of confidence.

In the US, the Geolocation Privacy and Surveillance Act already conditions the use of geolocalized data in a one-to-one relationship of a phone and its associated telco operator (this nominal provider of this specific issue will largely be expanded by the Internet of Things thrive). Nevertheless, as a de facto new kind of geolocalized data exchange platform, Mobinet potentially scales this personal data protection issue to unseen proportions until now. Interoperability promises of Mobinet multiply the problem by more than the number of service interoperating, since the interoperation in itself can be the way to associate a single person behind a geolocalized object. Such correlative techniques are used for surveillance reasons, and must remain under the control of justice. They should not be applicable by the Mobinet platform per se, and individual disclosure should only be possible under legal contexts. This is an absolute condition for Mobinet, in order to grow trust and attraction from the user perspective.

2.2.1. Emerging trend: Sticky policies

The indirect capability of matching requires the services to be very cautious when exchanging geolocation data with other services, particularly with respect to the consent their user gave them. It is to be noticed that the user gave them and only them their consent. If the user allows the service provider to share the data, then such data, when sent to another service, must be managed through a new consent between the second service and the user. There is not transitivity of consent, since the purpose description is under the responsibility of the service itself. If the first service takes the responsibility for the second, then it must describe explicitly the purposes of its subcontractor and becomes liable for any harm done in terms of privacy.

From this point of view, the minimal technology driver to support such exchanges is the notion of sticky policy: such sticky policies should be attached with the data, in order to tell processing services the consented usage from the data subject perspective, considering the processing purposes would be commonly described and understood (Mont, 2011). This minimal driver is also a very demanding one: it implies that all the platform-hosted services are complying with the exposed and explicit purposes. Nevertheless, for a very specific platform, having structured the hosted services through a number of APIs and data models, this minimal driver could be achieved, at the cost of reviewing hosted services to ensure they do implement the real APIs correctly. Under these conditions, it could be the responsibility of the platform to generically describe the APIs in terms of explicit roles, to attach such sticky policies to any data rendered by a hosted service, and finally, through the policy control facility, to filter such data sets to be sent as input when calling the subsequent service API.

2.2.2. Sticky policies in Mobinet context

The platform scheme described in the previous paragraph is not the one chosen by Mobinet as a project. For the good reason of letting the platform mature and host incoming services without constraints, the
service registry is more understood as a switch board, where self-described services may register, each of them under its own responsibility for its own API declarations. Thus, the data processing is no more orchestrated by the platform, only responsible for giving the opportunity for solution programmers to build programs calling APIs from services to services. Under these conditions, the notion of sticky policy is not possible anymore, since Mobinet cannot control and understand the purposes of exposed APIs. This does not mean that privacy cannot be protected in such a relaxed service platform where data models are let under the responsibility of services, and we will detail later on what kind of solution is recommended for Mobinet, based on a one to one consent scheme. The recommended solution must then be based on a privacy-by-default minimization of exchanged data. It will be the responsibility of each service provider to protect by default the privacy of its users, and to exchange only minimized data. The user consent will be needed for expanding such minimized data for explicit purposes of specific services. From the pure Mobinet point of view, the platform will only be responsible for protecting the collected geolocation data within the MobiCentre by default, to secure the communication between MobiAgents and MobiCentre, and to protect personal fields of the MIM component by default.

In Mobinet, the MobiAgent Mobicenter communication is definitely the engine where this couple object/location will be communicated to the MobiCentre, for serving then services which would be able to identify the considered object and offer the best business service solutions with the help of other registered service providers. So far so good, but everybody understands that the Privacy problem arises immediately after the association having been realized by MobiCentre, if this associated object can clearly help in identifying a physical person.
3. Generic privacy aspects with respect to ITS

A very good recommendation about Privacy and Data Protection in the particular context of ITS has been produced by the *iMobility Forum* Working Group in June 2013 (Pascotto, 2013).

The major issues addressed by this group are the following ones: “How can we ensure the protection of data in a transport system where connectivity has been rapidly increasing? How can we promote and build consumer confidence in a world of exploding data volumes? How can we reconcile privacy and digital growth, the rights of individuals and the needs of businesses?” This document gives a clear picture of the novel kind of applications supported by transport businesses, and identifies the associated threats and risk levels in terms of privacy.

Sub-sections 3.1, 3.2 and 3.3 follow the structure of the iMobility report. First we sum up the essential points made in the report and while providing some comments when needed. In particular, we will insert comments about current practices and recommendations expressed by Mobinet partners, in order to underline the following statement: Privacy enforcement must be fair in terms of business, and investors must take benefit from their investment; data collectors such as motorists expect to expand the business derived from captured data, by diversifying purposes for which data can be used, but always in an anonymous format.

Eventually, we will consider Mobinet requirements with respect to the previous points, prior to having a look at the Preserve initiative, which aims at providing and field testing some privacy-aware solutions for V2x systems.

3.1. Exchanged data and associated concerns

This subsection analyses the iMobility report with regard to data.

3.1.1. Data Location

The iMobility report on Privacy and Data Protection states that location data in vehicles can be divided in two cases with regard to data protection: first case, in-vehicle communications through In-vehicle wired interfaces (On-Board Unit [OBU], the most frequent case as of today), where privacy is not a real issue; the second case, on the contrary, where data is communicated outside the vehicle, raises very different privacy issues depending on the technical infrastructure used to transfer, store and diffuse the collected data. In this second case, four main concerns should be considered:

- The consent of data subject
- Informing data subjects about the conditions of data processing
- The data retention period
- Revocation of consent.

To complement this description, we’d like to underline that these concerns are not specific to traffic data, and that any kind of personal data should be considered under the same concerns. Mobinet is a Platform centred on transport services, but not restricted to transportation services. It will be of the highest importance to promote the same approach to any kind of personal data entering the scope of Mobinet.
3.1.2. Communication phase

For the sake of openness and evolution, an On-Board Unit should open a communication port for any potential application that manages to connect. Reinstalling or even reconfiguring an OBU each time a novel service appears, such as a local safety services or eCall for faster rescue, is definitely not a way to sustain the services growth. Yet customers must determine themselves which service, for which purpose, should receive relevant vehicle data.

We could reinforce this point by saying that the vehicle context could also be part of the decision. Typically, a damaged vehicle can decide to transmit much more information, for safety reasons, than in a nominal situation. But generally speaking, we must consider that this decision, based on a number of informed conditions, is the privilege and duty of the vehicle driver. This is why, in Section 3, we will develop details about the implications of user awareness.

3.1.3. Security

Security is THE foundation of Privacy. Securing the storage infrastructure, as well as securing the communication infrastructure, is mandatory for preserving user privacy.

With respect to this statement, we developed in section 3.2 a number of considerations about security for privacy, particularly in listing the technical needs able to balance operational and business performances with security needs.

3.2. Privacy sensitive ITS application and services

This subsection analyses the iMobility report with regard to applications and services.

3.2.1. Location-based services and traffic data

The iMobility report stresses that traffic data reveal individual communication profiles including information sources and geographical location of the user. To prevent the risk of further use of the collected data, a number of means to safeguard the individuals from undue monitoring applications are suggested, including pseudonymity and anonymity.

It should be noted that similar applications have also been identified as privacy-sensitive in the, as illustrated by a study of the ITS Institute of the University of Minnesota: ITS and Locational Privacy: Suggestions for Peaceful Coexistence (cf. diagram below).
3.2.2. Third party eCall as a private Service

This extends the case exposed in the paragraph above about the Communication phase, where some more data could be transmitted in case of accident. Then the question is whether the help service should transmit these data to local rescue services which are not part of the nominal scenario.

It seems reasonable for the service provider to ask for the consent of such a generic eCall possibility, without specifying the exact eCall Third Party Service (TPS), but describing clearly the nature of services expected from such a selected TPS at runtime. Moreover, the data retention duration must be part of the consent requested to the user as well as the extended data visibility in case of emergency. Then the liability should be endorsed by the main service provider if consent was not implemented by the selected eCall TPS.

