FUTURE INTERNET PPP

Instant Mobility

Multimodality for people and goods in urban areas

FP7 . CP 284906

WP6 – D6.6 Multimodal services in a city: security and privacy challenges - Final report

March 2013

Editors : Daniel Gidoin, Thalès
Bas van Schoonhoven, TNO
Gabriella Bodea, TNO
Nathalie Dubus, Orange
Sander van Oort, TNO

License

SEVENTH FRAMEWORK PROGRAMME

Project funded by the European Commission under the 7th European Framework Programme for RTD - ICT theme of the Cooperation Programme.

Instant Mobility WP6.3

D6.6 Instant Mobility Security and privacy challenges – final report

WP6	Multimodal services acceptability report - v1
Authors	Nathalie Dubus (Orange) Daniel Gidoin (Thales) Bas van Schoonhoven (TNO)
Short Description	This deliverable provides a final analysis of security and privacy challenges of Instant Mobility .
Dissemination level (select)	PU Public
Date	April 2013
Status	Deliverable
Contributions by:	Gabriela Bodea (TNO) Sander van Oort (TNO)
Internal review by	DLR, TLI
Internally accepted by	Nathalie Dubus
Date of acceptance	15 April 2013

Deliverable Abstract

This document represents the final deliverable of task 6.3. This task “Privacy, data and people protection” aims to evaluate the requirements of security and privacy for the Instant Mobility scenario, and proposes recommendations on privacy, anonymisation and security issues.

A first security risk assessment has been performed in Chapter 2, then a privacy impact assessment in Chapter 3: the security impact assessment identified three critical risks related to personal data, invoicing and visualization, and the privacy impact assessment identified three main risks. Based on these assessments, the deliverable provides in Chapter 4 recommendations for further detailed designed phase.

Contents

1. Introduction

The Instant Mobility project has created a concept for a virtual "Transport and Mobility Internet", a platform for information and services able to support radically new types of connected applications for scenarios centred on the stakeholder groups:

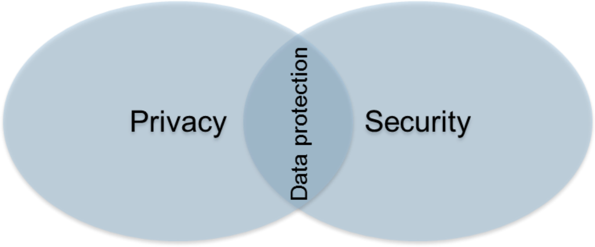
- multimodal travellers,
- drivers & passengers,
- passenger transport operators,
- goods vehicle operators, and
- road operators & traffic managers.

The project defines requirements for Future Internet technology tools and enablers, so that all these services will be available to any Internet-connected user, whether using a portable, vehicle-based or fixed terminal.[1]

In the Instant Mobility Deliverable 3.3, three conceptual scenarios were defined for different Instant Mobility applications:

1. Personal Travel Companion: demonstrates the capabilities provided by the future Internet technologies for multi-modal travel, mainly in urban and inter-urban areas.
2. Smart City Logistics Operations: describes how transport operations can be improved with respect to safety, efficiency, environmental performance and quality of service.
3. Transport Infrastructure as a Service: a study of the conditions needed for dynamic traffic & integrated urban space management, on how to use Future Internet technologies such as cloud data storage, Cloud computing virtualization or services-in-the-cloud.[2]

For each of these scenarios, both security and privacy are of critical importance for the user acceptance of such services. Security and privacy can be regarded as complimentary, each concept including aspects not directly relevant for the other. For example, anonymisation of personal data can be used as both a security measure and a privacy-enhancing one, whereas the security of critical non-personal data is highly important but not a privacy issue as such. However, with regards to the protection of personal data, there is a significant overlap:



To cover both security and privacy issues involved in Instant Mobility applications, two main activities were performed: a security risk assessment (described in chapter 2), and a privacy impact assessment (described in chapter 0). In this report we discuss the outcomes of both assessments that were performed on an instant mobility scenario. Based on these assessments we provide recommendations in chapter 4 for ensuring security and privacy protection when designing and implementing an instant mobility application, and promoting user trust and acceptance.

[1] This is taken from the Instant Mobility Grant Agreement Annex I - "Description of Work"

[2] As described in chapter 3 of Instant Mobility FP7 project, 2012, Deliverable 3.3 – Instant Mobility Use Case scenarios definition & analysis

2. Security Risk Assessment

2.1 Risk analysis terminology

Essential elements:
Functions or missions of the system susceptible to damage

Impact:
Impact of the damage as financial loss, loss or prejudice to the business reputation, suspension of the business activity, failure to comply with the law, loss of competitiveness, non-compliance..

Source of the threat:
Human accidental action, deliberate action by the Staff or external people, malware, backdoor, key logger…

Security criteria vector:
Confidentiality, Availability, Integrity, Accountability

Supporting assets or Targets:
Logical or physical components of the system subject to attacks

Threat:
Software modifications not approved, sniffing, denial of service, data theft, spying, server failure…

Vulnerability:
The Risk Assessment Viewpoint vulnerability can be populated with vulnerabilities as described in on-line vulnerability databases as the **Common Vulnerabilities and Exposures (CVE)** from National **Vulnerability Database (NVD)**.

2.2 Risk analysis methodology

Our Risk Assessment methodology is inspired by the French EBIOS risk analysis methodology, both version 2 and 2010, used for administration and defense, and adopted by the industry. Founded in 1995 by the ANSSI and regularly updated, the EBIOS method (Expression of Needs and Identification of Security Objectives) benefits from 15 years of experience in the field of risk management. It is used to assess and treat risks related to information systems security (ISS). It also allows communicating them within the organization and with its partners, thus forming a complete tool for managing ISS risks. Modular and consistent with international standards ISO / IEC 31000, ISO / IEC 27005, ISO / IEC 27001, the EBIOS method remains the essential toolkit for any discussion related to information security to build its ISS repository enterprise risk management and to integrate ISS into existing projects or systems regardless of their level of advancement.

Our Risk Assessment study shall split the activities in 7 steps:
Activity 1: Identifying essential elements
Activity 2: Analysis of the damages
Activity 3: Determination of the support elements
Activity 4: Determination of the vulnerabilities
Activity 5: Analysis of the threats
Activity 6: Definition of the risks
Activity 7: Definition of the Security Solutions

2.2.1 Activity n°1: Identifying essential elements

This activity takes as input the functional part of the system architecture elaborated during the mainstream system engineering process, by the system architect. The functional architecture of the system is analyzed by the system security risk manager in order to identify, within the functions and data of this system architecture, the essential elements that need protection. These essential elements define the scope for the system security analysis.

2.2.2 Activity n°2: Analysis of the damage

This activity requires the involvement of the system owner. It consists of imagining damage scenarios which could occur to the system and hurt it.

2.2.3 Activity n°3: Determination of the support elements

Typically, a target references the logical or the physical part of the system architecture which supports the functions annotated as **Essential Elements** of the study.

2.2.4 Activity n°4: Determination of the vulnerabilities

This activity consists in listing the vulnerabilities related to the previously identified target-types.
The Risk Assessment Viewpoint vulnerability can be populated with vulnerabilities as described in on-line vulnerability databases (CVE) – see 2.1 Risk analysis terminology.

Vulnerability scale: The vulnerability scale defines the value of the weakness of a target together with the ease to exploit it. The vulnerability scale is a scale from 0 to 4 can be defined as the following:

- 0 means “not relevant”;
- 1 is “low”;
- 2 is “medium”;
- 3 is “high”;
- 4 is “critical”.

Severity scale: The severity scale defines the severity of a risk if it occurs. The severity scale is a scale from 0 to 4 can be defined as the following:

· 0 means “not relevant”;
· 1 is “low”;
· 2 is “medium”;
· 3 is “high”;
· 4 is “critical”.

Opportunity scale: The opportunity scale defines the value of the chances for a risk to occur. The opportunity scale is a scale from 0 to 4 can be defined as the following:

- 0 means “not relevant”;
- 1 is “low”;
- 2 is “medium”;
- 3 is “high”;
- 4 is “imminent”.

2.2.5 Activity n°5: Analysis of the threats

The activity consists in analyzing the threats and their targets. Threats shall be associated with a breach strength which is valued for each security criterion according to the breach strength scale.

2.2.6 Activity n°6: Definition of the risks

Risks are expressed at both functional and architecture plans of the system architecture, respectively by means of the damages and of the threats.

All the system modeling tool layers of representation of the system model shall be relevant for the Risk review. At functional level, the risks shall occur because of the damages identified, at architecture level, the risks shall occur because of the threat identified. Otherwise for each risk, the system security risk manager shall review the damage associated to it, and the essential elements it applies to. He shall also review the threats associated to it, and the targets it applies to.

Risk level: The risk level scale shall score the level of security that is targeted on a given perimeter. The risk level scale is a scale from 0 to 4 can be defined as the following:
- 0 means “not relevant”;
- 1 is “low” (negligible, minor);
- 2 is “medium” (Significant);
- 3 is “high” (Serious);
- 4 is “critical” (Intolerable).

The two dimensions of severity and opportunity for risk quantification shall be projected on a single dimension called Risk level. This table is also named “risk aversion matrix”. The rule bellow has been decided at the beginning of the study.

Severity scale	Opportunity scale			
	1	2	3	4
1	Low	Low	Low	Low
2	Low	Low	Low	Medium
3	Medium	Medium	High	High
4	High	Critical	Critical	Critical

2.2.7 Activity n°7: Security solution

At this stage of the study, system security risk manager has got a list of valuated risks. He should now define a risk management strategy and security solution that set an acceptable risk level. The system security risk manager can review the security needs of the essential elements, and set the required risk level of the target. The risk manager defines the management strategy to cover the risk.

2.3 Risk analysis

2.3.1 Feared event 1

Unauthorized disclosure of personal information
The impact can be financial or damaging to the business reputation of the service providers or trusted authority, on the social image of the traveler or drivers.

