SECUR-ED
SECured URban transportation - European Demonstration

D46.6 Consolidation of societal and ethical impacts

Public document

Document identification	
Related SP / WP	WP54
Related Deliverable	
Lead Participant	FOI
Contributors	Brita Gjerstad (STA), Gottfried Heinzerling (STA), Karl Wesslau (FOI) Anders Eriksson (FOI), Christian Carling (FOI)

Reference	SCR-WP46-D-FOI-002
Dissemination Level	PU
Lead Author	Brita Gjerstad (STA)
Reviewers	Ron Iphofen (AG Ethical)

This document is issued in the frame and for the purpose of SECUR-ED project. This project has received funding from the European Union's Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 261605.

History

NB: a **status** is associated to each step of the document lifecycle:

- **Draft**: this version is under development by one or several partner(s);
- **Under review:** this version has been sent for review;
- **Issued**: this version of the document has been submitted to EC.

Version	Status	Date	Author	Main Changes
0.1	Draft	April 22	FOI STA	Draft
0.2	Draft	May 9	FOI	Implementing suggestions from Advisory group Ethics
0.3	Draft	June 6	FOI STA	Draft completion
0.4	Draft	June 12	FOI	Draft finalisation for review
0.5	Under review	June 13	FOI	Sent to peer review
0.6	Under review	June 27	FOI	Sent to coordinator
0.7	Under review	July 4	FOI	Sent to coordinator
1.0	Issued	July 4	FOI	Version submitted to the commission

TABLE OF CONTENTS

1 Abstract

This report documents considerations of the ethical, societal and privacy aspects of functions, systems and processes tested in SECUR-ED. The main analytic thread consists of bundling functions tested in demonstrations into problem areas which are then assessed in terms of key societal/ethical issues. While this analysis is firmly based on the demos as conducted, its purpose is to draw generic policy relevant conclusions, not to comment on the conduct of specific demos. Big Data and tracking of individuals are the problem areas particularly highlighted in the analysis. The report also contains background information on the demos as well as other types of analyses of the SECUR-ED demonstrations with regard to ethical, societal and privacy aspects. This includes a tentative suggestion for best practice for ethical and societal aspects in future large-scale experimentation and demonstration projects.

2 References

2.1 List of acronyms

CBRNE	Chemical, Biological, Radioactive, Nuclear and Explosive
CC	Control Centre
CCTV	Closed-circuit Television
DoW	Description of Work
EOP	Emergency Operating Procedure
ICT	Information and Communication Technologies
OCC	Operational Control Centre
PIS	Passenger Information System
PT	Public Transport
PTA	Public Transport Authority
PTO	Public Transport Operator
PTZ	Pan Tilt Zoom
QR	Quick Response
R	Radioactive
RFID	Radio-Frequency Identification
SOCC	Security Operational Control Centre
SOP	Standard Operating Procedure
WP	Work Package

2.2 Referenced documents

The following SECUR-ED documents are referenced:

D01.6 Ethical Management Report (Period 1)

D01.8 Ethical Management report (Period 2)

D11.2 Measures to Improve Security and Privacy

D35.2 AG Ethical Review of Privacy and Ethical Matters.

D42.1 Detailed description for Madrid demo

D43.1 Detailed Scenarios for Paris Demonstration

D44.5 Consolidated results for Milan demonstration

D45.5 Experimentation report for Berlin demonstration

D54.3 Improve the risk reduction system

The following other documents are referenced:

Burgess, J. P. (2008). Security After Privacy: The Transformation of Personal Data in the Age of Terror. I P. I. P. R. Institute (red.), Policy Brief. Oslo: PRIO International Peace Research Institute.

Clarke, R. (2006). 'What's Privacy?' Retrieved 08.01.09 from http//:www.anu.edu.au/people/Roger.Clarke/DV/Privacy.html.

Crime Concern 1997; 2004

EU Directive 95/46/EC - The Data Protection Directive

Gilbert, Richard et. alt., Transport revolutions – moving people and freight without oil, London 2008.