3.2.3. In-vehicle telematics services

The same problem arises with any service extending the nominal OBU offer, and not particularly targeted to emergency management. In this case, it is reasonable for each of these service newcomers, even when dynamically selected by the main service provider the user is registered to, to first request an explicit consent based on the transparent description of its processing and data flows.

The liability of the main service provider is not engaged, but the one of the new service selected with this scenario. Of course, for ease of use, the main service provider could decide to stick with the expressed policy for emergency calls. This would augment the risk of liability, since third party services would be less controlled and so less protected by laws. Moreover, the service provider would bring additional
services with lower added value, but for a higher level of risk. Those two arguments taken together would certainly influence the service provider to make explicit in its service description the call to a third party service, in order to delegate not only the processing of the service but also the liability linked to this processing.

For instance, the document below shows how Volvo Trucks presents their future business offering telematics services, as combination of core direct OBU functionalities potentially enriched with external services. Liability issues will remain to be addressed depending on who is the external operator and on the nature of the service.

Most commercial vehicle manufacturers offer telematics based Transport Information Systems for fleet- and vehicle management; Volvo Truck’s solution is called Dynafleet. Dynafleet consists of four solution packages which can be combined in different ways based on needs depending on the type and size of the truck owners operation.

Figure 4 - Volvo and telematics

With Dynafleet it is possible to follow up fuel consumption, emission levels, driven distance and more for each vehicle and driver. Dynafleet can also be used to support transport planning by providing the truck’s exact location, speed, load, vehicle type and more; information needed when planning transports but which also allows goods receivers to monitor the progress of their cargo. Data from the tachograph can automatically be downloaded from the truck to the office, facilitating a comprehensive view supporting planning and makes it easier to follow driver time regulations. The fourth area covers messaging functions in the same way as email and makes it possible to send text messages between the office and trucks.

In order for all this to function, a Telematics Gateway and a combined GPS/GSM-antenna is installed in the vehicle. Depending on which services the customer wants to include a keyboard and an additional display may also be installed in the vehicle. The customer back-office functions access all information through a web-interface, Dynafleet Online, but may also integrate the functionality with its existing administrative system.

3.2.4. Road User Charging

This future kind of service should be rendered while preserving the anonymity of the driver, and possibly the tracks of the trips. When all the consent-based protections needed by other applications will be available, this scenario should be easy to implement.
It should also be possible to render this service through pre-payment, such as via card phones, so that the full processing could be done in the vehicle itself, without communicating any information outside.

### 3.2.5. Pay as you Drive, Pay as You Drive Insurance

This service is a typical privacy-invasive application, since it can be based on tracking the vehicle by collecting data related to location, speed, type of road, time of driving: all this information is potentially sent to an insurance company to profile the user and define the insurance premium. As in the case of road user charging, a privacy-friendly Pay as you Drive (PAYD) scheme, where the premium computation is done in the car black-box, would drastically reduce the privacy concerns. But this would mean some very static computation rules.

In that vein, the Fédération Internationale de l’Automobile (FIA) has issued a recommendation re. PAYD scenarios which can be summarize as follows:

```
| Localisation of the stolen vehicle on-demand |
| Geo-localisation of the parked vehicle       |
| Emergency call: automated in case of accident |
| Stats of vehicle usage for the driver profile: this service consists on the provision, processing and storage of historical data (gathered by the OBU) about the vehicle usage (distance, type of roads, time of the day, etc.) The information anonymised in accordance with the current legislation it will also be used for statistics and other permitted purposes. |
```

There’s another chapter about the personnel data. Here there are two notable statements about the data:

1. All data collected can be used, in anonymous format, for other purposes different from the ones related to this contract.
2. Also, the data can be provided to third parties, anonymously and with different levels of aggregation, for purposes not related to the Telematic Services Contract.

Figure 5 - A summary of the FIA recommendation about PAYD scenarios

Another PAYD implementation could be to introduce a third company to collect and compute, in agreement with dedicated institutions, to run the charging rules provided by the insurance company.

We consider this second proposition as particularly interesting for two reasons: first, it separates the responsibilities, and moreover, the interests. The third company should be focused on privacy issues, deleting all the data once the necessary computation took place. The second reason is that this scenario introduces the notion of institutions, and their role in guaranteeing the business chain and viability. It is more than probable that the evolution of privacy-aware technologies will lead to privacy-aware services, centralizing a number of responsibilities that standard actors cannot handle at an affordable level of risk. Personal data will probably be managed by privacy-focused organisations, just as money is managed by bankers.
3.2.6. Traffic data collection

Among the two main methods to collect traffic data (using Internet connection or Roadside based), the latter usually collects anonymous data. On the contrary, the Internet based collection is highly intrusive and must be run under user consent considerations, as all the others exposed until now. The FIA proposes the following End User License Agreement for using traffic data services based on smartphone information collection. As usual an important remark is that the data is anonymous but it’s also notable that this data can be used for other third party paid services of the service provider.

![Figure 6 - FIA suggested EULA for traffic data based services](image)

An illustration of technical propositions to cope with the injection, or not, of vehicle data within the services ecosystem has been envisaged in the EU project Preciosa ([http://www.preciosa-project.org/](http://www.preciosa-project.org/)). Such a User decision does not manage the data lifecycle once injected, but they provide the user with the possibility to choose the risk level she accepts in order to take benefit of a service. The referred video explains quite well the PeRA (Privacy Enforcing Runtime Architecture) realized during this project: [http://www.youtube.com/watch?v=p6_6H3u1jTo](http://www.youtube.com/watch?v=p6_6H3u1jTo).

3.2.7. Cooperative systems

The iMobility report does not stress any particularity for cooperative systems, as long as anonymity is guaranteed by each of the cooperating services.

We do not follow this line, since the correlation of anonymous data can very quickly lead to a specific person. There is a specific risk raised when mixing privacy-aware services together (cf. work by Dr. L. Sweeney, Chief Technology Officer at the U.S. Federal Trade Commission, who, among other examples, re-identified patients by name by linking de-identified patient-specific medical data to a population register, such as a voter list.

In the mid-1990s, the Massachusetts Group Insurance Commission (GIC) decided to release "anonymized" data on state employees that showed every single hospital visit. William Weld, then Governor of Massachusetts, assured the public that GIC had protected patient privacy by deleting identifiers. In response, then-graduate student Sweeney started hunting for the Governor’s hospital records in the GIC data. She knew that Governor Weld resided in Cambridge, Massachusetts, a city of 54,000 residents and seven ZIP codes. For twenty dollars, she purchased the complete voter rolls from the city of Cambridge, a database containing, among other things, the name, address, ZIP code, birth date, and sex of every voter. By combining this data with the GIC records, Sweeney found Governor Weld with ease. Only six people in Cambridge shared his birth date, only three of them men, and of them, only he lived in his ZIP code. In a theatrical flourish, Dr. Sweeney sent the Governor’s health records (which included diagnoses and prescriptions) to his office.
Nevertheless, we agree with the iMobility report that, being at the very early stages of such cooperative systems, we will need to understand better the risk in order to cope with it at the platform level, such as with Mobinet.

### 3.3. List of privacy-friendly approaches to actively promote

The approaches recommended in the iMobility report for safeguarding users from the list of threats identified above include:

- Privacy by Design
- Promoting a consensus process that involves the industry
- Involving consumers – The importance of informed consent
- Consumer education and awareness.

One could observed that these iMobility recommendations are in fact domain-agnostic and not specific to ITS. They will be further discussed in their full genericity in the User Awareness section.

### 3.4. Mobinet privacy approach

The Mobinet project started with the general requirement of fulfilling the EU regulation obligations for service providers within the global concept of Mobinet Privacy Framework. Some precisions need to be provided here, in order to clearly differentiate the operational target in Mobinet and the research challenges Mobinet will support with the Privacy Framework. As an introduction to Mobinet Privacy Framework, consider the three following project points of view at the time of Mobinet platform release 1 delivery:

> The Mobinet Privacy Framework is a preliminary research component. The initial concepts of the Framework have been implemented and delivered, even if not fully integrated with the release 1 platform. The conceptual integration is done, since the delivered tool can already be applied to the code base of release 1. One can already, by linking the delivered editor with release1.jar packages, point out all the touchy records (and fields) of release 1 code. The lacking part is the enforcement of privacy on the Mobinet platform. This lack is partly a question of integration, but mainly a question of dev maturity yet. The enforcement is the last deliverable of Privacy Framework, due month 29. So in the ideal case, MP-58 could not be considered fulfilled prior to this date. Mobinet Privacy Framework targets the research challenge of postponing the Privacy Design when the application is functionally defined.