Essential Element	Personal data (identity, credit card information, preference, GPS data..)	
Impact	Privacy violation, risk financial loss, misused identity	
Source of the threat	Description	Probability

	Internal human source & Service Providers with or without malicious intent	Strong
	External malicious action with low or significant capacities	Maximum
	Malware	Maximum
	Internal event	Significant
Security criteria vector	Confidentiality	
Supporting Asset	Data Distribution Service, Billing Service, Journey Monitoring Service	
Threat	Software misusing, Unauthorized modification of software, passive listening, man-in-the-middle attacks, key logging software, "backdoor"..	
Vulnerability	CVE data base concerning OpenSplice DDS, Red Hat OS, Java server, MySQL server, encryption and anonymization tools)	
Risk Level	CRITICAL	
Security solution	Strong authentication, Access control policy, Security monitoring service, regular risk analysis, software updating, PKY with Pseudonym certificates, Traveller & Driver data (route, GPS position..) anonymization, Anonymisation audit tool	

2.3.2 Feared event 2

Inaccessibility of the Journey Monitoring

The impact can be financial (delay due to modes of traveler transport not well aligned with traffic, missed appointment) on the social image (delay for an appointment, absence from work), or legal (failure to comply with a legal obligation...) for the traveler, financial for a taxi or private driver (car-pooling failure), financial or damaging to the business reputation of the service providers.

Essential Element	Journey monitoring updated in real time	
Impact	Financial, business reputation, image, legal obligation failure	
Source of the threat	Description	Probability
	Internal human source & Service Providers with or without malicious intent	Significant
	External malicious action with low or significant capacities	Strong
	Malware	Maximum
	Internal event	Significant
Security criteria vector	Availability	
Supporting Asset	Journey Monitoring Service	
Threat	Software misusing, Unauthorized modification of software, denial of Service (DOS or DDOS)	

Vulnerability	CVE data base concerning Java server and Red Hat OS
Risk Level	HIGH
Security solution	Security monitoring service, regular risk analysis, software updating

2.3.3 Feared event 3

Inaccessibility of the Route Determination Engine

It is not possible to compute a route or update The impact can be financial (delay caused by transport not well aligned with traffic..) on social image or legal (missed appointment) for the traveler, financial for taxi or private driver (car-pooling failure), financial or damaging to the business reputation of the service providers.

Essential Element	Route Determination	
Impact	Financial, business reputation, image, legal obligation failure	
Source of the threat	Description	Probability
	Internal human source & Service Providers with or without malicious intent	Significant
	External malicious action with low or significant capacities	Strong
	Malware	Maximum
	Internal event	Significant
Security criteria vector	Availability	
Supporting Asset	Route Determination Engine	
Threat	Software misusing, Unauthorized modification of software, denial of Service (DOS or DDOS)	
Vulnerability	vulnerability on C++ code and Red Hat OS CVE data base	
Risk Level	MEDIUM	
Security solution	Security monitoring service, regular risk analysis, software updating	

2.3.4 Feared event 4

Unavailability of travel data

The unavailability of travel data does not allow for alternative routes offering and thus the usage of the "Instant mobility" services. The impact can be financial or on social image for the traveler, financial for taxi or private driver, financial or damaging to the business reputation of the service providers.

Essential Element	Shared Data Distribution	
Impact	Financial, business reputation, image, legal obligation failure	
Source of the threat	Description	Probability

	Internal human source & Service Providers with or without malicious intent	Significant
	External malicious action with low or significant capacities	Strong
	Malware	Strong
	Internal event	Significant
Security criteria vector	Availibility	
Supporting Asset	Data Distribution Service	
Threat	Software misusing, Unauthorized modification of software, denial of Service (DOS or DDOS)	
Vulnerability	CVE data base concerning OpenSlice DDS and Red Hat OS.	
Risk Level	MEDIUM	
Security solution	Security monitoring service, regular risk analysis, software updating	

2.3.5 Feared event 5

Invoicing errors

Financial impact for public transportation providers, drivers and taxis (inability to bill), legal (billing dispute and litigation) or damaging to the business reputation of the service providers (claims, suspected fraud ...).

Essential Element	Billing	
Impact	Financial, business reputation	
Source of the threat	Description	Probability
	Internal human source & Service Providers with or without malicious intent	Strong
	External malicious action with low or significant capacities	Maximum
	Malware	Maximum
	Internal event	Significant
Security criteria vector	Integrity	
Supporting Asset	Billing Service	
Threat	Software misusing, Unauthorized modification of software, man-in-the-middle attacks, "backdoor"..	
Vulnerability	vulnerability on C++ code and Red Hat OS CVE data base	
Risk Level	CRITICAL	
Security solution	Security monitoring service, regular risk analysis, software updating	

2.3.6 Feared event 6

Inappropriate assessment of traffic

Databases supplied by the road traffic and rail, traveler requests, delays etc.. are not reliable. It is impossible managing traffic and combating traffic jams, and optimizing public transportation. Environmental impact (increased pollution, passenger discomfort), safety and security impacts (delayed intervention of rescue and police), financial and image impact.

Essential Element	expected traffic and optimization	
Impact	Environmental, safety, security, financial, image	
Source of the threat	Description	Probability
	Internal human source & Service Providers with or without malicious intent	Significant
	External malicious action with low or significant capacities	Strong
	Malware	Strong
	Internal event	Significant
Security criteria vector	Integrity	
Supporting Asset	Public Transportation database, Journey monitoring data base	
Threat	Software misusing, Unauthorized modification of software, man-in-the-middle attacks, "backdoor"..	
Vulnerability	CVE data base concerning MySQL server and Red Hat OS	
Risk Level	MEDIUM	
Security solution	Security monitoring service, regular risk analysis, software updating	

2.3.7 Feared event 7

Lack of trust in the authentication service

The impacts: Risk of billing errors not taken into account preferences, unable generating traveler and drivers certificates, or sending the identity information to the police in case of aggression.

Essential Element	Traveler and Driver Authentication	
Impact	Financial, legal, Security	
Source of the threat	Description	Probability
	Internal human source & Service Providers with or without malicious intent	Significant
	External malicious action with low or significant capacities	Strong
	Malware	Maximum

	Internal event	Significant
Security criteria vector	Accountability, availability	
Supporting Asset	Trusted Tierce Party Service	
Threat	Software misusing, Unauthorized modification of software, man-in-the-middle attacks, "backdoor"..	
Vulnerability	CVE data base concerning PKI and Red Hat OS	
Risk Level	HIGH	
Security solution	Security monitoring service, regular risk analysis, software updating	

2.3.8 Feared event 8

Inaccessibility of Enrollment services

Financial impact for Instant Mobility Service Providers, the registration of new customers being impossible.

Essential Element	Identity Management	
Impact	Financial	
Source of the threat	Description	Probability
	Internal human source & Service Providers with or without malicious intent	Significant
	External malicious action with low or significant capacities	Strong
	Malware	Maximum
	Internal event	Significant
Security criteria vector	Availability	
Supporting Asset	Identity Management Service	
Threat	Software misusing, Unauthorized modification of software, man-in-the-middle attacks, «backdoor"...	
Vulnerability	CVE data base concerning IDM tool and Red Hat OS	
Risk Level	HIGH	
Security solution	Security monitoring service, regular risk analysis, software updating	

2.3.9 Feared event 9

Failure of Visualization Services

Impact: Instant Mobility Services becoming unusable, we can be expected to lost of image with a Financial impact.

Essential Element	Visibility on current request, route, traffic, billing, events..

Impact	Financial, image (Services in full unusable)	
Source of the threat	Description	Probability
	Internal human source & Service Providers with or without malicious intent	Significant
	External malicious action with low or significant capacities	Maximum
	Malware	Maximum
	Internal event	Significant
Security criteria vector	Availability	
Supporting Asset	Display Server	
Threat	Software misusing, Unauthorized modification of software, man-in-the-middle attacks, "backdoor"..	
Vulnerability	CVE data base on java server and Red Hat OS	
Risk Level	CRITICAL	
Security solution	Security monitoring service, regular risk analysis, software updating	

2.4 Risk responses

The risk responses table will provide the base of security specifications for the target system and its environment. Each of identified risks (first column) refers to a feared event above.

Feared event	Risk	Risk avoidance	Risk mitigation	Risk-taking	Risk transfer
1	Risk related to unauthorized disclosure of personal data		X		(X)
2	Risk related to Inaccessibility of the journey monitoring	(X)	X	(X)	(X)
3	Risk related to inaccessibility of the route determination	(X)	X	(X)	
4	Risk related to unavailability of travel data		X	(X)	
5	Risk related to errors in invoicing	(X)	X		(X)
6	Risk related to an inappropriate assessment of traffic		X	(X)	
7	Risk related to the lack of trust in the authentication service	(X)	X		
8	Risk related to inaccessibility of Enrollment service	(X)	X	(X)	(X)

9	Risk related to Failure of visualization services	(X)	X		(X)

A cross fits at first choice, a cross in parentheses fits other possibilities.

Definitions:

- Risk-taking: in such case, the risk is accepted and no preventive action is taken.
- Risk transfer: Risk is transferred toward an insurance contract.

Remarks:

- Avoidance was not selected when it requires the implementation of solutions too expensive or technically almost impossible.
- Risk transfert was not selected when it is inadequate risk solving.

2.5 Security Recommendations

The Risk responses table above is the entry point of our recommendations, each of security measure referring to one or more identified risk (column 2 in the Risk responses table).

Security measure	Risk related to unauthorized disclosure of personal data	Risk related to Inaccessibility of the journey monitoring	Risk related to inaccessibility of the route determination	Risk related to unavailability of travel data	Risk related to error in invoicing	Risk related to inappropriate assessment of traffic	Risk related to the lack of trust in authentication service	Risk related to inaccessibility of Enrollment service	Risk related to visualization failure
Development of Security Policy	X	X	X	X	X	X	X	X	X
Strict obligations of confidentiality	X				X				
Agreement on data exchange (customers & partners)	X			X		X			
Annual audit of security measures	X	X	X	X	X	X	X	X	X
No lax management of access rights (least privilege policy)	X	X	X	X	X	X	X	X	X

Security measure	Risk related to unauthorized disclosure of personal data	Risk related to Inaccessibility of the journey monitoring	Risk related to inaccessibility of the route determination	Risk related to unavailability of travel Information	Risk related to errors in invoicing	Risk related to inappropriate assessment of traffic	Risk related to the lack of trust in authentication service	Risk related to inaccessibility of Enrollment service	Risk related to visualization failure
Keys management policy	X			X			X	X	
measures to preserve legal evidences	X	X	X		X		X	X	
Insurance contract extended to IT risks	X	X			X			X	X
Security event feedback from service providers	X	X	X	X	X	X	X	X	X
Strong authentication service	X	X	X	X	X	X	X	X	X
Encryption of data	X			X			X	X	
Encryption flow	X			X			X	X	
Promote Security by design (FI-WARE MulVal Attack path Engine GE)	X	X	X	X	X	X	X	X	X

Security measure	Risk related to unauthorized disclosure of personal data	Risk related to Inaccessibility of the journey monitoring	Risk related to inaccessibility of the route determination	Risk related to unavailability of travel Information	Risk related to error in invoicing	Risk related to inappropriate assessment of traffic	Risk related to the lack of trust in authentica-tion service	Risk related to inaccessi-bility of Enrollment service	Risk related to visualization failure
Promote Security monitoring (FI-WARE Security Monitoring GE)	X	X	X	X	X	X	X	X	X
(1) FI-WARE Decision Making Support	X	X	X	X	X	X	X	X	X
(2) FI-WARE Data handling GE	X				X		X		
Deploy anti-malware tool	X	X	X	X	X	X	X	X	X
Deploy IDS tool	X	X	X	X	X	X	X	X	X
(3)Pseudonym Certificate	X						X		
(4) Anonymizer	X								
(5) DB Anonymiser	X								

(1) FI-WARE Decision Making Support provides tool to security operators for proposing cost-sensitive remediations to attack paths. It computes remediations that could reduce or cut an attack path, ordered by cost, to security operators.