Greenleaf, G. 2008. Function Creep – Defined and still dangerous in Australia's revised ID Card Bill, Computer Law & Security Report 24

Hamilton and Jenkins 2000, referred in Yanuz and Welch 2010

Hessler, R.M. and K. Freerks (1995) Privacy ethics in the age of disclosure: Sweden and America compared. The American Sociologist, 26: 35-53

Iphofen, R. (2014) Ethical issues in surveillance and privacy (Ch. 4 in Alex Stedmon & Glyn Lawson (Eds.) *Counter-terrorism & Hostile Intent: Human Factors Theory and Application*, London: Ashgate (forthcoming)

Iveson, K. (1998) Putting the public back into public space. Urban Policy and Research, 16, 21-33

Johansen et al. 2001. Personopplysningsloven. Kommentarutgave. Universitetsforlaget, Oslo.

Kumaraguru, P. and L. F. Cranor (2005). Privacy Indexes: A Survey of Westin's Studies. CMU-ISRI. I. o. S. R. International, Institute of Software Research International, Carnegie Mellon University: 1-22.

Lace, S (ed.) 2005. The Glass Consumer: Life in a Surveillance Society. Polity Press

Leino-Kilpi, H., Välimäki, M., Dassen, T., Gasull, M., Lemonidou, C., Scott, A. (2001). Privacy: a review of the literature. International Journal of Nursing Studies, 38, 663-671.

Lomell, H. M. 2004. Targeting the Unwanted: Video Surveillance and Categorical Exclusion in Oslo, Norway. Surveillance & Society 2(2/3)

Lynch and Atkins, 1988, ref, in Yanuz and Welch 2010).

Norris, C and Armstrong G 1999: The maximum surveillance society: the rise of CCTV. Oxford, Berg

O'Hara, K. and N. Shadbolt (2008). The spy in the coffee machine. The end of privacy as we know it. Oxford, Oneworld Publications.

Olivero, N. and P. Lunt (2004). 'Privacy versus willingness to disclose in e-commerce exchanges: The effect of risk awareness on the relative role of trust and control.' Journal of Economic Psychology 25: 243-262.

Owens, P. 1999, No teens allowed: The exclusion of adolescents from public spaces,

paper presented at Living At The Edge - Youth and Social Exclusion Conference, University of Strathclyde, U.K

Raguse, M., M. Meints, O. Langfeldt and W. Peissl 2008. PASR Preparatory Action on the enhancement of the European industrial potential in the field of Security research. In PRISE privacy security

Schartum, D. W and L.A Bygrave 2004. Personvern i informasjonssamfunnet: en innføring i vern av personopplysninger. Bergen, Fagbokforlaget.

Shoeman, D.F. 1992 Privacy and social freedom. Cambridge University Press

Solove, D. 2007. 'I've Got Nothing to Hide' and Other Misunderstandings of Privacy. GW Law Faculty Publications & Other Works. George Washington University Law School

Sætnan. A. R., H.M. Lomell, C. Wieck 2004. Controlling CCTV in Public Spaces: Is Privacy the (Only) Issue? Reflections on Norwegians and Danish Observations. Surveillance & Society 2(2/3)

Tonnelat, S. 2010 The sociology of urban public spaces. Proceedings of the first Sino French Urban Planning Conference

Ustaran, E. 2013:

https://www.privacyassociation.org/privacy_perspectives/post/yes_consent_is_dead._further_continuing_to_give_it_a_central_role_is_danger

Walsh 1999, referred in Yavuz and Welch 2010

Whitman, J. Q. 2004 The Two Western Cultures of Privacy: Dignity versus Liberty. Yale Law School Legal Scholarship Repository, Faculty Scholarship Series, Yale Law School

Wilson, J.Q. and G. L. Kelling (1982) Broken Windows. The police and neighborhood safety. Atlantic Monthly (March), pp. 29-38.

Yavuz, N. and E. W. Welch (2010). Addressing Fear of Crime in Public space: Gender Differences in Reaction to Safety Measures in Train Transit. Urban Studies 2010 (12)

3 Introduction

This report consolidates findings regarding the ethical, societal and privacy aspects of tools, systems and processes tested in SECUR-ED. SECUR-ED is a demonstration project, whose aim is to improve urban transport security in mass transit settings. The project provides a consistent, interoperable mix of technologies and processes, covering all aspects from risk assessment to complete training packages and technologies (www.secur-ed.eu). The demonstrations and their results are documented in a number of reports. These reports have focused on functionalities, performance, flexibility, maturity and so on. In this report those questions are put aside and instead the focus is on ethical, societal and privacy aspects.