**Figure 7** The Mobinet technical point of view re. Privacy

> For the beauty of the approach, it is a kind of magic to come very late in the platform lifecycle and comply with the 'privacy by design' principles. This is a bit risky but we can potentially all agree that if the Privacy concerns had corrupted the initial phases of maturation of the platform, nothing could have been realized, neither decided.

**Figure 8** Agile Privacy in support of innovative services
This intense research oriented approach is easy to argue given the number and complexity of issues exposed in this document. Nevertheless, we do believe that Mobinet is the ideal ecosystem where the future Privacy oriented development techniques will mature. Providing the proof of concept of a new principle for privacy enforcement (namely Agile Privacy, cf. supra) is a huge challenge per se.

3.5. The Preserve project – preparing secure v2x communication systems

The goal of Preserve (http://www.preserve-project.eu/) is to “bring secure and privacy-protected V2X communication closer to reality by providing and field testing a security and privacy subsystem for V2X systems”. Based on results of previous projects such as Preciosa, Preserve will investigate a number of feasibility and scalability issues. From this perspective, Preserve and Mobinet have the potential to mutually contribute: Mobinet by providing a new field experiment in a privacy-aware prototype platform, and Preserve in establishing the analysis about the ability to scale such solutions up. For instance, one could implement data exchange between MobiAgent and MobiCentre with the help of the Mobinet Privacy Framework, and assess the resulting communication properties based on Preserve outcome. Of course, the goal of the Mobinet Privacy Framework is not strictly to secure the communication between MobiAgent and MobiCenter (vehicle / Back office service), but to master privacy all along the chain of services triggered by data sensors in a consistent way. From this point of view also, complementarities should be optimal.
4. User awareness

One important evolution observed during the elaboration of the draft EU regulation consists in placing the user at the core of any data exchange system.

To some extent the recommendations of the iMobility report mentioned earlier for safeguarding users from privacy threats echoes this evolution. As a reminder, these recommendations include:

- Privacy by Design
- Promoting a consensus process that involves the industry
- Involving consumers – The importance of informed consent
- Consumer education and awareness

Similarly, the Annual General Assembly of the Fédération Internationale de l’Automobile (FIA) has resolved in December 2013, that:

- consumers have the right to own and control the data generated from their vehicle and to transfer it to a service provider of their choice;
- consumers have the right to understand the nature of all data generated from their vehicle;
- consumers have the right to choose the applications and functions provided to their vehicle through telematics or other platforms, as well as their suppliers.

However, the shift towards reinforcing user awareness and control is becoming significantly stronger among privacy experts and the general public in the light of the Snowden case and similar cases. The FIA resolution, for obvious business reasons, only addresses the consumer role when entering the system and selecting services, while user awareness should encompass the whole lifecycle of data exchange, eventually up to the right to be forgotten.

The era when the service provider can be trusted to comply with some initial, global and fuzzy consent the user must approve to benefit from the service is reaching its limit. In this respect, the following experiment, led by Maurizio Borghi and his team, is informative about the limits of such an approach ([http://ijlit.oxfordjournals.org/content/early/2013/03/09/ijlit.eat001.short?rss=1](http://ijlit.oxfordjournals.org/content/early/2013/03/09/ijlit.eat001.short?rss=1)). From a legal perspective, the current trend is to make the consent much more informed and explicit about the nature of the captured data, and the purposes of this capture. Through this explicit description of purpose, the user should be able to evaluate the associated risk and could decide to consent or not first with the capture, but also with each of the exposed purposes. The service provider must then be accountable for respecting the exact consent provided by the user, and ultimately should be liable for processing data for purposes the user would not have consented to.

This generic protection scheme, based on user consent and explicit service descriptions, is to be coupled with the ability to enforce, technically and legally, the explicit consent of any particular user. Whenever technologically enforced, this legal framework would give the opportunity for the user to consider her digital privacy through the traditional conceptual tools of the physical life associated privacy. These main concepts are the notions of **risk**, **trust** and **social networks**. The objective risk has first to be considered when using a service. (Typically, what if I provide my credit card number to a service
provider?). Then, the evaluation of the probability of damage associated with this risk when dealing with particular instances of a service (what if I provide my credit card number to THIS service provider?) matters as well. And finally, the evaluation of the effect any possible disclosure in my personal social network needs to occur. Is my reputation in danger or only my money? All these questions become a dilemma, subject to personal evaluation for the user in order to choose in all conscience when to provide consent and when not, depending on the risk management approach each individual is willing to pursue.

4.1. Risks

Risks related to privacy management are implicit and numerous. Starting from personal risks, and the associated list of potential damages associated with a deficient risk management, we will review the counterpart risks for businesses whenever running their users privacy rights in an inappropriate way. Finally this sub-section will examine the dominant proposal to reconcile in a fair and balanced way those multiple and conflicting risks, namely Privacy by Design.

4.1.1. Personal risks

To begin with this personal risk aspect, let’s consider one particular right associated with privacy management, the right to be forgotten: any human organisation needs resilience and this was already managed with respect to press and justice decisions, prior to our digital era. For example, in France and other countries, the right to be forgotten has been considered with respect to press and information right. Typically, justice decisions are legally published in the press with the name of the persons implied in the case, for the sake of the information right. After a given delay, such a publication can be considered as defamation, if no present reason can be invoked for such a reminder. This limitation is very subtle, and under the decision of the judge, since the understanding of the motivation is important. Now considering that press archives can be consulted online, the problem of the right to be forgotten is not attached to the intent of re-publishing the same justice decision, but simply about archives management. In theory, all the online archives should be anonymous after a certain period. This gives an example of the complexity of evaluating this period, depending on the context, as a judge would consider. This particular aspect of the right to be forgotten highlights that, as with any other right, it must be associated with the notion of responsibility. In the civil society, a citizen cannot erase their acts, but the traces of these acts when no more justice consequence can be expected. When it comes to the digital world we live in, it is difficult to separate acts and traces. Also, no notion of justice is clear, due to the extraterritoriality of all the social networks. The pure transcription of the right to be forgotten from the press to online services is then impossible.

On the other hand, the concepts of consequences, reputation and traces are at the core of those new exchange media. As the absolute right to be forgotten in the press case would correspond to a form of censorship (imagine if citizens could never know the justice decisions concerning politicians), it is probably not desirable to establish such a possibility for online service users. One may envisage that the right to be forgotten should be proportional to the benefit gained from the usage of the service. It is not fair for the service provider to be obliged to erase all traces of a very intensive work which has benefited the user. This balance, amongst others, should be part of the consent, defining a limitation period, proportional to the usage rate of the service.
The right to be forgotten is a very symbolic part of the personal risks, since it could be seen as the ultimate answer to the risk: I do whatever I want, without risk evaluation since I can erase all my past actions on a click. From the citizen point of view, this behaviour is also very far from the usual privacy management, where all the actions have to be taken in a proactive manner. It is important for any responsible person to clearly manage traces and risks, relying on this ultimate right to be forgotten for extreme cases. The risk evaluation, and the answer to this risk, must be based on some experimental learning of the side effects of private information disclosure. The goal is to behave in control, disclosing personal information for good purposes, since the absolute secrecy corresponds to a social death of individuals.

To this extent, information and training programs could help citizens identify risks with respect to personal information management. But nothing will prevent them to manage this risk on their own, based on their own acceptance and trust levels. Once this risk is understood, they must be in a position to build their own strategies and tune by experience their privacy depending on the social interaction context. These strategies are envisaged in the section below, on Trust and Acceptance.