(2) FI-WARE Data Handling GE is a privacy-friendly attribute-based access control system permitting to store information together with an attached privacy policy, which regulates its usage. Thus, Data Handling GE can reveal certain attributes, according to specific supplied prove conditions.

(3)Pseudonym Certificate can be used as trusted Traveller and Driver identity since the Traveller initial planning request until arrival for destination. This certificate will be used also to pay the services delivered as e-tickets and carpool driver. The police department that receives a call for help, automatically queries the Trusted CA (Certificate Authority) to know the identity associated with the Pseudonym Certificate received.

(4) Anonymizer: The Travellers and Drivers Data (Routes, GPS position..) used by Public Transportation, for traffic Optimization, should be anonymised before processing.

(5) FI-WARE DB_Anonymizer allows understanding if a certain anonymization policy, used to anonymize a dataset, should be considered safe or not. A function calculates a value representing the likelihood that an attacker can reconstruct exactly the dataset’s content, starting from the anonymized data.

3. Privacy Impact Assessment

In the previous chapter a number of security risks were identified, and means to mitigate these risks were discussed. In this chapter we turn to the privacy issues involved in the envisioned Instant Mobility applications. First the approach that was taken in the impact assessment is discussed, then a key Instant Mobility scenario is analysed, and finally risks and means of mitigating these risks are identified.

3.1 Approach

The description of the approach taken here consists of several steps: first some key concepts are introduced, such as privacy and privacy by design. Then the privacy impact assessment methodology itself is described, and the scope of the assessment is defined.

3.1.1 Privacy

The concept of privacy has a long history and it has been defined in many ways. Back in 1890, Warren and Brandeis defined it as "*the right to be let alone*".[3] In 1967, the influential privacy researcher Alan Westin described it as "*an instrument for achieving individual goals of self-realization*" and "*the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others*".[4]

More recently, it has been recognized that privacy is a concept that is impossible to fully define in a single definition, and that there are multiple forms of privacy, for example by Daniel Solove in his book "Understanding Privacy".[5] Finn et al. provide an up-to-date and workable description of privacy in which seven types of privacy are identified:

1. privacy of the person / body;
2. privacy of behaviour and action;
3. privacy of communication;
4. privacy of data and image;
5. privacy of thoughts and feelings;
6. privacy of location and space; and
7. privacy of association.[6]

In order to analyse the privacy issues involved in Instant Mobility applications, the full breadth of what the concept of privacy means should be understood. It is not just the privacy of personal data ("data protection") or information security; it is a broader issue involving several other types of privacy such as privacy of behaviour and action, privacy of location, or privacy of association.

The general context increases the privacy issues. The multiplication of usage, especially on Internet and mobile devices (social networks, online services and tracking services) has implied an augmentation of the volume and variety of data that concerns privacy issues and that increase

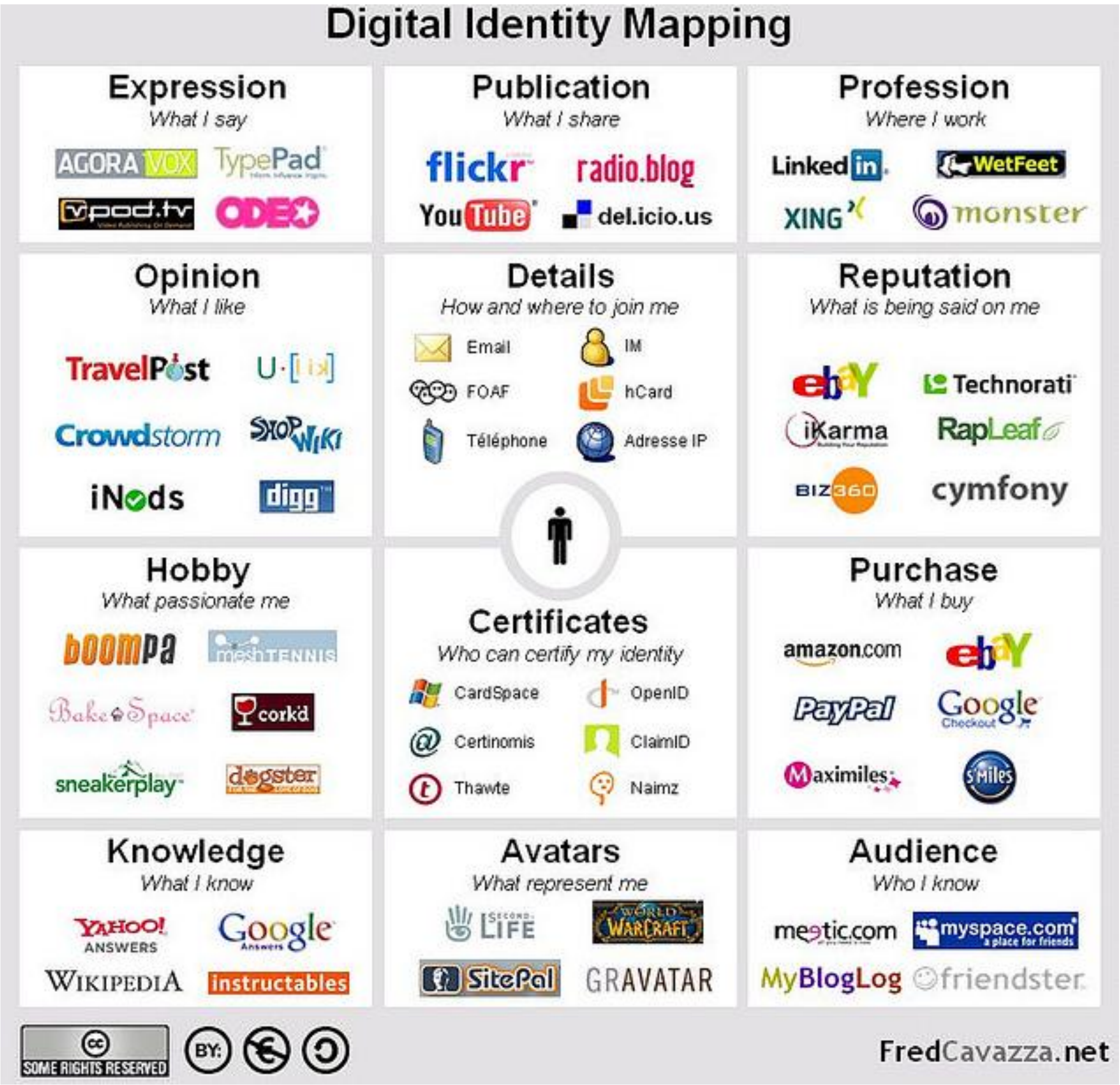
[3] Warren, S. D., & Brandeis, L. D. (1890). Right to Privacy. (K. Ziegler, Ed.) Harvard Law Review, 4(1), 72.

[4] Westin, A. F. (1967). Privacy and Freedom. Atheneum.

[5] Solove, D.J. (2008). Understanding Privacy. Harvard University Press.

[6] Rachel L. Finn, David Wright, and Michael Friedewald. "Seven Types of Privacy" *European Data Protection: Coming of Age*. Ed. S. Gutwirth et al.. Dordrecht: Springer Science+Business Media, 2013.

awareness. As the global traffic on mobile networks will double each year through 2014 and the awareness of people about their fragmented digital identity (see the Digital Identity Maping below) will spread, the privacy will be more and more a matter of concern. All the content the user gives when leaving marks on sites and on the index of search engines, and the digital reputation of individuals and its valuation (audience monetization, expertise ...) recently led more and more users to worry about their digital identity. The notion of "digital identity" is interesting as it shows to the user that his identity on Internet is made of both formal data (contacts, certificates) and informal data (comments, notes, pictures, etc.) :



Instant Mobility is also a context where interactions between users within Social Networks will be important, and the amount of data exchanges between heterogeneous actors will be high. So the travellers may have different acceptance level to give private data according to the type of data. For instance, name and first name are more acceptable – nearly 90% in the last IDATE French study [20] - than the location – 39%. Other criteria influence the acceptance: the actor you give it to, and the purpose. In the same study, the trust differs according to the actor legitimacy: 74% of the respondents agree to give their name and first name to a local government but only 5% of them agree to give their bank details (against 62% and 34 % to a e commerce website).

According to many studies, the main value the users need are: transparency, security, protection and self managing of the data. As proposed by the EC, trust and privacy may go through informed and explicit consent.