Many actors consider privacy, societal and ethical aspects highly relevant. The reasons for this are many. Concerns include misuse of data and the fear of unintended consequences in the future. Another point raised is the need for discussions about how to deal with dilemmas rising from conflicting needs. All of these issues can be seen as reasons for considering privacy, societal and ethical aspects when working with security in public transport. Several security systems register and store large amounts of passengers' personal data, of which much is of interest to other actors. Furthermore, there is little knowledge of the long-term consequences of these security systems, nor is it clear how the need for security should be balanced against the need for privacy in open spaces.

As a result, these issues emerge both in industry, politics and academia. Politicians (and others) discuss the Directive on privacy and electronic communications, in industry there is the concept of 'Privacy by design', and academics offer empirical and theoretical studies through which they discuss experienced and potential implications of security capacities. In some cases the focus is exclusively on privacy, society and ethics; in other cases these topics are dealt with as aspects of other issues. The latter is the case in SECUR-ED. As already stated, SECUR-ED's aim is to improve security in urban transport. Naturally, its main questions are therefore about security, such as whether the capacities have the intended effects and if they, alone or together, contribute to increased security. Such questions are at the core of the project. Questions about privacy, societal and ethical aspects can be seen as additional. However this does not mean that they are less relevant or not necessary to consider. They are. Nor does it mean that they have not been dealt with in the project. They have. This being said, privacy, societal and ethical aspects are not at the core of the project, nor is the project designed with those aspects in mind. SECUR-ED's overall design thus put some restraints on the consolidation of privacy, societal and ethical issues.

3.1 The task of this deliverable

According to SECUR-ED's Description of Work (DoW) the present report 'will consider the social aspect related to the use of the technologies, system, procedure tested during the demonstration experiments:

- respect/possible impact on human right[s]
- privacy issues
- impact of solution on social context
- impact of solution on use of mass transit systems'

The DoW also identifies the need for a strong relationship with the project's ethical and societal advisory group.

The aim of this deliverable is not to review the individual demos but to consolidate the experience gained from them for extending the understanding of emerging social/ethical issues in mass transport. Even though the demos took place in certain regions, the conclusion to be drawn in this report should have global or at least pan-European relevance.

Societal and ethical issues represent a broad area of concern, and such issues arguably feature in all evaluation oriented components of SECUR-ED. Therefore in this task we have focused on unintentional and / or potential consequences not in focus in the project. . In identifying such consequences we are not restricting ourselves to what has directly been observed in the demonstrations. For example several mechanisms were at play to prevent ethically problematic issues from being included in the demos, e.g. the legislation currently in force in the demo countries. Here, in identifying possible threatening developments we do not take it for granted that these mechanisms continue to function in the future. But on the other hand we strive to maintain plausible links with today's world in sketching problem scenarios inspired by the demos, e.g., something needs to be said about how current defences against a problematic development could, in the future, disappear.

3.2 Brief presentation of the demonstrations

SECUR-ED is based on several demonstrations which are built around different scenarios. Four of them are defined as flagship demonstrations, while the others are smaller-scale and called satellites. The main demonstrations took place in Berlin, Madrid, Milan and Paris.

The Berlin demonstration provided security training for different groups of employees in order to improve job performance. The programs consisted of security awareness training for front-line employees, passengers and top management as well as other training programs for security employees, operators in control centres, security managers, police and railway staff and security awareness. In addition, the demonstration included standard and emergency operating procedures (SOP & EOP), field level security plans and decision making models for threat, emergency and crisis situations, and table top exercises for police and railway staff. The training programs cover a number of threats, varying from criminal activities such as pickpocketing, vandalism, evasion of fare payment and public disorder, to anonymous bomb threats, suspicious objects, assaults with cold weapons and dispersion of toxic material.

The Madrid demonstration aimed at enhancing stakeholder's cooperation with the help of an interoperable incident management tool, a CCTV system and communication between control centres in case of incidents. The demonstration involved four scenarios. Scenario 1 tested procedures as well as legacy technologies, scenario 2 checked how the incident management system and a geographical information system allowed interoperability among different stakeholders, scenario 3 added an intermodal CCTV to scenario 2 in order to check the efficiency of decision making procedures, and scenario 4 checked the interoperability between CCTV on board and the PTA.