4.1.2. Business risks

One of the major business risk to come is the liability risk. User could consider that disclosing private information is so harmful that new trial cases could come every day to the service provider legal offices. In the US, some class actions will also be conducted and the service provider will be accountable for any of the uses done, even by third parties, from the collected personal data. It is of the highest importance for companies to be able to assess and track all the privacy-centric operations in order to be effectively prepared against such attacks. A new kind of role appears in most headquarters, named Data Protection Officer, or Privacy Officer, responsible for applying all the recommended procedures in order to lower the risk of being sued, and if then, to lower the risk to lose the trial, and if losing, to lower the fine and other consequences.

The second type of risk concerns business reputation, followed by customer retention and margin markers. It will be a very high differentiation to prove an ethical position with actual accountability figures, compared to marketing acknowledgement or negative press articles. Privacy management capabilities will provide online services with the possibility to target the high end segment of their markets. On the other hand, a low capacity to treat privacy respectfully will condemn service providers to low end segments, and will force them to find business models with very low margins, based on very fast expansion. If the service area is quite protected, such an option could be the right one, but whenever competition is hard, the sustainability of business becomes very closely tight to privacy management capabilities of the proposed solution.

Moreover, when it comes to the role of an interconnection service platform such as Mobinet, then the difficulty is to put this platform in a safe situation with respect to the risk of breaking privacy. In other words, Mobinet should give tools for the Privacy Officer of any Mobinet instance, to lower all the enumerated risks. The ideal situation would be the one where Mobinet is considered as a switch board, interconnecting services with pipes in which no divulgence is possible. Such a divulgence could only happen when data is used by services, under consented contexts at service level, and so independently from Mobinet. Mobinet should stick with its role as data controller, but never play the role of data processor, in the spirit of Internet neutrality. Is this possible today? The answer is clearly no. There is still a lot of research to be conducted in this direction, but we should take the Mobinet development opportunity to propose some potential architectures leading to the expressed target.
4.1.3. Societal risk

Digital data protection has traditionally been tackled under the ‘security’ point of view. User authentication, user identification and access control mechanisms have supported digital service providers to protect data from intrusion. But privacy is much more than data protection; it consists in adapting the level of data transparency to the usage context, exactly as a person reveals more of her intimacy in a private area to trusted people than in a public area. The ability to modulate the depth of exchanges in function of contexts is one of the necessary conditions for a service ecosystem to thrive. Moreover, considering the digital era we are already in, such ability must be extended to any digital footprint of any individual. Each citizen must be in a position to decide which level of transparency she offers about herself when interacting with a digital service, live or batch. Privacy is to be considered from a citizenship point of view, as a matter of human rights and democracy.

On the other hand, the respect of privacy, needed for democracy and associated economic prosperity, conflicts with the other mandate of the states, which consists in maintaining global security through surveillance methods. In ‘Surveillance and Criminal Investigation: Blurring of Thresholds and Boundaries in the Criminal Justice System?’ (Vervaele, 2014), John Vervaele focuses on the current redefinition of competencies amongst traditional criminal justice systems, induced by the heavy use of digital-led investigations. He shows that ‘the expansion of the judicial investigation into a pro-active investigation and the increasing overlap between the law enforcement community and the intelligence community has been further increased by the technical developments in investigative devices: the sword of technology with far-reaching eyes and razor-sharp edges.’

Surveillance is increasingly used as an investigative technique, both as a tool of judicial investigation to gather evidence as a tool in a pre-active setting, before the preparation of an offence, to gather information about risks, threats and dangerousness of personal behaviour and thinking. The net widening and function creep of investigative surveillance imply conceptual changes which are strongly related to the information society and to transformations in the criminal justice system under the security paradigm. Classic thresholds and procedural guarantees in the criminal justice system have become obsolete. The human rights dimension of these surveillance measures are mostly dealt with under the protection of privacy. However, given the potential intrusive impact of surveillance and the coercive character of some surveillance techniques, also in the pre-emptive setting, it is logical to build in guarantees against disproportionate infringements of privacy, human dignity and the presumption of innocence. The latter could then be related not to the commission of offences, but also to the definition of dangerousness.

One particular handicap of democratic countries is that they also have the mandate to protect their citizens’ privacy. The current balance is, as Snowden told us, frankly oriented towards surveillance, and will remain so as long as technology does not allow better tuning. Some very interesting developments of this opposition is debated in the IRISS report (IRISS EU Project - Deliverable D2.2, 2012) entitled ‘Increasing resilience in surveillance societies’, with the overall following point of view:
Moving on to consider the surveillance in relation to rights, freedoms and the rule of law, we point out that the rule of law has formal and substantive dimensions, respectively connoting rule by law, legislative processes, and consent, on the one hand, and individual rights, justice and the right to dignity, and substantive equality of welfare, on the other. Privacy and data protection are directly implicated in all of this, with privacy as a tool of opacity and data protection as a tool of transparency. The European Court of Human Rights has struggled to reconcile surveillance with democracy by means of interpretations of the rule of law in specific cases. This discussion of law, rights and freedoms leads to an analysis of the broader governance of surveillance through a range of instruments of which the legal order and the rule of law are not the only ones currently experienced or capable of further development.

Actually those concerns apply not only to state agencies in charge of surveillance, but also to business at large given that similar intelligence techniques are used by service providers and especially big internet players to survey customers and users. It is a matter of collective business responsibility for the digital economy actors and possibly of regulation, as with fishing quotas or food production and logistics traceability. But until this happens, Mobinet can be a reference player to identify what a responsible business behaviour could be with respect to personal data protection. What should Mobinet provide in terms of privacy management to become and remain the reference platform for Intelligent Transport Systems? As explained in the User Awareness section, there are not so many directions to follow at this point. As of today, the most accepted approach is known as Privacy by Design (Information and Privacy Commission, Ontario).

4.1.4. Privacy by Design, the current guidelines to manage the identified risks

Privacy by Design is an approach to systems engineering which takes privacy into account throughout the whole engineering process. The concept is an example of value sensitive design, i.e., to take human values into account in a well-defined matter throughout the whole process and may have been originally derived from this. The concept originates in a joint report on “Privacy-enhancing technologies” by a joint team of the Information and Privacy Commissioner of Ontario, Canada, the Dutch Data Protection Authority and the Netherlands Organisation for Applied Scientific Research in 1995. The Information & Privacy Commissioner of Ontario, Canada, Dr. Ann Cavoukian, has marketed the concept of Privacy by Design since the late 1990s (From Wikipedia).

In order to promote Privacy by Design, the Information & Privacy Commission of Ontario advocates all this approach on a global scale (cf. the Privacy by Design Resolution at the 32nd International Conference of Data Protection and Privacy Commissioners, http://www.ipc.on.ca/site_documents/pbd-resolution.pdf). The 7 foundational principles are defined (see below, from Wikipedia),
The objectives of Privacy by Design — ensuring privacy protection and gaining personal control over one’s own information and, for organizations, gaining a sustainable competitive advantage — may be accomplished by practicing the 7 Foundational Principles:

1. **Proactive not reactive; preventative not remedial:** The Privacy by Design approach is characterized by proactive rather than reactive measures. It anticipates and prevents privacy invasive events before they happen. Privacy by Design 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, Privacy by Design comes before-the-fact, not after.

2. **Privacy as the default setting:** We can all be certain of one thing — the default rules! Privacy by Design 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.

3. **Privacy embedded into design:** Privacy by Design 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.

4. **Full functionality — positive-sum, not zero-sum:** Privacy by Design 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. Privacy by Design avoids the pretense of false dichotomies, such as privacy vs. security — demonstrating that it is possible to have both.

5. **End-to-end security — full lifecycle protection:** Privacy by Design, having been embedded into the system prior to the first element of information being collected, extends securely throughout the entire lifecycle of the data involved — strong security measures are essential to privacy, from start to finish. This ensures that all data are securely retained, and then securely destroyed at the end of the process, in a timely fashion. Thus, Privacy by Design ensures cradle to grave, secure lifecycle management of information, end-to-end.

6. **Visibility and transparency — keep it open:** Privacy by Design 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.