3.1.2 Designing for privacy

Protecting the privacy of Instant Mobility users requires that we start paying attention to privacy issues involved in Instant Mobility applications during its design. This is usually referred to as a *Privacy by Design* approach: systematically taking privacy issues into account, not only after implementing a system or service, but as early as possible. There are a number of ways in which we can approach this. First we can define a number of principles to adhere to when designing and operating a system or service: so-called principles of fair information practice (FIPs). A commonly referred to set of principles are those that were formulated by the U.S. Department of Health, Education and Welfare in 1973, which are in brief:

1. **Notice/Awareness**: Consumers should be given notice of an entity's information practices before any personal information is collected from them. Without notice, a consumer cannot make an informed decision as to whether and to what extent to disclose personal information.
2. **Choice/Consent**: giving consumers options as to how any personal information collected from them may be used.
3. **Access/Participation**: an individual's ability both to access data about him or herself and to contest that data's accuracy and completeness.
4. **Integrity/Security**: personal data must be accurate and secure.[7]

These principles form the starting point for most data protection regulations, and have been updated and extended over time, most recently in the proposed EU Data Protection Regulation. We use an updated and condensed set of these fair information practice principles as a practical set of high-level privacy requirements for Instant Mobility applications:

1. *Limited collection and use of personal data:* Personal data is only collected and processed for a clearly defined purpose. The data must be adequate for this purpose, and may not be used for other purposes without consent of the data subject or stored longer than required for achieving the purpose.
2. *Transparency of personal data processing*
   There must be an easy way for a data subject to find out what information about him or her is collected and how it is used.
3. *The user is in control*
   Personal data will only be collected or used for a purpose with the data subject's clear consent. The user must have a way to correct or amend his or her personal data.
4. *Security of personal data processing*
   Appropriate organizational and technological security safeguards are used to protect personal data from loss or theft.

These principles are related. Consent is meaningless unless it is *informed* consent as consent is only meaningful if the data subject understands what information is collected or processed and for what purpose. Consenting with the processing of personal data also implies consent for the processing of this data for a specific purpose.

[7] Ware, W. W. (1973) Records, Computers and the Rights of Citizens. United States: U.S. Department of Health, Education and Welfare. Read more on the FIPs online at: http://www.ftc.gov/reports/privacy3/fairinfo.shtm

The principles provide guidance in *what* to do. However, they do not tell us *how* to do this. One approach is through purely technological means, through the use of so-called Privacy Enhancing Technologies, for example specific forms of encryption or the use of anonymisation tools.[8] However, the use of technologies alone cannot guarantee a sufficient level of privacy protection, as human behaviour, organizational processes, and even the organization of physical spaces are important factors as well. The concept of Privacy by Design is used to promote this broader approach: taking privacy into account at an early stage, and looking at both the technological and the organizational side.[9]

A simple yet very effective step in ensuring privacy protection is "Privacy as the Default Setting" [10] or Privacy by Default. This is a Privacy by Design basic principle that – by default – personal data are not processed, and the processing of personal data is an exception that requires justification. This as opposed to a "collect by default" approach which is often taken in practice, in which as much personal data are collected as possible, just in case it may prove to be useful later.

3.1.3 User-centred design for privacy

A focus on technological and organizational means of protecting privacy, while useful, also has a weakness: the focus is not on the needs of the data subject, and because of this certain issues may be overlooked. This is related to the principles of transparency of processing and the user in control. Recently, more attention has been given to the user interface side of Privacy by Design, for example in an excellent discussion of Privacy by Design and an analysis of Google and Facebook incidents by Ira Rubinstein.[11]

In this regard Helen Nissenbaum's theory of privacy as contextual integrity is useful. She understands privacy as a set of norms covering different social contexts. A social context may for example be a health care setting, a schoolyard, a dinner in a living room, or a community meeting. In different social contexts, different norms with regards to privacy and the way personal information are expected to be observed.[12] For example, in an intimate setting, such as when among close friends, much more detailed personal data may be expected to be shared than during a work meeting.

3.1.4 Legal framework on privacy

Privacy is a fundamental human right that is enjoys extensive yet complex legal protection. In article 8 of the European Convention on Human Rights the right to privacy is described as "*Everyone has the right to respect for his private and family life, his home and his correspondence."* With regards to personal data protection, the EU regulatory framework is based on the 1995 Data Protection Directive[13], which is currently in the process of being revised. The Data Protection Directive shares the same ethos as the Fair Information Principles as many other similar legal and regulatory efforts,

[8] E.g. as described in Koorn, R., Gils, H. van, Hart, J. ter, Overbeek, P., & Tellegen, R. (2004). Privacy-Enhancing Technologies: White Paper for Decision-Makers. The Hague.

[9] Lieshout, M. van, Kool, L., Schoonhoven, B. van, & Jonge, M. de (2011). Privacy by Design: an alternative to existing practice in safeguarding privacy. Info, 13(6), 55–68.

[10] Cavoukian, A. (2009). Privacy by Design - The 7 Foundational Principles. Toronto, Ontario.

[11] Rubinstein, I., & Good, N. (2012). Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents. New York.

[12] Nissenbaum, H. (2010). Privacy in Context: Technology, Policy, and the Integrity of Social Life. Palo Alto, CA: Stanford University Press.

[13] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

and has been translated into national law in the EU Member States (although there are differences in how the different Member States have interpreted the Directive).

The on-going revision of the current EU regulatory framework on data protection is expected to result in a Regulation[14] that will replace the current Directive as the general regulatory framework for data protection in the EU. Although the process is still on-going, some of the possible changes to be expected are already known, including: a data breach notification obligation (within 24 hours), a data portability clause (i.e. more extensive provisions for data subjects to access as well as transfer their personal data), and a "right to be forgotten", which proposes that people should be able to delete their data for example if there are no legitimate grounds for retaining them.

Protection Directive of 1995 was already revised in January 2012 to harden existing legal obligations, particularly on explicit consent and introduces right to be forgotten and portability right.

Since the legal framework is currently undergoing revision, and the currently envisioned Instant Mobility applications are at an early stage, a precise compliance check to current or future EU privacy regulation is not possible. However, we assume that by acting at such an early design stage based on the four high-level principles described earlier (*Limited collection and use of personal data, Transparency of personal data processing, The user is in control, Security of personal data processing*), we are already taking significant steps towards ensuring adequate privacy protection of the eventual Instant Mobility services.

3.1.5 Privacy Impact Assessment

A Privacy Impact Assessment (PIA) is a prospective and systematic assessment of potential privacy impacts that new or changed systems or programmes pose to individuals. Additionally, the PIA can investigate means to avoid negative impacts or suggest mitigation strategies. In a PIA the impacts are assessed in terms broader than those of legal compliance or security risks. In that, a PIA is process- rather than output-oriented. The key elements in this brief description are shared by the most commonly used definitions of what a PIA is. [15]

The systematic use of Privacy Impact Assessments is typically advocated by data protection authorities such as the UK Information Commissioners Office, that provides a PIA handbook online.[16] In a number of countries, including the USA and parts of Canada, performing a PIA is compulsory for government agencies whenever a new or significantly changed IT system is introduced.

With regards to the handling of personal data, it is important to avoid focusing on a single stage in the lifecycle of data. Typically, data (such as personal data) goes through a number of different steps, from its collection, processing, dissemination or disposal, see Figure 1.

[14] EU directives lay down certain end results that must be achieved in every Member State. National authorities have to adapt their laws to meet these goals, but are free to decide how to do so. A regulation is a binding legislative act which must be applied in its entirety across the EU.

[15] Linden Consulting, 2007, Privacy Impact Assessments: International Study of their Application and Effects

[16] UK ICO Privacy Impact Assessment Handbook, available online at: http://www.ico.gov.uk/pia_handbook_html_v2/files/PIAhandbookV2.pdf

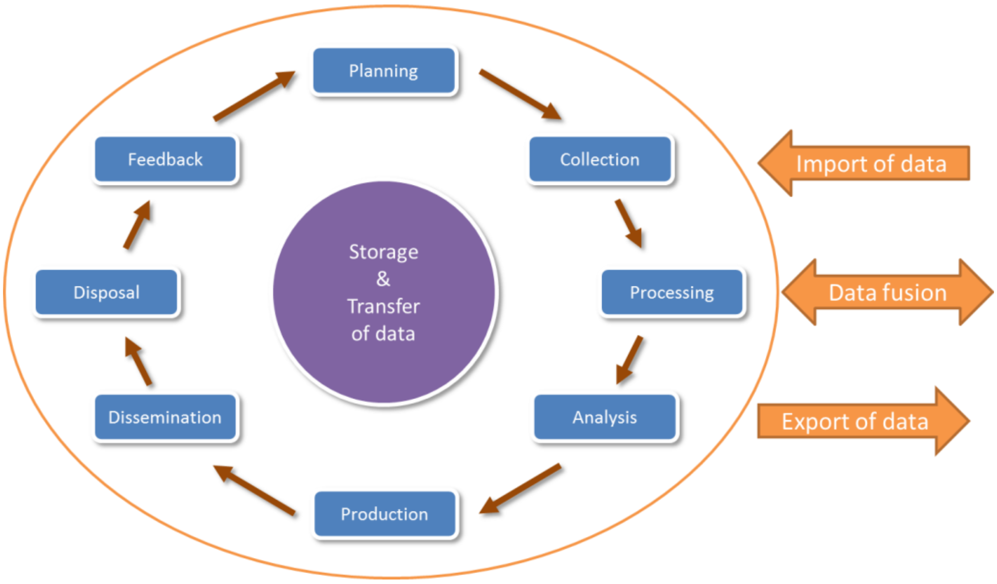


Figure 1 –Data lifecycle

Source: Bodea, G. in Deliverable 3.1, sub-deliverable PIA, FP7 Virtuoso

Each stage may pose privacy issues specific to that stage, e.g. during collection it is essential to obtain the data subjects consent to the collection of his or her data for a specific purpose, while during disposal data carriers such as hard drives or USB storage devices need to be adequately erased.

Risks to privacy may occur on many different levels, including the:

- technical,
- operational or organizational,
- institutional,
- of policy or strategy and
- legal or regulatory level.

Solutions to these risks, or means to mitigate the risks, may be defined along the same lines. However, the solutions may be of a different kind than the problem, e.g. a technical solution to an organizational problem may be feasible. Finally, some risks may be impossible to mitigate, and other risks may still be unidentified after the risk assessment, as shown in Figure 2.