The Milan demonstration also consisted of four scenarios. Scenario 1 checked how the integrated use of different technological systems and the exchange of information between actors made it possible to track a person behaving suspiciously. Scenario 2 tested the protection of vehicles in depot, while scenario 3 tested reaction and event management for three levels of situations: alert, alarm and crisis. Scenario 4 developed and tested a system of system in order to improve procedural coordination between different stakeholders.

The Paris demonstration evaluated protection from various forms of attacks and assessed technical and organisational devices in security matters, aiming at improving protection. This demonstration consisted of five scenarios. Four of them concentrated on one particular type of attack. Scenario 1 focused on cyber-attacks, scenario 2 on toxic attacks, scenario 3 on radiological attacks and scenario 5 on explosive attacks. Scenario 4 tested the cross function operation of CCTV and the use of video analytics applications.

The flagship demonstrations were followed up with satellite demonstrations. The satellites aim to further validate solutions developed and/or tested in the flagship demonstrations, and to ensure the wider applicability of project results and solutions. By the time the present deliverable is written, satellites have taken place in Bergen and Lisbon. Further demonstrations are planned and will take place by August 2014, in Bilbao, Bucharest and Izmir. In addition, a satellite might be arranged in Brussels.

The Bilbao satellite addresses capacities for person tracking, intrusion from platform to tunnel, perimeter anti-intrusion detection, and training. Both in Bergen and Bucharest the demo content involves training programs. The latter also involves basic CCTV. The satellite in Lisbon dealt with graffiti, crowding and abandoned luggage, making use of basic CCTV (fixed & on-board), intrusion/presence detection, fall detection and crowd density detection. The Izmir satellite is planned to deal with trespassing, hooliganism, unattended luggage, pickpocketing, drunkenness and copper theft. This means that the satellite will test the use of security control centres and training and crowd detection technologies. In addition, technologies for abandoned luggage, person tracking and explosive detection technologies are under consideration. The Brussels satellite plans to deal with disorderly behaviour, vandalism, trespassing, lack of security awareness and lack of security training.

Section 5.2 gives a more elaborate presentation of the demos focusing on the theme of this deliverable.

3.3 Efforts concerning ethics, privacy and societal issues within SECUR-ED

SECUR-ED has an overarching Advisory Board and four advisory groups. One of them is called AG Ethical and Societal issues (often referred to as AG Ethical) and provides advice to the consortium on ethics, privacy and societal issues. As already mentioned this deliverable has been elaborated in cooperation with AG Ethical.

While addressed already in the planning, ethical, privacy and societal issues have been taken more and more into account during the conduct of the project. This has been done in a number of ways. Some of them are described in D01.6 Ethical Management Report (Period 1). These are 1) periodical ethical management reports, 2) privacy policies deliverables, 3) compliance with EU directives, 4) the advisory group on ethical and societal issues (AG Ethical). Moreover this report, i.e. this consolidation of the societal aspects of the demonstrations, is presented as one way of dealing with ethical and societal issues.

The ethical management reports describe activities and discussions regarding ethical and societal issues throughout the SECUR-ED project. The privacy policies deliverable has resulted in a report describing policies, regulations and standards dealing with privacy and security in mass transportation at both national and European levels. In order for the activities to comply with EU directives, the descriptions of the demonstration scenarios

detailed access, storage and use of personal data before handing it to the appropriate national authorities for checking compliance and then communicating to the EU. Also at an early stage, a team of ethical experts was established as AG Ethical. AG Ethical follows the activities in the demonstrations and satellites. Independent ethics experts were involved, focusing especially on the flagship demonstrations. Each flagship demonstration had a person in charge of ethical and data protection issues.

3.4 Methodological approach

SECUR-ED's main task is to demonstrate the relevance and usefulness of tools, systems and processes for enhancing security of public transport in urban regions. Thus the starting point for SECUR-ED is mainly a technological and organisational one. Privacy, societal and ethical matters were of course recognised from the outset but here as elsewhere the consequences of the mutual influence between tools, systems and processes were not well understood; the difficulty of such foresight being the main reason for engaging in large scale experimentation in the first place. In line with this relevant research perspectives regarding the subject matter of this report hence were derived incrementally during the project. The empirical base was defined in correspondence with this.

Given the project's design, we have chosen a methodological approach built on the following two interacting knowledge sources:

1) Discussion of privacy, societal and ethical aspects based on experience from the SECUR-ED demonstrations
2) Discussion of privacy, societal and ethical aspects based on relevant literature.