7. **Respect for user privacy — keep it user-centric.**

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

A number of projects have been implemented based on those principles, addressing diverse applications areas such as surveillance in mass transit systems, smart meters or mobile devices and communications.

To highlight in a more concrete case the application of such principles, let’s consider the related US-Canada border case, supervised by the Information and Privacy commission of Ontario (http://www.ipc.on.ca/images/Resources/edl.pdf ). The initial project plans to equip Canadian citizens with a device, able to send their identity to the custom officer some seconds before their effective crossing. This should speed the crossing up and reduce the recurrent jams in a significant manner. Privacy by Design does participate to the initial design. This initial design considers a RFID device and the corresponding sensor. From the privacy point of view, the Ontario Commission recommends to make this device dumb when not in the proximity of the boarder. So the design integrates the Privacy by default concern and evolves the following way. The RFID device will be inactive by default, and a press
button will be added in order to make the device active. By pressing this button in front of the dedicated sensor, the user will decline her identity as envisaged by the plan. The big improvement is that this device will never disclose the citizen identity without an explicit action of the owner of the device.

In particular, this use case is definitely user-centric (Principle 7), transparent (Principle 6) since verified by the Ontario Privacy Commission, and positive (Principle 4) as nobody’s interest is hurt with the proposed adaptation. Also, privacy was embedded into design (Principle 3) by considering privacy protection as the top priority for the product from the beginning (Principle 1).

This specific and ideal case highlights very well the benefits of Privacy by Design. Nevertheless, the Ontario commission itself recognizes (communication at the CPDP 2014 conference), that all the studies are not as ideal. In particular, a mono-functional device for a single context does not represent the nominal complexity of modern projects. When it comes to software systems that deliver hundreds of interoperating services in the cloud, respecting the Privacy by Design principles becomes much more challenging.

One of the main difficulties comes from the software engineering field itself, where lifecycles are not so rigid and deterministic than with simple hardware. Co-design techniques between contributors are still very badly mastered by software project teams, and product maturation is often the result of a kind of Darwinian process. Situations where the design is nothing but a starting point that does not describe the actual target of the development make it difficult to guarantee the applications of Privacy by Design principles from end to end.

4.2. Trust and Acceptance

It is absolutely necessary, when dealing with privacy, to consider trust concerns. Generally speaking, privacy needs to be managed taking into consideration the accepted risk associated with the corresponding service. This risk can be evaluated based on the user experience, or other users experience, if they agree to share this experience. But risk is not trust. Risk evaluation results from the aggregation of the trust granted to a service provider, together with the estimation of the damage incurred, should the service fail to comply with its promise. It could be acceptable to trust any service provider in a low risk area, while only some very reliable providers should be trusted in risky areas. A long term approach to trust may be for a user to establish trust within low-risk areas, and to integrate gradually trusted providers into more risky areas.

To take a metaphor in the medial domain, and assuming medical consultations are available online, would you undress as easily as you do at your doctor’s? You would probably start with consultations where undressing is not required, in order to check your confidence level with the service, trying to get some assurance that the medical secrecy is respected. And gradually, as your confidence grows, you might disclose more and more information about yourself, finally feeling more secure naked in front of your webcam.
This personal trust-building process could be reinforced with collective reputation systems in some cases, but would they need to reveal some private information to qualify their recommendations?

We could see the Risk function as a function over the services area space, while the Trust function would be a function over the service providers and time.

### 4.3. Social Aspects

We can see Personal data protection issues in the digital society as an extension of individual privacy in traditional social life. Privacy is a social matter by definition, and Personal data protection could be seen as a Social network matter by extension. We list hereafter a number of privacy concerns linked with the current era of intensive Social Networking, and then anticipate the convergence of Social Networks with ITS systems.

#### 4.3.1. The social impact of Social Networks

We propose to consider the conclusion of Paulan Korenhof, when analyzing a real case known as ‘the drunken pirate’. This article (Korenhof, 2013) describes how ‘Information on the Internet can sometimes damage people by interfering with offline life. A high-school teacher-in-training experienced this first-hand when a photo with the caption “drunken pirate” and a message on her MySpace website led to the end of her career as a teacher. This case received a lot of media attention and is used in academic debate as illustrating the need for a “right to be forgotten”. The question is how and to what extent the Internet contributed to the fact that the teacher-in-training’s information ended up with the wrong audience. The problems in this case did not arise due to any memory related capacities of the Internet or the Internet being a place where information can be easily copied and reproduced. The problems arose because audience segregation on the Internet is a difficult task.’

The full reading of the case analysis is highly informative, and led to a very interesting conclusion containing in essence the full challenge of using Internet to promote and share individual representations. The following excerpt of the conclusion sums all what needs to be said in this section:
This conclusion fits well with the Mobinet proposed vision, where purposes and roles should be considered when sharing information. Ultimately, some temporal considerations should also be added in the context analysis prior to deciding if the information access control is granted or not, depending on the user consent.

### 4.3.2. Current Privacy Issues

When a person uploads photos on a social networking site, or when this person tweets or uses any other means of networking interaction, others can follow them. If other users can do so, some dedicated applications can use software agents, bots disguised in 'users', to grab all this personal information for any kind of future use. For an individual, the danger of being victim of cyberstalking is growing as fast as their presence on the network. Criminal endeavours represent the biggest threat for individuals naive enough to reveal transparently themselves in the digital space. But some other threats exist, with serious legal and social implications:

- Social profiling, used internally by social networks to connect people together, is a kind of discrimination. As such, when deployed at a large scale like in Facebook or LinkedIn, it adds potential rigidity and distortions in the necessary social fluidity, and could be dangerous for democratic fundamentals.
- Third party disclosure, the real target of social profiling, is done without even informing the profiled user.
- Most current consents force the user to give the ownership of the exchanged content over the network to the infrastructure owner.
- As the most vulnerable users of social networks, one may expect that teenagers, increasingly concerned by their privacy, will more likely adopt privacy-protecting behaviours in the future. This indicates that many of them experienced undesirable situations in the past, or understood from others experience the risk of bad reputation or exclusion based on digital traces.

- Law enforcement is more and more active on the networks. High visibility on the network increases chances to be suspected, especially when the network is considered as a free space where everything can be claimed.

4.3.3. Big Data trend and related public clouds initiatives

Social networks show that correlating data is accepted by users, for the sake of the (often limited) offered service. As ever, when a minimal drawback is accepted, this eventually means that the deep motivation behind is also accepted. We can then predict, based on current social network practices, that we will enter an era of massively aggregative and profiling processes. Of course, all the threats carried out by social networks will be amplified, exponentially, with this new step. The good news is that such threats have already been uncovered in relatively harmless environments (à la Facebook), so that they can be already projected on the scenarios promised by the Big Data approach.

Nowadays customers don’t exactly know what is done with their data. End-users normally accept to give their data in exchange of services, apps, etc. But more and more customers are having more awareness about the value that personal data have for companies or the consequences that can be caused by the use of personal data.

To put an example, a bank can make an analysis of the risk to grant a credit to a customer depending on her activity on social networks. If you are friend of defaulters then your credit will not be approved. And that’s something that users have not taken into account.

For these reasons in the near future the customer will decide to whom she gives access to personal data and, more importantly, for what purpose. This will allow her to maximize the benefits obtained in the exchange or to not allow the use of her data for certain purposes.

Initiatives around public clouds where rules are clearly agreed about data protection and visibility, depending on the purpose of the processing, are emerging. These initiatives are very interesting but are still at their very beginning. In that spirit, one can mention cooperatives created by users, like TheGoodData or Healthbank, with the 3 main principles:

- End-user is the owner of the data
- Let’s collaborate to talk to companies on an equal footing and to act as real owners of the data
- Decide what to share, with whom and for what purpose.

4.4. Data ownership perspectives

As mentioned above, mobility traces provide some of the most concrete and revealing information to profile individuals. Some applications, based on Wi-Fi sensors, are already tracking supermarket customers in their peregrinations throughout alleys, for any kind of post-treatments one can think of. This is a first entry point but very soon, vehicle traces will be used in the same spirit, with potential closed
loops in the navigation system, depending on the driver’s profile. These consumption-oriented scenarios primarily depend on the capacity to collect data, and consequently raise the issue of data ownership.