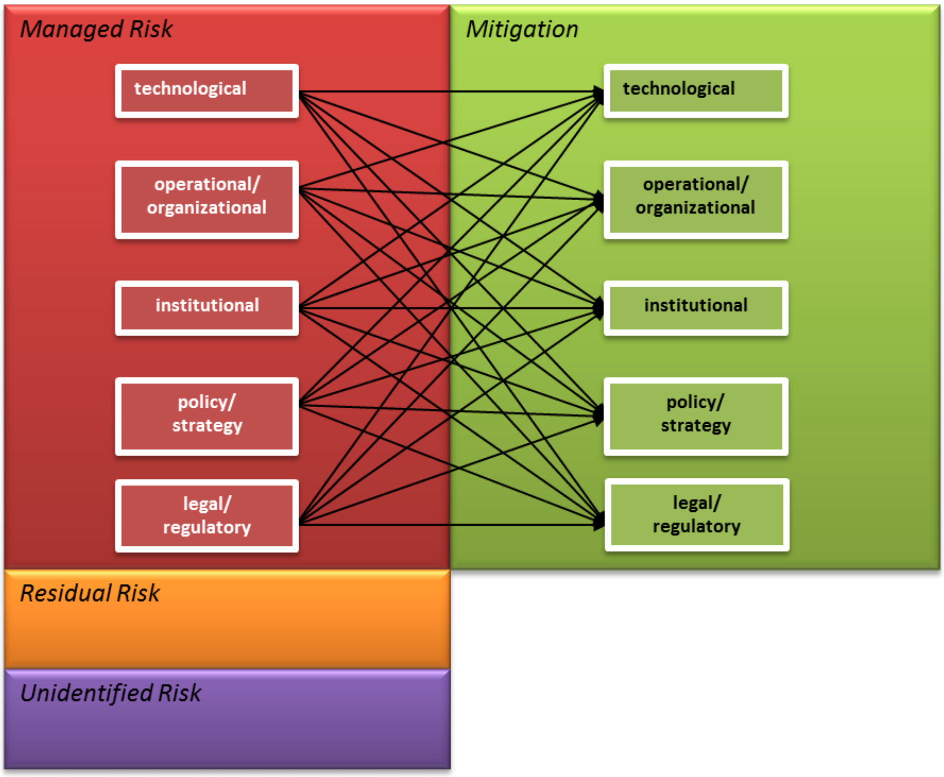


Figure 2 – risk assessment framework

Source: Bodea, G. in Deliverable 3.1, sub-deliverable PIA, FP7 Virtuoso

For the present Instant Mobility PIA we only look at some of the technological, institutional and organizational risks; risks originating in government policy and the legal framework are here out of scope.

In this report we describe the application of a PIA approach to assess privacy issues involved in Instant Mobility applications. In our PIA approach, we took the following steps:

1. analysis of scenario described in FP7 Instant Mobility project (2012) Deliverable 3.3 "WP3.3 – Instant Mobility Use Case scenarios definition & analysis – final report", personal travel companion scenario (p. 15 – 59), as a typical use-case for Instant Mobility applications;
2. analysis of the roles and information flows in the scenario, identification of roles that are handling personal information;
3. a privacy risk assessment and inventory of means to avoid or mitigate the risks.

3.1.6 Scope of the PIA

Privacy issues may exist for many different individuals in an instant mobility application, including risks that exist for e.g. the employee administration in the organizations making up an instant mobility application. However, the Instant Mobility PIA is limited in scope to the privacy of the end-user of instant mobility applications.

In scope is: information about a traveller (i.e. a traveller's personal information), and roles that require handling personal information of a traveller. Out of scope is: information that is not about a traveller, and roles that do not require handling personal information of a traveller.

3.2 Personal Travel Companion scenario

Smart mobility is a broad concept that covers many different kinds of applications. In Instant Mobility Deliverable 3.3, a set of three scenarios has been described in which different types of Instant Mobility applications are conceptualized. The three scenarios are:

4. Personal Travel Companion: demonstrates the capabilities provided by the future Internet technologies for multi-modal travel, mainly in urban and inter-urban areas.
5. Smart City Logistics Operations: describes how transport operations can be improved with respect to safety, efficiency, environmental performance and quality of service.
6. Transport Infrastructure as a Service: a study of the conditions needed for dynamic traffic & integrated urban space management, on how to use Future Internet technologies such as cloud data storage, Cloud computing virtualization or services-in-the-cloud.[17]

While privacy issues may be present in all three scenarios, the Personal Travel Companion scenario appears to be the most privacy-sensitive, as it puts a personal device (a “Companion”) in the centre, that, in order to provide its services, collects personal information about its user (e.g. his or her location) and communicates this with other devices and other parties.

Because of this, we take the Personal Travel Companion scenario described in Instant Mobility Deliverable 3.3 as the basis for the present Privacy Impact Assessment. After assessing this scenario, we discuss briefly key similarities and differences with the other two scenarios. To make a PIA possible, we have to expand the technically oriented scenario definition with roles which would be required in an operational setting, e.g. an Instant Mobility Provider that would be needed to operate the multi-model planning service and application for the traveller. These roles allow us to define the purposes, activities and responsibilities related to each role.

Also, two additional roles that are typically relevant from a privacy perspective were added, namely marketing and public authorities. Organizations in these two roles are typically interested in information about the behaviour of individuals and will likely be involved in some way in an operational setting.

3.2.1 Roles and Information Demands

The following roles were identified:

Role	Description
Traveller	Needs to travel from one location to another. Carries a mobile device (typically a smart phone) with an application offered by the Instant Mobility Provider.
Shared Vehicle Driver	May be a taxi driver or a traveller that drives a vehicle and shares vehicle capacity with other travellers on common parts of the route.
Public Transport Operator	Provides means of public transportation for travellers.
Public Transport Driver	Drives a public transportation vehicle that may transport travellers.
Instant Mobility Provider	Offers multi-modal planning service and application to travellers. Interacts with public transport operators and shared vehicle drivers in order to plan a journey for a traveller.
Marketing	May be interested in information about traveller behaviour for targeted

[17] As described in chapter 3 of Instant Mobility FP7 project, 2012, Deliverable 3.3 – Instant Mobility Use Case scenarios definition & analysis

	advertising / marketing.
Public Authority	May be interested in information about traveller behaviour for police surveillance or other purposes for the public interest (e.g. “mobility tax collection”).

Each role requires certain information about the traveller to perform its tasks:

Role	Information demand
Traveller (Instant Mobility Application on mobile device)	- Log-in credentials - Real-time position - Current journey plan(s) - Position expected according to plan - Origin - Destination - Start and arrival time - Virtual tickets - Mobile wallet - Ranking of the service (ride sharer, mean of transport) - Preferences (preferred mode of transport, language, etc.)
Shared Vehicle Driver	- (Pseudo-)identification - Common ride origin and destination (pick-up and drop-off points) - Common ride start and end time (when to pick-up or drop-off) - Common ride rate (i.e. price paid by traveller) - Real-time position reported by vehicle OBU
Public Transport Operator	- Virtual ticket: - (Pseudo-)identification - Trajectory origin and destination - Trajectory start and end time (if required by transport)
Public Transport Driver	- Virtual ticket: - (Pseudo-)identification - Trajectory origin and destination - Trajectory start and end time (if required by transport) - Real-time position of public transportation
Instant Mobility Provider	- Name, address, billing information - Log-in credentials - Travel preferences - Real-time position reported by traveller device - Current journey plan(s) - Position expected according to plan

	- Origin - Destination - Start and arrival time - Virtual tickets - Journey history - Journey satisfaction ratings - Billing history
Marketing	Behavioural profiles: - (Pseudo-) identification - Real-time position, expected position - Journey plans - Journey history - Journey satisfaction ratings - Travel preferences
Public Authority	Behavioural profiles. Detailed behavioural information about specific, identified, individuals. - Identification - Real-time position, expected position - Journey plans - Journey history

It is worth noting that continuous location information may be very sensitive information as it may reveal many details about an individual. Not only can that be construed as tracking and tracing; also, it can reveal other potentially sensitive data (medical conditions may be inferred from visits to the doctor; religious beliefs may be inferred from visits to a church or mosque, etc.). Hence, an instant mobility provider should be very careful in handling and protecting this information.

3.2.2 Interfaces

In Figure 3, a simplified representation of the roles and the interfaces between them is given, based on the scenario description. Two roles that were not provide in the scenario description but that play a role in any realistic setting are marketing and public authorities. Marketing may be a role performed by an instant mobility provider (e.g. marketing the instant mobility application itself), or by a third party (e.g. wanting to advertise based on a user's location). Public authorities may be interested in location information for criminal investigations, traffic safety or other purposes. Note that this schematic does not imply what *should* be shared in an Instant Mobility application, it is merely a sketch of what *could* be shared and with whom in a fictional setting. Different roles may be performed by the same organization (e.g. Instant Mobility Provider and Marketing).

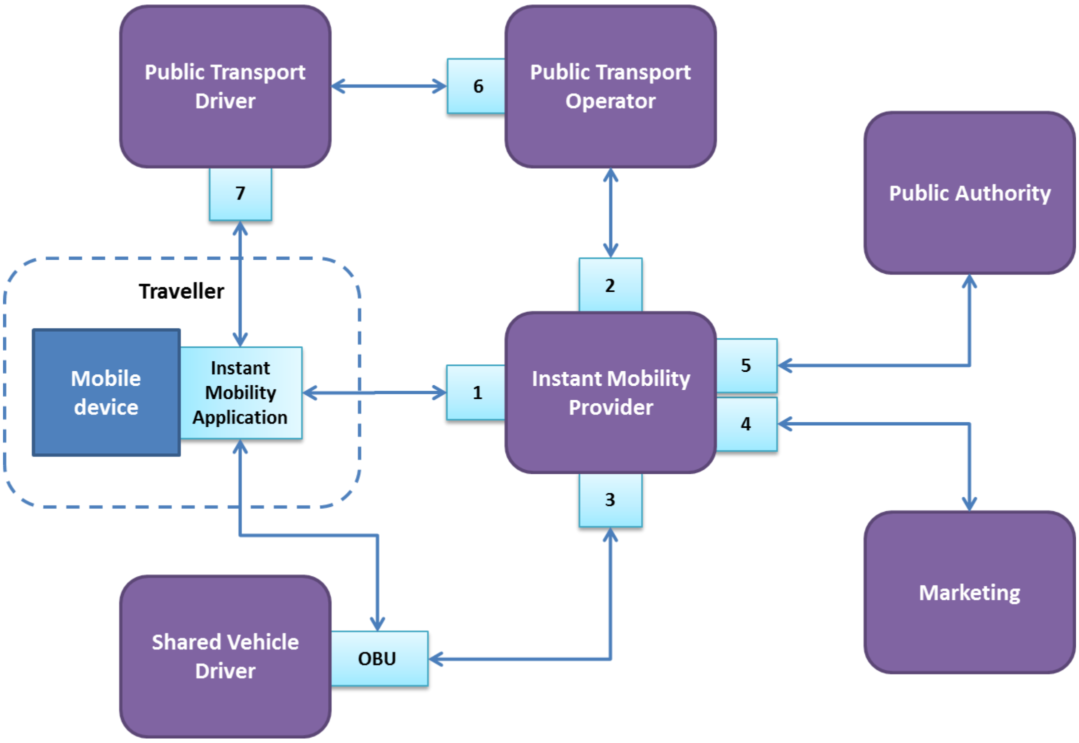


Figure 3 – roles and interfaces for exchanging personal information

A number of possible interfaces between the different roles can be identified (numbered according to the schematic above):

1. The Instant Mobility Provider (IMP) is the main point of contact for the traveller, through an Instant Mobility Application (IMA) on her or his mobile device. The IMP provides a contact point, e.g. through a (mobile) internet connection, for the application to connect to. The IMA also sends regular position updates to the IMP.
2. The Public Transport Operator (PTO) allows an IMP to request timetables (e.g. a bus route schedule and availability) and to book virtual tickets (e.g. a seat on a bus).
3. The On Board Unit (OBU) of a Shared Vehicle Driver (SVD) provides real-time updates of the vehicle's position and communicates with the IMP to arrange common rides with travellers.
4. The IMP provides behavioural profiles and real time location to marketing to allow for targeted advertising, e.g. for alternative means of private or public transport, etc.
5. The IMP provides behavioural profiles, journey plans and real-time updates to public authorities after a (legally valid) request, e.g. for tracking suspects.