This approach enables us to learn from the demonstrations. However, some privacy, societal and ethical aspects of security effort may not appear directly during the demonstrations, but are still of relevance. Others may emerge over time. As we want to comment also on such potential problems in relation to our subject, we combine the empirical results with literature. Needless to say the described approach does not allow us to fantasise freely: Demo results provide an understanding of what is feasible within a policy relevant timespan beyond the scenarios actually experimented – or simply in a context where other rules apply. These potentialities define the space for our not directly matter-of-fact based analyses.

3.4.1 Evidence generated by the demonstrations

The empirical basis of the present deliverable is taken from SECUR-ED's four flagship demonstrations plus two of the satellite demonstrations, Lisbon and Bergen. As mentioned in Chapter 3.2, the flagship demonstrations were followed by satellite demonstrations that aimed at further validating the solutions tested in the flagship demonstrations. The remaining satellite demonstrations were not performed in time to be incorporated in this report.

Each of the demonstrations has been described in a number of reports. While some reports described how demonstrations were planned, others reported the general results of the demonstration. Such reports are parts of our evidence base. In addition, the 46.6 team has visited all the mentioned demonstrations except Berlin and Milan. That means that team members were observers when the demonstrations took place. The collection of information,

including on-site observation, informal interviewing and the written reporting from the demonstrations, was conducted in collaboration with WP54.

3.4.2 Privacy, societal and ethical aspects based on literature

As reviewed in Section 3.1 the DoW asks for respect/possible impact on human right[s], privacy issues, impact of solution on social context and impact of solution on use of mass transit systems. The privacy, societal and ethical aspects cover a wide range of academic interests. Especially privacy has attracted much academic attention. In this report, no complete presentation of fields, debates or perspectives can be given. That way the literature study reported in Chapter 4 has been of explorative character, thus being more open to capturing relevant issues and perspectives not foreseen in planning the study.

3.5 Structure of report

After this introduction the report first presents literature based perspectives on privacy, societal and ethical issues from the vantage point of mass transport security (Chapter 4). Chapter 5 provides background on the demos including transport market characteristics of the demo regions.

The conclusions are provided in two chapters. Chapter 6 draws generic conclusions on emerging privacy, societal and ethical problems based on functions demonstrated in SECUR-ED, while the analysis of potential problems generalises beyond the specific experience of the project, but firmly based on its results in terms of technical feasibility. Chapter 7 presents results in other areas. Largely these can be described as SECUR-ED's contribution to the 'eternal questions' of the field, i.e. not particularly pertaining to novel technologies. One strand in the chapter deals with experimentation related issues, and it ends with a tentative suggestion for best practice for ethical and societal aspects in future large-scale experimentation and demonstration projects.

4 What are privacy, societal and related ethical issues?

Privacy, societal and ethical issues are broad concepts. In this chapter we clarify these and suggest some understandings of what is at stake with regard to these issues. We decided to focus on privacy, societal issues and the use of mass transit systems. We have not focused on human rights in general; however, privacy is seen as a human right. Neither have we specifically focused on ethical aspects. A main question in ethics is if a consequence or measure is right. The definition of 'right' is difficult to state, and will vary according to times, circumstances, cultures etc. Implicitly, in this consolidation we have assumed 'right' as not threatening privacy, and not reducing accessibility to public transport and places.

4.1 Privacy

When talking about societal consequences of security technologies, privacy often becomes an issue. We want both, but it seems that they represent values that are in opposition to each other. Privacy protectors claim that security measures threaten privacy, and that fear of terrorism (and consequently, a demand for security measures) tends to trump privacy concerns (Lace 2005). Naturally, we want security. However, privacy is an important topic for several reasons. The main reasons are that 1) privacy is often enshrined in law and 2) privacy is seen to be a basic value and premise for a democratic society. The former is in some ways the easiest aspect to deal with, offering regulations as a starting point for analyses. We will return to that after a discussion of what sort of value privacy is.

4.1.1 What is privacy

Although it is hard to find a commonly agreed upon definition of privacy (Raguse, Meints et al. 2008), it is without doubt widely accepted that privacy is a fundamental right and common good. It cannot be isolated from other goods. As all common goods, it competes with some and supports others: it clashes for example with the right to free speech while it promotes autonomy and dignity (Solove 2007). The fact that it promotes other values means that limitations on privacy also place those other values at risk. We may not always be able to foresee which other values, and how they are threatened, and this is a reason to treat privacy issues carefully. Here, we want to draw attention to the relation between privacy and autonomy.