In that vein, let us consider what the FIA (Fédération Internationale Automobile) proposes with respect to data ownership, when the data is collected from the vehicle. In Dec. 2013, at a meeting of the World Council for the Automobile, Mobility and Tourism (WCAMT), FIA Mobility clubs unanimously backed a resolution underlining the rights of consumers to own and control the data generated from their vehicle and to transfer that information to a service provider of their choice. The document inserted hereafter further documents the FIA’s position on Data access and data ownership especially in the context of repair and maintenance operations.

---

**Access to repair and maintenance information (RMI)** is essential for aftersales market services. In addition, new technologies such as the rising number of in-vehicle telematic systems will allow the deployment of new add-on telematic services, but also can threaten existing ones, if access to data is restricted for independent operators by implementing new telematic systems in the vehicle.

Motorists across the world should have the right to choose who services, repairs or maintains their vehicle, and who has access to data produced by their vehicle, who owns the data, and importantly, who controls it. The issue comes down to the question of who owns the equipment and the data produced from the vehicle.

**Issues to be addressed**

New technological advances, such as complex on-board vehicle technology, telematic and cloud data storage, combined with business model drivers from the vehicle manufacturers designed around forcing a one-to-one relationship between them and the vehicle owner, have combined to threaten the freedom of consumer choice, impose restrictive trade practices, and disrupt the activities of organisations devoted to providing assistance to motorists.

Limiting access to data generated by a vehicle to only one service provider may inhibit innovation of additional services to motorists/consumers and the development of safety services by other providers. However, since the vehicle manufacturers will install the telematic systems ex works, they also control the access.

Companies that provide innovative services or products which require access to certain vehicle data should not be prevented from competing against vehicle manufacturers who do not allow anyone, including the consumer, access to certain types of vehicle data.

With the new in-vehicle telematic systems comes the potential for infringement of the right to self-determination in information and communication, since e.g. the unfiltered transmission of a vehicle’s location might involve personal data. Vehicle manufacturers should not be in a position to use a claim of proprietary rights of data systems as a reason for not allowing access to consumers and third parties.

Reasonable steps must be taken to ensure that the individual is aware of the data being collected.

Security standards for vehicle data established by law or industry practice could complicate access to vehicle data.

**Capture:** Telematics opens up whole new areas of vehicle communication, but it also poses challenges and threats to data protection, consumer choice and fair competition.
**Data protection**

Consumers should in principle own all data generated by their cars, get clear information about the data gathered and its potential use, and be free to share it with service providers of their choice.

The use of private telematics add-on services and the required data transmission should be selected by the vehicle owner on a voluntary basis.

Progress in wireless communications and embedded telematic system technologies has created a shift in vehicle diagnosis and maintenance. These developments threaten consumer handling of their data since remote communication with the vehicle is possible without the customer knowing what data is transferred.

The unfiltered transmission of a vehicle’s location might involve personal data. Before the information is collected, reasonable steps must be taken to ensure the individual is aware of the data being collected.

Justification: the German ADAC commissioned a legal opinion on the question of who owns the vehicle data. Most of the scenarios described below are based on that study and are linked to German (data protection) law. In addition, the working group tried to identify common legislative data protection in Europe and Australia.

In principle, nobody owns the data: Owning the control units or data carriers does not imply that manufacturers have unlimited access to the data. On the other hand, customers, on the basis of their data protection rights are entitled to determine who should receive relevant data and even stop third parties interfering with their vehicles. For data protection rights to be applicable, data must correlate both to a specific vehicle and to its driver or owner, or whoever else habitually uses the vehicle. Typically, vehicle data is personal. In this case, a restricted interference would include all use which is not in line with the owners’ intentions, i.e. retrieving data from on-board data carriers, let alone monitoring vehicle usage. Further, consumers should be able to give access to their data to independent operators.

Anonymised data is never personal. To access anonymised vehicle data, some interest groups, e.g. workshop and breakdown service providers may have certain rights under competition or anti-trust laws. In chapter IV of this paper, the working group took a closer look at this aspect.

- Europe: The problem with the new in-vehicle telematic systems which the data protection community faces is their (possible) infringement of the right to self-determination in matters of information and communication. At EU-level e.g., this could be in non-compliance with EU Directive 2002/58/EC.

- Australia: The Privacy Principles in Australia also foresee that, if the collection of personal information by an agency or organisation is within the law and is necessary to undertake its functions, the privacy principles do not prevent that collection and use, but set out guiding principles on how personal information is collected and used. This means that, at, or before the information is collected, reasonable steps must be taken to ensure the individual is aware of the data being collected.

An exemption is the public eCall. As long as vehicle location positioning (including Cell-of-Origin positioning within the mobile telephone network) is applied for individual emergency situations only, with the data transmission unit remaining dormant until triggered by a crash, data privacy is unlikely to be at risk.

---

**Findings and recommendations**

Consumer’s choice is strongly connected to fair and free competition in the future field of telematic add-on services. Linked to this, are the aspects of data protection, being informed about data transfer as a consumer, and the right to handle vehicle data. Standardized and secure access for independent operators to the vehicle via telematic systems will help prevent misuse and ensure that the remote services offered to the consumer are useful, secure and beneficial.

**Proposal of FIA**

Motorists deserve the right to own and control the data produced by their vehicle. They also have the right to determine which third party operators or service providers can access data generated by their vehicle, and determine what ancillary services they want from any third party provider.
This document indicates that the fight for data ownership has somehow already started, and it can only get tougher in the coming years. Nevertheless, we can anticipate that focusing on the notion of capture device, in its specificity to a motorist, is not sustainable at mid-term, since the vehicle itself will soon be considered as a sensor for the platform which manages the full driver’s life. Then the question will be: does the data subject continuously own the data, whatever channel of capture and whatever infrastructure is being used to process them? This is the central question policy makers and data protection stakeholders should priorily consider and resolve. If the data subjects lose data ownership during the data processing lifecycle, then they will have the responsibility to anticipate threats and unwanted privacy breaches. This may induce protective behaviours from consumers who would be more reluctant to share personal data and to participate in social activities. In such a scenario, the social dynamics would be greatly endangered and the digital economy growth would be hampered.

4.5. User awareness vs. community awareness

Another interesting point, besides data ownership, is access control to the knowledge derived from data processing, particularly in a big data context.

From a legal point of view, is the knowledge derived from collections of anonymous data to be considered as added value or as a simple case of data reuse? For instance, when profiles are generated based on data clustering, should the profile owner be the data processor who computed the clusters or should the profile owner be the set of profiled users (and original data owners), grouped in a given cluster? When the computed profile clearly identifies a real community, it makes sense to consider this identified community as the owner of the generated profile, and as such, this community should be able to consent or not to further use of the corresponding profile, depending on the invoked purpose. If the generated profile cannot be mapped in any way to a particular community, then the decision could be to let the profile generator own the profile.

This issue can be illustrated with one of the D4D experiments (http://www.unglobalpulse.org/D4D-NetMob), which studied cell phone data in order to redraw bus routes in Ivory Coast (http://www.technologyreview.com/news/514211/african-bus-routes-redrawn-using-cell-phone-data). It is true that the individual’s privacy had fully been respected during the experiment, but what about the derived knowledge? The first question is about user clustering between those who phone while using public transportation, and others. Is it fair to redraw bus routes for the benefit of the first category? The second question is more pernicious. Can it be a source of collective danger for phone owners to be identified on particular bus routes? This may depend, in particular on the political context and on public safety conditions. It should be the privilege of phone owners in Abidjan to answer this question collectively.

In this sense, the collective consent is not the sum of individual consents (User awareness), but the result of a collective and conscious debate (Community awareness). When talking of consciousness, we mean the collective understanding of the identified profile behind the grouping of individuals in specific clusters.