6. PTO provides an interface for Public Transport Drivers (PTD) to validate virtual tickets of travellers.
7. PTD's can interface with a traveller's IMA to validate virtual tickets.

3.2.3 Other scenarios

The other two scenarios described in Deliverable 3.3 are Smart City Logistics Operations and Transport Infrastructure as a Service. We briefly discuss key differences and similarities with regards to flows of personal data between these two scenarios and the Personal Travel Companion scenario.

The Smart City Logistics Operations scenario does not focus on the mobility of individuals, but rather on the transportation of goods. Because of this, this scenario is very different with regards to its privacy impact: information about movements is collected primarily about goods, not individuals. In that, the security issues will prevail and different types of privacy will need to be addressed, in this case specifically employees' privacy.

The Transport Infrastructure as a Service scenario is different still from both the Personal Travel Companion scenario and the Smart City Logistics scenario. While the Transport Infrastructure as a Service scenario does not centre around a single individual, it does involve large-scale monitoring of traffic movements and collecting and processing this information, possibly through the use of cloud-computing approaches. This scenario approaches the same problem as the Personal Travel Companion scenario, but from a different angle: that of the overarching system and not of the individual's personal device. Because of this, we expect that the privacy issues involved in an Instant Mobility platform will become visible by assessing one of the scenarios.

3.2.4 User needs survey

Scenario 1 users : Travel Companion

The Instant Mobility project has decided to involved citizens in the design of the services in order to study how Internet will improve their urban mobility. To this end, Instant Mobility has conducted a first survey of more than 6,500 people in the partner cities to know under what conditions their inhabitants are willing to take advantage of future services of Instant Mobility. This survey was conducted online in Rome (Italy), Nice (France), Trondheim (Norway) and Istanbul (Turkey).[18] We discuss the outcomes of this survey here to get a better idea of the user perspective with regards to Instant Mobility applications.

The survey results clearly showed that privacy is a major acceptability issue for Instant Mobility applications. When asked "would you be willing to accept the transmission of your location during your daily travels in this new system?", between 8% to 10% refused this outright under any condition, and between 60% and 66% would only allow this under some conditions.

The conditions under which they would allow this are shown in Figure 4.

[18] Instant Mobility Deliverable 6.1 - Multimodal services acceptability report (month 12 update)

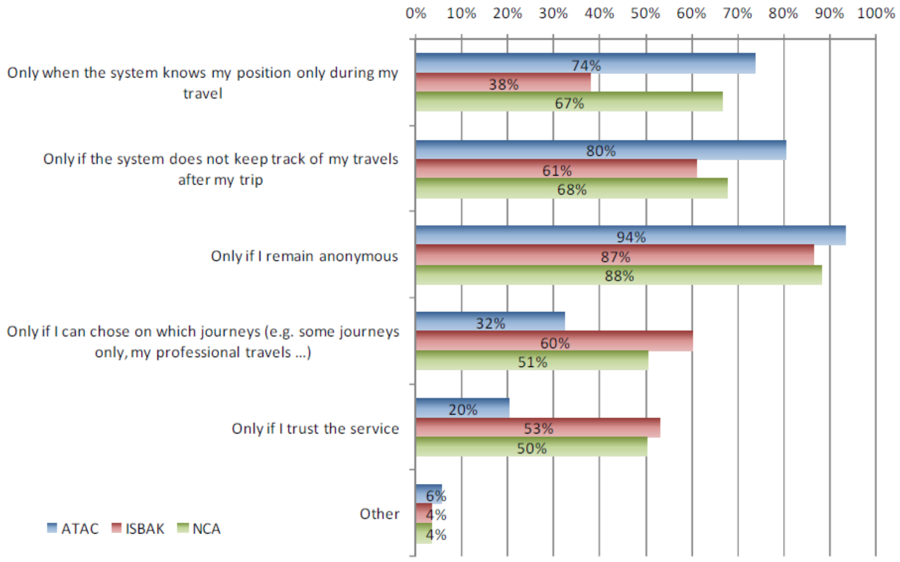


Figure 4 – conditions under which users indicate they will accept transmission of location data

The main condition for acceptance here appears to be that users want to remain anonymous (between 68% and 89% of respondents choose this option). Other important conditions are a high degree of control over when location data is transmitted, and that the system should “forget” about a trip after it has been completed.

Scenario 2 users : professional drivers

According to the professional target survey (see D6.4 *Instant Mobility Multimodal services acceptability final report*), the acceptance of real time location for the professional drivers, eco driving and sharing data is mainly:

. To be guided for the most efficient route is an important acceptance factor, and also for Dutch respondents, to be able to “overrule the advised route and pick an alternative”

. Eco-optimized driving service: the main condition is to be in control and be able to overrule the service

. Sharing data (Dutch respondents):

- 24% may be prepared or is prepared (44%) to share location data for personal navigation.
- 71% of them are prepared to share location for a more efficient route planning.
- 21% are prepared to share location to share load with other companies. 49% are not prepared to share location data for this purpose.
- 34% are prepared to share location data to get advised about eco optimized driving. 40% are not prepared to share location data for this purpose.

The survey shows 3 groups of Dutch respondent types:

- **proponents**: would like to share data.
  Profile: larger fleet size company. Higher perceived usefulness of the services. Higher level of current use of navigation, planning and messaging functionality of fleet management system
- **doubters**: might want to share data.

- **opponents**: do not want to share.

Profile

- For both: smaller fleet size company
- For opponents: they judge the upcoming services less useful and less satisfying

The privacy design should take into account the different needs of users, let the user be proactive according to his acceptability level and use various mechanisms to preserve their privacy according to their need, context and cultural and technical background.

As Instant Mobility proposal is based on a new collaborative way of travelling, the social networks are a key lever as identified in Deliverable D6.6 *Instant Mobility Data Business cases Final report*: as observed by an English report from TRL[19], the networks must be built with “closed” communities (because of preferences of respondents to get information from friends and family).

For contextualization to be accepted, the users will clearly need to see what is the clear benefits for them and if the user privacy is respected.

The privacy policy for Instant Mobility applications could be:

- **All the personal data** that are used by the applications are displayed clearly to the user (allow transparence) and are managed in a secured way (trustworthy and secure tools);
- For **each** personal data type used, the application must easily:
  - Ask the traveler to give his explicit consent (and consent opt in stays available during the life of the data) for real time use and storage use;
  - Give opportunity to the traveler to withdraw his consent;
  - Let the traveler be able to manage the data (correct it) at any time;
  - Explain the purpose of the collect of the data and who is using it;
  - Take the explicit consent if the data is transmitted to a third party (advertiser for instance);
  - Identify the type of information that is being shared and whom users are sharing this information with;
  - Give the traveler an easy way to access to his personal data.

A dashboard could be designed to allow the user to access easily the privacy policy and manage their personal information.

So, the private policy may be different for the user according to his case or context (for instance he could agree to give anonymous location when travelling in public transports and non anonymous location when ride sharing –but pseudonym instead of name).

3.3 Impact when incident occurs

Privacy incidents can have negative results for the traveller. Here we discuss a number of different kinds of impacts, which are often not directly related to specific risks. Instead, different risks may cause the same impact, or one incident may have different impacts.

[19] Binsted A, Hutchins R, 2012, The role of social networking sites in changing travel behaviours, TRL Published project Report: http://www.trl.co.uk/online_store/reports_publications/trl_reports/cat_traffic_and_the_environment/report_the_role_of_social_networking_sites_in_changing_travel_behaviours.htm

Database leak – location data about travellers is leaked to the public because of either a technical or human error. The impact of such an incident may be either very low, when only little data about few individuals is leaked, or high when a lot of data about a large number of individuals are leaked. A database leak is unlikely to continue over long periods of time, which at least limits the possible negative impact in time.

Criminal activity enabled by real-time location data about travellers. For example, a criminal might want to know when an occupant of a home is away to plan a break-in, or real-time location information may be used to rob or otherwise harm a traveller when he or she is in a vulnerable location. For this purpose, real-time location information is much more valuable to a criminal than stored location information over a longer period of time (although this may be used to infer patterns of behaviour).

Criminal activity enabled by identity fraud. A criminal may assume the (digital) identity of a traveller to travel on the travellers' expense, or to implicate an innocent traveller in a criminal activity (by implying that the traveller was at the location of a crime).

Use of personal data for other purposes than agreed upon by the traveller and the instant mobility provider. An example is the use of location information for unsolicited marketing of location-based products or services (e.g. nearby restaurants). While in most cases the impact of such secondary use will be limited for the traveller (e.g. discomfort, a feeling of being followed), it can be in breach of current legislation and in some EU countries may result in fines for the Instant Mobility Provider.

Surveillance with no legal basis. Public authorities may be interested in real-time or stored location information to perform surveillance or to support criminal investigations, without having a sufficient legal basis for requesting this information. Alternatively, an instant mobility provider may decide to work together with public transport operators to use real-time location information to detect whether an individual is travelling without paying the travel fee.