A central principle to ensure privacy is consent: Personal information should be registered only when the person gives his or her consent to do so and the consent is informed and freely given. We will discuss the concept of consent in the next section and we will therefore not go into details here; instead we want to point out its' deeper meaning, namely that the consent is a tool for limiting others' access to our lives. Thus privacy limits the control of others over our lives, and in doing so it promotes social freedom (Shoeman 1992). Only with such freedom, can we act as free citizens. The 'others' can be both authorities and persons. By limiting others' access to information, also their power is limited. Privacy thus is a defence mechanism against societal pressure on individuals (Leino-Kilpi et al 2001). By being a prerequisite for freedom, privacy also becomes a prerequisite for democracy. Following from

this, privacy involves two levels; an individual level, at which it promotes the individuals control over others' access to their information, and at a societal level, at which it functions as a premise for democracy.

The concept of privacy has changed in recent decades (Burgess 2008). A variety of perspectives and dimensions have been presented (Leino-Kilpi, Välimäki et al. 2001; Clarke 2006; Burgess 2008). It will not be part of this analysis, but it is worth mentioning that privacy is regarded important for several reasons: *philosophical*, as it ensures the *individual's* freedom and integrity, *psychological*, as it meets our need for personal space, *sociological*, because we need the freedom to engage with other persons without the prospect of being surveyed, *economic*, as competitive power requires innovations and new thoughts, which again require freedom of thought, and *political*, as human beings must have the possibility to think, talk and act freely (Clarke 2006).

Another way of categorizing privacy is to distinguish between perspectives focusing on integrity, power and decision-making (Schartum and Bygrave 2004). When focusing on integrity, control over personal information is an important aspect. The basic idea is that every person has a private sphere, and anyone entering that sphere must either have permission or a very good reason. A focus on power raises questions about whether or not the registered information disturbs or changes the balance between groups, as knowledge can be tools of both power and control (Johansen et al. 2001). A focus on decisions draws attention to fact that many decisions are made on the basis of personal information, as is the case for many public services. Such decisions can have tremendous impact on individuals' lives, and it is therefore important that both information and decisions are correct.

A fourth focus is the one of knowledge: Privacy is knowledge about persons' private sphere. It is also meta knowledge, as it is knowledge about the knowledge: who knows what? Why do they know? In addition, it relates to control over knowledge, that is, how it is used (Burgess 2008).

4.1.2 Privacy according to legislation

Privacy and related ideas can be found in the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, the European Convention on Human Rights and the Charter of Fundamental Rights of the European Union. Also many national laws deal with privacy. National differences occur, however, some recurring issues are consent, function and access.

As already stated, control over personal information is central. We will therefore in the following passages have a closer look at the concept that helps to keep that control, namely the principle of free and informed consent. Registration of personal information requires consent. The consent shall be 'freely given, specific and informed' (EU Directive 95/46/EC, Article 2 (h)).

'Informed' means that the individuals being registered in some way or another is told that the registration is taking place. The amount and shape of such information varies and can be anything from a sign on the wall notifying a 'video surveyed area' to a lengthy text with small letters stating rights, procedures etc. in different situations. Everyone who, in order to give his or her consent, has ticked off in a box on the Internet when buying for example a ticket, knows that it is easy to skip the reading and just tick off the box. This is such a common thing to do that law experts start to think that the informed consent is an illusion.

In order to be 'freely given' a consent requires a choice. Consent is not freely given if there is no possibility to *not* consent. However, what counts as an option is not always clear. Sometimes the option involves long ways around, inconveniences, or not receiving discounts. It can be questioned if such options are to be considered as options. If the difference between what individuals gain if they give their consent and what they reject if they do not is imposing, it might not be realistic to consider the choice 'free'. Relevant questions regarding consent are thus: Is the consent freely given? Does a realistic option exist? Does the option(s) involve inconveniences? To what degree?