---

2 “For the first time, a big mobile telephony database has been anonymized and opened up to the international scientific community with research teams at some of the world’s best academic institutions competing against each other to use it for social good. Global Pulse has partnered with Orange to help deliver the challenge and is represented on the Data for Development Selection Committee.”
5. Responsibilities and Actors

This section considers the dominant pragmatic approaches promoted to ensure privacy, mostly based on access control. Behind these approaches, one recognises habits, rules or balances adopted by actors usually concerned by public and private life matters. In particular, police and legal authorities need to be part of the picture. Private business players also have some responsibilities, and we need to balance their duties with a fair consideration of their interest, particularly by considering the potential business handicap introduced by heavy obligations. We then propose experimental directions for Mobinet.

5.1. Public security vs. Democracy

The need for public authorities to surveil and secure the digital space becomes more and more accepted. At the same time, western citizens expect more transparency with respect to security and surveillance. The balance between the free circulation on the one hand, considered as a pillar of democracy, but also of economic development, and the national security on the other hand, is difficult to establish. The Snowden case illustrates very well the current tension, particularly in the US public opinion. The surveillance of foreign countries is accepted as one means among others to secure the future of a nation, but the same technique applied to the citizens forced President Obama to promise the methods of US security agencies would change.

5.2. Technical Security vs. Operational Excellence

Privacy depends a lot on security. Typically, we all need to operate in a secure environment to manage our privacy: if anyone can steal my personal information, how can I expect to control the conditions of its dissemination? A secure environment must guarantee that I am the one who decides how the personal information I introduce in the public space is to be represented and disseminated. For this and for many other reasons all along the information propagation chain, security is needed.

Security is very often addressed through access control. This is why, when apposed on private information, access control is wrongly seen equivalent to privacy enforcement. In fact, access control constitutes a mandatory layer of privacy enforcement, but does not cover the full spectrum of what privacy enforcement is about, as described throughout this document. In this section, we will focus on the Access Control dimension, considering classical security architectures at a very high level, with their advantages and current evolutions. Access control may be exercised on the data container, on the content or on both. Access controls applied on the container in a software platform are often grouped under the generic name of Access Control Lists, while, when directly applied on the content, they fall under the cryptographic domain. As access control is typically thought as an exchange agreement between providers and consumers, there may exist a need to certify the authenticity of each of those agreements. This is done through certificate mechanisms.

5.2.1. Access Control Lists

Access control lists (ACL) are rules or policies possibly associated with any managed resource of a system. The rule contains access grants to the content of the resource, depending on the subject s and the purpose of the access. In most classical resource management systems, such as all the modern
operating systems or databases, the purposes are Read, Write and Delete. The subject of the access must be characterized in terms of credentials, and those credentials will be compared to the granted ones at the time of the resource access. This generic mechanism is a centralized service provided to application developers and users. Their own responsibilities will then be to define the rules for their own resources, explicitly (resource by resource) or implicitly (through conventions or hierarchies). This centralized service requires all the device drivers to implement the Access Control APIs expected by the central control system. This way, ACL are managed the same way from the user or developer perspective, be the container located on a disk, on a USB key or on an IPC. This architectural commonality is known as GFAC (Generalized Framework for Access Control) (Abrams, October 1990). The application of GFAC approaches have been considered for privacy concerns since 1998 (S Fischer-Hubner, 1998). In their paper From a Formal Privacy Model to its Implementation, the authors present a task-based privacy-model which can be used to technically enforce legal privacy requirements. The authors show how the privacy policy has been specified and implemented according to the GFAC-approach.

5.2.2. Encryption

Encryption is another way to protect access to data. It consists in obfuscating the meaning of data, and controlling the access to its semantics by applying decryption keys. This can be done in a symmetric or asymmetric way. Cryptographic algorithms are said to be symmetric when the same key is used for encryption and decryption. If symmetrically encrypted data is exchanged between two parties, then the receiving party needs to know the encryption key to access the data semantics. Asymmetric algorithms use different keys for encryption and decryption. Most of the time, a pair of keys is generated by the receiver, one public and the other private. The public key is transmitted to the data originator, so that she can encrypt the data prior to sending it. This encrypted data can only be decrypted with the private key. The asymmetric mechanism is much more secure, since the decryption capability does not leave the receiving side.

Such encryption mechanisms contribute to software systems, in order to secure communications. They also contribute to data storage, so as to prevent data breaches. To this end, a number of supporting technologies are proposed, mainly based on encryption of the database itself. The problem with this is that it also puts surveillance in an absolute fog, and the expected balance between public security imperatives and free flow of information is not reached at all.

A more global approach to surveillance, allowing anticipation of major threats through numeric analysis of massive databases, but tightly integrated within legal procedures, has been elaborated in the following article (Introducing Privacy-Protective Surveillance: Achieving Privacy and Effective Counter-Terrorism, http://www.ipc.on.ca/images/Resources/pps.pdf).
The long-term bet behind this optimal scenario is to achieve an acceptable, not yet achievable, operational performance at all levels of the software chain: the ability for the database to efficiently store encrypted data, the ability to index, join and filter them while in their encrypted format. This calls for a number of technological improvements to become a realistic scheme, but clearly provides a reachable common objective to all concerned specialists. The key element resides in the properties of cryptographic algorithms, in particular their capacity to compute and compare data without having to decrypt them, which is now achievable in some cases, thanks to the so-called homomorphic encryption algorithms. We are at the very beginning of this homomorphic encryption era, and we cannot expect to use it on a large scale, as requested by this scenario, but this would be an interesting research option for future Mobinet developments.

5.2.3. Certificates

The authentication of resources and access requesters is essential from a security point of view. It is not enough to be the only one able to decrypt encrypted data. One must be sure that it is the right one that is being decrypted. It can be more damaging to use false or inaccurate information than not being allowed to use the right one. Certificate mechanisms are used to ensure users they do use the right resources. Traditionally, certificates are digitally signed documents that mainly convey identity, but potentially credentials and attributes. The digital signature asserts information validity without the physical presence.
of the document or physical possession of the document. But the nature of the document may be wider than the usual identity oriented documents. In particular, certificates can convey any encrypted information, be they personal or privacy oriented ones (e.g. access rules or user policies), adding the required security with respect to the information integrity. Distributing access control policies via certificates has a significant cost on performances. As an example, the experiment described in the following article Certificate-based Access Control for Widely Distributed Resources (Mary Thompson) shows the overhead induced by such access control system, namely Akenty in their case.

<table>
<thead>
<tr>
<th></th>
<th>With Akenti (seconds)</th>
<th>No Akenti (seconds)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1Kbyte</td>
<td>0.76</td>
<td>0.02</td>
</tr>
<tr>
<td>1Mbyte</td>
<td>1.96</td>
<td>0.75</td>
</tr>
</tbody>
</table>

Table 2: Document fetch with and without Akenti access control

Based on such certificate technologies, authentication systems have been developed to keep transactions secure on the Internet, while protecting identity (cf. the EU-funded project Attribute-based Credentials for Trust, ABC4Trust, https://abc4trust.eu/). Still this focuses on authentication, and does not address personal data at large. It would be an interesting topic to investigate how such certificates could be used to represent not just people but also data through certified proxies.

5.3. Business performance and Privacy Lifecycle Costs

The previous operational handicaps induced by technical security are not negligible, but they become acceptable if the expected benefits can be assessed. This is more of an issue for Privacy by Design, since the impact of the methodology remains to be measured on complex projects. In particular, one cannot forecast the cost of Privacy by Design across all the phases of a complex project lifecycle.

5.3.1. Privacy-aware applicative design

Introducing privacy as a major concern in a project lifecycle is hampered by limitations and gaps in all the phases of a project, design, development, tests, deployment, maintenance —, since all these phases should consider privacy as a top priority. This is even more true within complex projects. Even in the simplest phase of design, complex projects require co-design capabilities across multiple domains of expertise. This will make privacy by design almost impossible to follow, since all facets and viewpoints around privacy will have to converge across subsystems, while functional consensus is already difficult to reach without considering privacy. No need to mention that this complexity exponentially increases along all the subsequent phases of the project lifecycle.