Retaining personal information after it is necessary for the instant mobility service. The service providers should destroy personal data when they are no longer necessary for providing the service for which they was collected and no legal obligation exist to retain them longer. While violating this principle may not directly have an impact for the traveller, it may have negative effects on the long term as it increases the risk in case of a database leak or of use of data for other purposes than agreed upon.

Inability of travellers to amend or correct personal information. An instant mobility provider or other party in an Instant Mobility service may corrupt personal data about the traveller either through human or technical error. If the traveller has no means or easily accessible procedures for correcting such errors, this may result in a highly negative impact for the traveller, for example billing based on incorrect journey plans or virtual tickets.

3.4 Risk of incident occurring

In some risk assessments it is feasible to more or less rank if not quantify the impacts and risks. However, since the present privacy impact assessment is based on a hypothetical scenario, this is not possible here. Instead, we will indicate whenever we think a risk deserves specific attention, either because the expected impact will be very high, or the chance of an incident occurring will be high.

Risk R1. Instant Mobility Provider provides travel data to marketing service providers without prior consent of data subject

An Instant Mobility Provider (IMP) may have a commercial interest in making location information of travellers available to its own marketing department, or selling the information to third parties. This enables, for example, location-based advertising (e.g. for restaurants near the traveller's location), or targeted marketing for transportation means based on travelling habits (e.g. advertisements for a taxi service on a trajectory the traveller may pass along). While this could provide a valuable service to the traveller and is permissible when he has given explicit consent, a risk exists that an Instant Mobility Provider may overlook the need to ask the traveller permission for this, or may choose not to ask permission.

The chance for such a risk occurring depends largely on the privacy awareness within the IMP organization, and on the processes and organizational safeguards that prevent this from happening without consideration for implications to privacy.

Risk R2. Instant Mobility Provider provides travel information to public authority without legal basis

Public authorities may be interested in (real-time or historical) location information, either to track potential suspects or to assist in criminal investigations. This may be permissible when a legal basis exist and the right procedures are followed, but a risk exists that an Instant Mobility Provider may receive a request for location information that does not have a sufficient legal basis or in which the right procedures were not followed. If such an incident occurs, it may have a negative impact on the privacy of travellers, and may cause an image of an Instant Mobility Provider as an extension to public authority surveillance to arise.

The chance for such a risk occurring depends largely on the privacy awareness within the IMP organization, and on the processes and organizational safeguards that prevent this from happening without consideration for the legal basis for such requests.

Risk R3. Instant Mobility Provider "leaks" personal information via internet

Technical information security failures or human error (e.g. in configuration of servers or websites) may cause an unintended leak of travel information or other personal data through the internet. The impact of such a leak can depend on how detailed the leaked information is and about how many individuals it is (e.g. a leak of detailed location information over a long period for only a few individuals may have a high impact, or a leak of a database filled with travel information of many individuals may have a very high impact).

The chance for such a risk occurring depends largely on the technical security safeguards that were taken, and on security processes and organizational safeguards that prevent this from happening.

Risk R4. *Travel information for billing gets corrupted in instant mobility application*

Either through technical or human error, or through intentional human manipulation, location, travel or other personal information may be corrupted. For example, an employee of the Instant Mobility Provider may erase certain billing information for a friend or family member (which is not necessarily a privacy issue). Another example is the wrongful attribution of travels, or the unauthorized change of personal details of a traveller by an employee with malign intent.

Risk R5. Travel information for billing gets corrupted in platforms connecting to IMP

Similar to the risk for Instant Mobility Providers, travel information may be corrupted in systems that connect to the IMP's systems either through technical or human error or intentional manipulation. Identifiers may be mixed up, and possibly travels accounted to the wrong individual, e.g. by the systems at the Public Transport Operator.

Risk R6. Shared vehicle driver OBU "leaks" personal data

If a vehicle driver has an On Board Unit (OBU) that enables the Instant Mobility application, this OBU may have technical flaws and "leak" location or travel information of both the shared vehicle driver and the traveller(s) sharing the vehicle. For example, the OBU wireless communication signals may be intercepted if insufficient encryption is used, or the signals it emits may be used to track the vehicle.

Risk R7. Processing of travel information / other personal data is outsourced without sufficient guarantee of correct handling of this information or without consent

Whilst in our simplified schematic in Figure 3 the Instant Mobility Provider is portrayed as a single unit, it may in a realistic setting consist of different organizations working together. For example, part of the information processing may be performed in cloud environments which may be partially located in different countries, such as the USA. Also, the IMP may choose to outsource the handling of certain personal information (e.g. for billing purposes) to a third party. A risk exists that the IMP shares this information with third parties (such as cloud computing providers or billing providers) without sufficient guarantees for the privacy of travellers, either through legal or technical means.

Risk R8. Personal data is used by IMP or other parties in the IM platform for purposes for which no consent was given

Apart from marketing or public authorities, an Instant Mobility Provider or another party in the instant mobility platform may choose to use personal data for new or significantly altered services, for which the traveller has not given consent. For example, use of location information for estimating traffic density may be a use of location data that was not originally imagined, but may turn out to be a useful application. However, the risk exists that a travellers location information is used for such a new purpose without adequately informing the traveller and acquiring his or her consent for this use.

Risk R9. Personal data are not destroyed after not being needed anymore for the purposes they were collected

Personal data are collected and used within the Instant Mobility platform for the purpose of enabling multimodal travel for the travellers using the platform. However, these personal data may be useful for other purposes long after it stopped being useful for enabling multimodal travel. Or, an Instant Mobility Provider may simply forget to erase the personal data when it is no longer used. In both cases, there is a continuing risk of personal data being misused.

Risk R10. A traveller is unable to correct his personal data, or to see what personal data are collected, stored and used by the IMP

Data protection laws require that a party that processes personal data, such as the Instant Mobility Provider, enables the data subjects to see what information is collected about them, and for what purpose. Also, if the data is incorrect, the data subjects should be able to request the necessary corrections. And generally, data subjects should be able to remove any of their data. A risk exists that an IMP does not implement adequate procedures to handle such cases, makes these procedures too complicated or expensive, or does not inform its users about how to follow these procedures.

3.5 Managing privacy risks

In a setting in which a new type of service is being designed and implemented, the **risk of use of personal data for purposes other than those to which the data subject had consented** (e.g. Risk R1 and Risk R8) is relatively high. In such a case the focus is likely to be more on adding new features and finding innovative uses of (personal) data. Hence, when implementing a new system such as the instant mobility application, checks must be put in place to ensure secondary use is permissible. A second risk that may arise in a complex and relatively new system and the organization offering it, such as an instant mobility provider, is **a lack of transparency and a lack of options for users of the**

system to get their personal data corrected or erased (Risk R10). The third main risk lies in **insufficient security for databases and web-based services**, which may result in large-scale leaks of personal information (Risk R3 or Risk R6). Considering the potentially large amount of personal data (e.g. detailed location data over longer periods of time) that may be stored, special care must be taken to avoid risks large-scale leaks.

3.5.1 Technical means

A good starting point when designing an instant mobility system that avoids these risks is to follow the principle of data minimization: collect and use as little personal information as possible to enable the service. For example, if for the mobility applications location data are only needed for certain modalities, or at a certain density (e.g. once every minute), the risks to privacy are reduced if only this information is collected, and not more. In addition to this, privacy risks may be reduced by making data anonymous where possible, or by using pseudonyms.[20]

Information security is a topic on its own and is discussed separately. However, for safeguarding the privacy of users of instant mobility applications, strong security is a strict requirement. For example, sufficiently strong encryption and other safeguards must be taken to ensure that communicated and stored data cannot be accessed by unauthorized (third) parties.

A technical means providing users with insight into what personal data are stored about them and how to correct possible mistakes is to provide them with a web-based interface. The web-based interface would allow users to see what personal data are stored about them, and for what purpose, etc. This may also include options to remove stored data (where possible), or request corrections or removal of data.

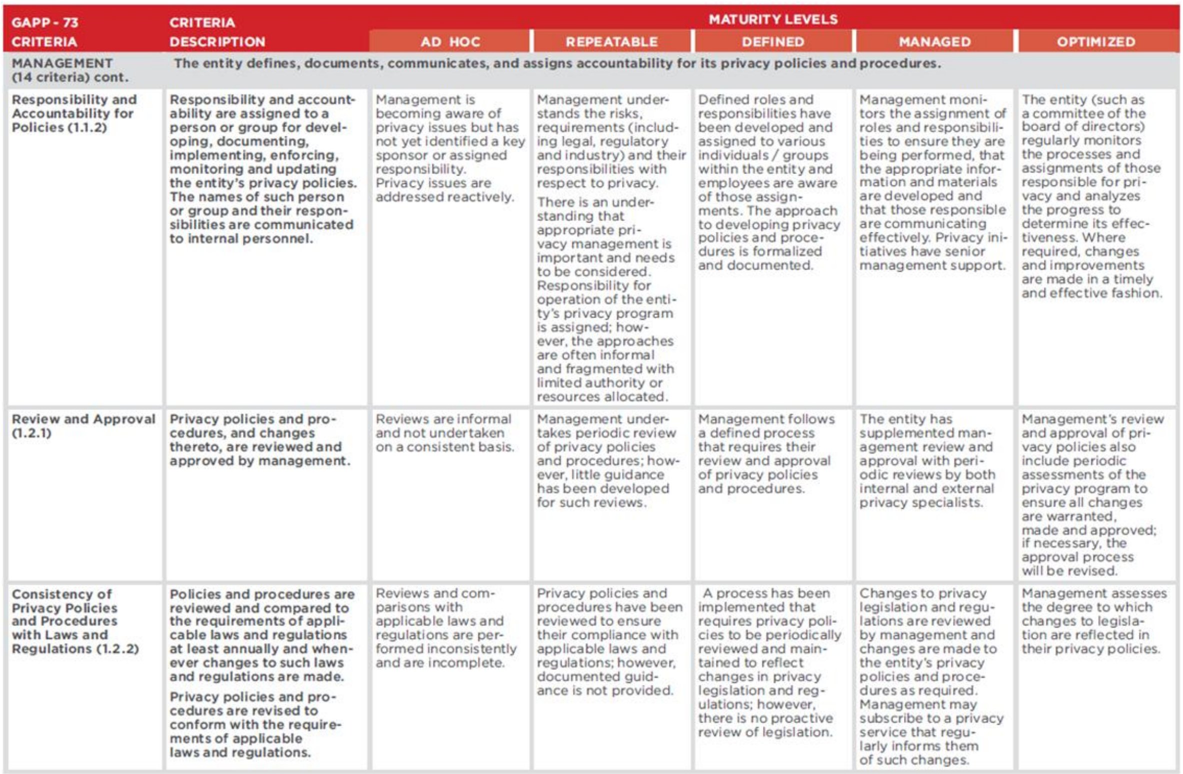
3.5.2 Organizational means

Complementary to the technical means that may be employed to avoid these privacy risks are a number of organizational means. First of all, this Privacy Impact Assessment is just a preliminary one at a very early stage. Many implementation details are still unknown, which is why the risk analysis is necessarily high-level, and lacks specifics. If an Instant Mobility application were to be implemented, a new and more detailed PIA should be performed during and supporting its design stage.