A consent being informed, implies that individuals know what information is registered and for what purpose. In other words: the purpose of the registration must be stated. However, data is attractive, and databases are therefore vulnerable to function creep. Function creep is data being used for other purposes than the original intended one. Due to information-thirst, rules are broken or bent, and prior specifications of how information use should be limited, or data not shared, are of no value (O'Hara and Shadbolt 2008). Both policies and technologies make function creep possible. An examination of Australia's revised ID Card Bill shows how a number of features can provide possibilities for expansion in relation to the functions and purposes the Bill was claimed to have. The features included open objectives, the content of the registered information, the card itself, inadequate legislative requirements to protect chip content and also inadequate definition of who was given the right to access the data (Greenleaf 2008). All in all, function creep is regarded a threat towards privacy, as it violates the basic premise that we should have control over the information over ourselves. When information is used for additional purposes, we are no longer asked to consent, and we thus do not have any control of who uses it and for what purpose.

On the other hand, many find function creep positive and even desirable. In many cases, the use of data collected for a specific purpose can be of great help in other situations; not doing so due to privacy issues related seems to miss an opportunity. For example, several cases of function creep take place at police stations, where investigators make use of databases originally established in order to serve central or local government administrations. This is in many cases made legal by law. The same counts for CCTV; their purpose is for example to survey a room in order to avoid shoplifting, but the police can ask for the tape based on a request for hearing of evidence, also when the purpose is the investigation of another crime. Another example could be police authorities' access to London's congestion charge cameras, allowing them to track all vehicles entering and leaving the zone. The result is an infrastructure of cameras built to help manage congestion in London but now being used for routine surveillance by the Police (http://thesamovar.wordpress.com).[1] The Police assures that the camera data will only be used for national security purposes and not to fight ordinary crime. Thus the expanded use of data can be seen as both opportunistic and a planned function creep (ibid.). In order to check whether consent is informed, relevant questions are: Is the consent informed? How is the purpose specified?

Another aspect of privacy is the principle of proportionality: that the effort shall be proportional to the benefits. This is most easily measured in cost, but many cases involve benefits that cannot be readily measured in money. That makes the question about proportionality hard to assess. It is not easy to hold privacy up against passengers' feelings

[1] http://thesamovar.wordpress.com/category/politics/civil-liberties/id-cards/

of security, or decide how much data are reasonable to collect in order to improve security, perhaps to an unknown degree.

Another problem relating to proportionality are the questions about decision making (Iphofen 2014): Who decides? How do they decide, that is, on what criteria do they decide? When can they decide? The answers are not given, and depending on how decision powers are allocated, the weighing procedure necessary to ascertain proportionality in practice may be biased in different ways; proportionality is a difficult standard to interpret and apply.

4.2 Societal consequences

Social consequences are here mainly understood as accessibility. Partly accessibility is regulated by law; partly it has to do with other factors.

4.2.1 Accessibility by design

Universal Design or Accessibility refers to transport facilities and services designs that accommodate the widest range of potential users, including people with mobility and visual disabilities and other special needs. It can be defined as the ease with which a building, place or facility can be reached by people and/or goods and services. Further, it can be shown on a plan or described in terms of pedestrian and vehicle movements, walking distance from public transport, travel time or population distribution.

Different modes of public transport are integrated in the urban space in different, more or less segregated ways. This again means accessibility is ensured in different ways connected to different modes of public transport.

Accessibility, operationalized as barrier-free public transport, has its legislative foundation in the UN – Convention on the Rights of Persons with Disabilities (valid since May 3rd 2008). The convention has formally been confirmed by the EU (December 28th 2013) and equally ratified by the different members of the EU (and EEA). Ratification is furthermore formalized in different national laws. On a national legislative basis it is formalized as acts for the ‘equal treatment of disabled’, passenger transportation acts and technical guidelines for public transport infrastructure, vehicles and operations.

A barrier-free public transport is to be established and maintained with regard to

- Different types of infrastructure (including station areas)
- Vehicles
- Information and services (including training for drivers and service staff and mobility- and safety-related training for passengers with restricted mobility)

Perspectives of barrier-free public transport are also applicable in crisis and emergency situations. New technologies improving security and safety must not worsen the conditions for barrier-free public transport.

In addition, in general within the project SECUR-ED and its demonstration sites, there is a focus on high quality public transport. This means public transport that is able to compete with private vehicles in terms of convenience, speed, price and reliability. The term is used to

include underground services, heavy rail commuter services, light rail, guided bus ways, and high quality bus networks.