5.3.2. Privacy-aware application development
Formal languages and tools to enable privacy-aware application development are still in their infancy. Moreover, if one were to follow V-cycle development phases, one could at least decide to slow down each of the phases, letting privacy mature in the test and design phases, and waiting for the project to mature as a whole to start the actual development of privacy aspects. But V-cycle development is now largely abandoned, since agile development techniques are much more effective. We are hereby talking of effectiveness and not efficiency. With agile methodologies, organisations are sure to obtain something from the allocated resources, but with limited guaranty that the outcome will provide the intended target. Ironically, one of the main arguments for agile techniques is that they integrate better with co-design techniques. Our opinion is that because of the current impossibility to co-design complex targets, agile techniques put the focus on quick development and fast adaptation of objectives. This corresponds to a reactive design instead of a proactive design. Introducing privacy analysis, without accepting compromises that would contradict the Privacy by Design principles, will potentially ruin down all the benefits of agile development techniques.

5.3.3. Privacy-aware application deployment

It is one thing to obtain a privacy-aware application, but it is another matter to deploy it in a privacy-aware environment. This means in particular that all the administrative tasks of the application are, by default, configuring the application in a privacy-by-default mode, in order to optimally support the product administrator with compliance. As seen above in the subsection about Access Control Lists and GFAC, centralized access control services do not prevent malicious or risky configurations of resources. Even worse, they do not prevent the deficient implementation of access control APIs by resource hosting subsystem. This phenomenon can clearly happen with a service platform as Mobinet, where hosted services can be considered as resources providers. A privacy-aware deployment of Mobinet should qualify not only Mobinet central services, but also all the registered services, since the privacy chain has only the robustness of its weakest link. The privacy qualification process is a new domain to be discovered by platform providers, which could be based on a series of static tests, dynamic tests and certification processes. However, agile application development could also be considerably slowed down with such constraints.

5.3.4. Privacy-aware applicative maintenance

The ‘patch’ method is a well-known temporary correction measure in case of emergency with software maintenance. To solve a major problem as fast as possible, typically to quickly defuse dissatisfied or worried customers, this approach bypasses the standard procedural lifecycle steps from development to deployment.

No need to say that this is totally incompatible with the Privacy by Design principles. From a traditional maintenance point of view, bug correction for future releases should re-enter the full set of tests, considering privacy as a top priority. As a consequence, patching under Privacy by Design would likely take much longer, since a lot of mandatory tests would certainly fail from a privacy perspective. This would necessitate costly engineering reiterations, starting from the privacy-aware design phase. This is not a new type of cost in itself, but the repetitive effect of the same privacy centric constraints in each occurrence of the lifecycle loop would certainly force organisations to revisit their maintenance strategy.
5.3.5. Privacy-aware application governance

A new kind of functionality should ideally complete nominal applications: the privacy-aware dashboard, through which privacy officers could supervise and control the full set of access controls and their efficiency. In addition, this dashboard could help privacy officers to cope with their accountability responsibility, when services are delivered to external customers. Again, this might induce extra costs in terms of software lifecycle. It should be noted that such a tool should itself be developed in compliance with Privacy by Design, since all the produced visualisations would need to respect the privacy of the managed resources.

5.4. The Mobinet Privacy Framework: an interpretation of Privacy by Design for agile platforms

All the above considerations explain why Privacy by Design, expressed as the reference guideline of the implementation of the EU regulation is far from putting service providers in the best business situation. Based on those considerations, Xerox proposes an interpretation of Privacy by Design, reminiscent of the emergence of the GFAC (Generalized Framework for Access Control) in the nineties. This approach consists primarily in providing a generic access control service operating in conjunction with privacy policies defined externally. This architectural component would then concentrate the cost of privacy enforcement on the development, deployment, maintenance of this central access control engine. Applications would be responsible to simply redirect Access Control for each of their private field, as identified through privacy impact assessment, to this central service. Such an architectural approach would then reduce the privacy enforcement costs for a given application to a kind of functional post-design, exactly in line with agile methodologies.

For service providers, this proposed architecture induces two autonomous software development lifecycles: the traditional one, bound to the application proper, and the associated privacy development lifecycle bound to the evolution of privacy policies. The consistency is to be ensured via the privacy impact assessment through which private fields, applicative purposes and roles are identified.

At any time in the life cycle, it could be necessary to re-apply a technical translation of the privacy impact assessment: this translation will be in charge of pointing at the private fields and records in the application byte code, as required by the privacy impact assessment. This will make it possible to redirect the private fields to the privacy-centric access control engine. Roughly said, this would limit the privacy related cost to this specific privacy oriented post design, betting on the fact that the binding towards the enforcement engine could be generated through adjunction of aspects to the legacy applicative byte code.

This non-intrusive way at runtime could also be systematized through a dedicated privacy design tool. This privacy design tool would offer three main capabilities:

- Privacy by Default policy edition would leverage introspection capacities of modern software languages to formalize the identification of private fields and their binding to the applicative code, as well as the applicative purposes and roles
- Generation of aspects redirecting fields towards the generic access control engine, as prescribed in the edited policy.
- Consent edition based on previous Privacy by Default edition, enabling relaxed access control on specific fields, for informed purposes and roles; such consent, when deployed on the service provider server, would be directly interpreted, in real time, by the generic access control engine.

We do not detail here this technical proposal, as it is one of the challenges tackled by WP3.3, where we will experiment with the Mobinet Privacy Framework, based on the architectural principles described above. Mobinet is an ideal test bed for such experimental approaches, where the extra costs for service providers to address privacy concerns would be limited to the specific functional characteristics of their service software (application code introspection and aspects), while all the other costs induced by privacy would be concentrated on the generic access control engine and privacy-oriented design tools.

If the proposed approach appeared to be feasible at a reasonable performance rate, then Mobinet could be the instrument to promote a very new platform-oriented view of Privacy by Design, introducing Privacy by Agile Design to all the privacy stakeholders identified in this report. Eventually, Mobinet could offer innovative services to help service providers and users manage privacy in compliance with their respective obligations, concerns and interests.
6. Conclusion

This report highlights the complexity of personal data protection in projects focused on services interconnection platforms. The need for Mobinet to cope with this complexity is particularly reinforced by the nature of geolocation data at the core of mobility services, given that the geolocation data model is so straightforward that it enables persistent data propagation and correlation. We underlined that, when associated with individuals, this becomes a major threat to their privacy. From a state or surveillance perspective, we observe an increasing technical overlap between law enforcement and intelligence practices. Similarly, from a business perspective, the same intelligence techniques can be used for service improvement, to the user benefit, but also for intrusive and abusive tracking and cyberstalking.

After some geopolitical considerations, generic lessons have been drawn from the intent, content and status of the EU General Data Protection Regulation currently under discussion. The study of lobbies’ reactions led to the recognition that the lack of technical means to handle such a regulatory challenge may dangerously handicap the digital economy in the European Union. Recommendations placing user awareness at the core of privacy-oriented methodologies, such as Privacy by Design, are difficult to follow within projects whose complexity stems either from the number and diversity of actors or from the dynamicity of the system lifecycle.

Considering these tensions and threats, the report analysed social aspects and associated risks, and identified responsibilities and actors involved in the building of an acceptable response that would benefit all stakeholders. We introduced Mobinet as one of these responsible actors by establishing the rationale behind the Mobinet Privacy Framework.

The Mobinet Privacy Framework will enable to experiment with this methodology (this is the main purpose of Task3.3.3 in WP3.3). It is not meant to provide the final answer to the broad privacy issue, but aims at establishing innovative tools to be considered together with other advances in the field. The Mobinet project is a vehicle of choice to disseminate such findings.

From a software engineering point of view, we propose an innovative interpretation of Privacy by Design for agile platforms, focusing on the lifecycle particularities of any service oriented architecture instance.

From a business perspective, the rationale behind the envisaged Mobinet Privacy Framework could be summarized as follows:

1. Being focused on mobility, Mobinet must consider geolocation data as private by default.
2. Mobinet takes the responsibility for admin data and geolocation data collected via the MobiAgent component.
3. The platform is not responsible for data collected by services registered in Mobinet, but could qualify services with respect to Privacy Management.
4. New kind of services could be offered by the Mobinet consortium, in order to support the privacy compliance of registered services.
References