In addition to this, the organizations working together to enable the IM platform, and especially the Instant Mobility Provider as a central element should implement procedures and organizational checks to avoid secondary use of personal data. Procedures must be implemented to enable users to see what data about them are collected and for what purpose, and to enable users to correct errors in their data or to erase data. While standards and best practices with regards to organizational embedding of privacy safeguards are still in development, some guidance is available. One example is the Privacy Maturity Model released by the accountant organizations AICPA & CICA, which is based on the Capability Maturity Model (CMM) (see Figure 5).[21] While not every organization needs to achieve "Optimized" maturity level for every criterion, an organization such as an Instant Mobility Provider should at the least make a conscious decision on the maturity level towards which it strives.

[20] Recently the UK ICO released a best practice guide on anonymisation which may be useful to this end: Information Commissioners Office, 2012, Anonymisation: managing data protection risk code of practice. Available online at: http://www.ico.gov.uk/for_organisations/data_protection/topic_guides/anonymisation.aspx

[21] AICPA/CICA Privacy Maturity Model, Available online at: http://www.aicpa.org/privacy



GAPP - 73 CRITERIA	CRITERIA DESCRIPTION	MATURITY LEVELS				
		AD HOC	REPEATABLE	DEFINED	MANAGED	OPTIMIZED
MANAGEMENT (14 criteria) cont.	The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures.					
Responsibility and Accountability for Policies (1.1.2)	Responsibility and accountability are assigned to a person or group for developing, documenting, implementing, enforcing, monitoring and updating the entity's privacy policies. The names of such person or group and their responsibilities are communicated to internal personnel.	Management is becoming aware of privacy issues but has not yet identified a key sponsor or assigned responsibility. Privacy issues are addressed reactively.	Management understands the risks, requirements (including legal, regulatory and industry) and their responsibilities with respect to privacy. There is an understanding that appropriate privacy management is important and needs to be considered. Responsibility for operation of the entity's privacy program is assigned; however, the approaches are often informal and fragmented with limited authority or resources allocated.	Defined roles and responsibilities have been developed and assigned to various individuals / groups within the entity and employees are aware of those assignments. The approach to developing privacy policies and procedures is formalized and documented.	Management monitors the assignment of roles and responsibilities to ensure they are being performed, that the appropriate information and materials are developed and that those responsible are communicating effectively. Privacy initiatives have senior management support.	The entity (such as a committee of the board of directors) regularly monitors the processes and assignments of those responsible for privacy and analyzes the progress to determine its effectiveness. Where required, changes and improvements are made in a timely and effective fashion.
Review and Approval (1.2.1)	Privacy policies and procedures, and changes thereto, are reviewed and approved by management.	Reviews are informal and not undertaken on a consistent basis.	Management undertakes periodic review of privacy policies and procedures; however, little guidance has been developed for such reviews.	Management follows a defined process that requires their review and approval of privacy policies and procedures.	The entity has supplemented management review and approval with periodic reviews by both internal and external privacy specialists.	Management's review and approval of privacy policies also include periodic assessments of the privacy program to ensure all changes are warranted, made and approved; if necessary, the approval process will be revised.
Consistency of Privacy Policies and Procedures with Laws and Regulations (1.2.2)	Policies and procedures are reviewed and compared to the requirements of applicable laws and regulations at least annually and whenever changes to such laws and regulations are made. Privacy policies and procedures are revised to conform with the requirements of applicable laws and regulations.	Reviews and comparisons with applicable laws and regulations are performed inconsistently and are incomplete.	Privacy policies and procedures have been reviewed to ensure their compliance with applicable laws and regulations; however, documented guidance is not provided.	A process has been implemented that requires privacy policies to be periodically reviewed and maintained to reflect changes in privacy legislation and regulations; however, there is no proactive review of legislation.	Changes to privacy legislation and regulations are reviewed by management and changes are made to the entity's privacy policies and procedures as required. Management may subscribe to a privacy service that regularly informs them of such changes.	Management assesses the degree to which changes to legislation are reflected in their privacy policies.

Figure 5 – A small part of the Privacy Maturity Model

A key part of the organizational aspect of privacy protection is the awareness that employees in an organization have on privacy issues.

3.6 Conclusion

The Instant Mobility concept is still at an early stage. Even though many implementation details are still unclear, the scenario descriptions give an indication of what an Instant Mobility application may look like which allows us to assess some of the privacy risks involved, and the means that are available to mitigate these risks.

Three main categories of potential risks were identified at this early stage:

- the use of personal data for purposes other than which the data subject has given consent, for example the use for surveillance, trade of personal information or unsolicited marketing;
- a lack of transparency, and a lack of options for users of the system to get their personal data corrected or erased; and
- insufficient security for databases and web-based services.

Such risks may be mitigated or avoided by the use of a combination of technical and organizational means. Technical means may include anonymisation or the use of pseudonyms, data minimization, encryption and other information security means, and providing users with an accessible web interface in which they can overview and correct their personal data. Organizational means centre around raising privacy awareness within the organization behind the Instant Mobility Platform and implementing checks and procedures that could help identify and avoid privacy-invasive decisions.

Most importantly, extensive attention should be paid to the privacy aspects of an Instant Mobility application, were it to reach a concrete design and implementation stage. During the design phase of an actual application, a more detailed Privacy Impact Assessment should be performed in close cooperation with the main design, to identify specific privacy risks and think of means to avoid or mitigate these.

4. Conclusions and recommendations

The security impact assessment identified three critical risks related to:

- Unauthorized disclosure of personal data
- Errors in invoicing
- Failure of visualization services

Three high risks related to:

- Inaccessibility of the journey monitoring
- The lack of trust in the authentication service
- Inaccessibility of Enrollment service

And three medium risks related to:

- Inaccessibility of the route determination
- Unavailability of travel data
- An inappropriate assessment of traffic

Technical and organizational security measures proposed (§ 2.5 Security Recommendations) aim establishing a defense in depth to reduce and transfer risks.

The privacy impact assessment identified three main risks that are visible in this early stage of development of Instant Mobility applications:

- the use of personal data for purposes other than which the data subject has given consent, for example the use for surveillance, trade of personal information or unsolicited marketing;
- a lack of transparency, and a lack of options for users of the system to get their personal data corrected or erased; and
- insufficient security for databases and web-based services. The importance of security of personal data underlines the conclusions from the security risk assessment.

Privacy risks may be mitigated or avoided by the use of a combination of technical and organizational means. Technical means include anonymisation and the use of pseudonyms, data minimization, encryption and other information security means, and providing users with an accessible web interface in which they can overview and correct their personal information. Organizational means centre around raising privacy awareness within the organization behind the Instant Mobility Platform and implementing checks and procedures that help identify and avoid decisions that harm privacy.

From both security and privacy point of view, the Instant Mobility concept is still in an early stage, and it is not yet possible to identify risks that arise from specific implementation details that will become known in later stages of development of Instant Mobility applications. A key recommendation is to perform a more detailed security risk assessment and a privacy impact assessment when a specific implementation design is being created. Doing this early in the design phase will help avoid risks that may be very difficult to correct later on.

5. REFERENCES

1. Bodea, G., Lieshout, M. van, Kool, L., Deliverable 3.1 PIA, FP7 Virtuoso, 2011
2. Instant Mobility Grant Agreement Annex I - "Description of Work"
3. Instant Mobility FP7 project, 2012, Deliverable 3.3 – Instant Mobility Use Case scenarios definition & analysis, chapter 3
4. Warren, S. D., & Brandeis, L. D. (1890). Right to Privacy. (K. Ziegler, Ed.) Harvard Law Review, 4(1), 72.
5. Westin, A. F. (1967). Privacy and Freedom. Atheneum.
6. Solove, D.J. (2008). Understanding Privacy. Harvard University Press.
7. Rachel L. Finn, David Wright, and Michael Friedewald. "Seven Types of Privacy" *European Data Protection: Coming of Age*. Ed. S. Gutwirth et al.. Dordrecht: Springer Science+Business Media, 2013.
8. Ware, W. W. (1973) Records, Computers and the Rights of Citizens. United States: U.S. Department of Health, Education and Welfare. Read more on the FIPs online at: http://www.ftc.gov/reports/privacy3/fairinfo.shtm
9. Koorn, R., Gils, H. van, Hart, J. ter, Overbeek, P., & Tellegen, R. (2004). Privacy-Enhancing Technologies: White Paper for Decision-Makers. The Hague.
10. Lieshout, M. van, Kool, L., Schoonhoven, B. van, & Jonge, M. de (2011). Privacy by Design: an alternative to existing practice in safeguarding privacy. Info, 13(6), 55–68.
11. Cavoukian, A. (2009). Privacy by Design - The 7 Foundational Principles. Toronto, Ontario.
12. Rubinstein, I., & Good, N. (2012). Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents. New York.
13. Nissenbaum, H. (2010). Privacy in Context: Technology, Policy, and the Integrity of Social Life. Palo Alto, CA: Stanford University Press.
14. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data
15. Linden Consulting, 2007, Privacy Impact Assessments: International Study of their Application and Effects
16. UK ICO Privacy Impact Assessment Handbook, available online at: http://www.ico.gov.uk/pia_handbook_html_v2/files/PIAhandbookV2.pdf
17. Instant Mobility Deliverable 6.1 - Multimodal services acceptability report (month 12 update)
18. Information Commissioners Office, 2012, Anonymisation: managing data protection risk code of practice. Available online at: http://www.ico.gov.uk/for_organisations/data_protection/topic_guides/anonymisation.aspx
19. AICPA/CICA Privacy Maturity Model, Available online at: http://www.aicpa.org/privacy