Underground and heavy rail commuter services by their technical definition are not at all integrated in the public space except within the station area. The light rail and bus services are to a much higher degree integrated in the public space. Accessibility, public space must be considered and treated in different ways between the above mentioned different modes of public transport.

In general, urban and transport planning focus on achieving the highest integration of public transport in the urban space, thus giving public transport a competitive edge.

4.2.2 Accessibility by security?

Public transport, including vehicles and facilities like stations, waiting rooms and stops, can be considered public spaces. Public spaces are mostly publicly owned and managed; this may often not be the case when public transport systems are concerned. Public transport has experienced an increase in privatization lately and its locations and facilities are not necessarily public anymore in terms of ownership. Instead, a variety of semi-public actors or a combination of private and public actors are involved. We still think of public transport as part of our public space; this is because we define it by its accessibility. It is space accessible to public. This does not mean that access is without limitations, for example that travelling is free. You do need to buy a ticket in order to go by bus. However access does not require membership of any sort. It is a liberal model, meaning it invites all people to use it (Iveson 1998, referred in Crane and Dee 2002)). Accessibility should here be understood in both physical and psychological terms. This means that a place which is considered too dangerous, or not suitable, is not accessible even though there are no physical barriers. Note that this approach lets us consider the same place in different ways according to time of day, number of passengers, day of week, etc. In other words the degree of accessibility can vary greatly according to these criteria.

Accessibility to public transport is crucial due to three reasons. One reason is the social task (the task incumbent on the community). Public transport should offer services to anyone who can pay for the required ticket. Another reason is its role in general mobility; accessibility is what guarantees the free circulation of persons and goods (Tonnelat 2010). A third reason is the effect accessibility has on demand. Reduced accessibility means fewer travellers.

A relevant question is thus: **Do the evaluated capabilities affect accessibility? If so: how?**

We want to avoid technological determinism. That means that we do not regard technology to have intrinsic features that lead to specific consequences. Instead, capabilities will always be influenced by contextual factors. Someone uses it, in order to reach specific goals. In this case, we sort the factor according to actors. Three types of actors can be identified: a) those who are being protected by the capacities, b) those who use capacities to protect, and c) those we are protected from. The latter group can be further differentiated, as we can distinguish the real criminals from the expected criminals. The main groups are the protectors and those being protected, and we will now have a closer look at the factors ‘located’ at these two main actor groups.

Those who are being protected by the capacities

When focusing on this group, we need to know how the public accepted the capabilities, in order to answer the question whether or not capabilities affect accessibility. We also need to know what individuals fear. It turns out that many are affected by fear of crime rather than crime itself and this fear might have behavioural consequences (Bannister and Fyfe 2001, ref. in Yavuz and Welch 2010). It turns out that fear of crime leads individuals to avoid places that are perceived to be dangerous, not go out at night and not travel alone in certain areas (Yavuz and Welch 2010). Fear of crime is among the most important reasons why people choose not to use public transit (Lynch and Atkins 1988; Walsh 1999, both referred in Yavuz and Welch 2010). This means that fear is not only concerned with the risk of crime, it also has to do with feeling vulnerable. We thus have to ask: What do individuals fear, and do the capacities respond adequately to these fears?

The SECUR-ED demonstrations and satellites were not designed to give an empirical base to answer this question. We will therefore draw on other research in order to find which responses are to be expected.

Train travel is one of the most fear-inducing activities in public space (Walsh 1999, referred in Yavuz and Welch 2010). This is because train riders often feel that they are confined and restricted in their ability to cope with dangerous situations (ibid.).

Research indicates that men and women fear different things in public spaces. In the UK, men worry more about the presence of groups of other men, and they fear violent assault. Women, on the other hand, worry more about single men and they fear rape and sexual assault (Crime Concern 1997; 2004). Women tend to feel more vulnerable when nobody is around to provide surveillance against crime or in the presence of social incivilities (Yavuz and Welch 2010). Men tend to feel more vulnerable when they have less control over their environment or when surrounded by unfamiliar people in public space (ibid.).

The same factors that induce fear in public space tend to also induce fear in public transit. There are gender differences: compared to men, women are more likely to avoid walking after dark, preferring to drive or take a taxi rather than walking or using public transit (Yavuz and Welch 2010). Darkness, poor lighting and isolation contribute more to women's fear, and women often mention lonely bus stops, unstaffed stations and pedestrian subways among the places that cause fear. 'In addition, they report higher perceived insecurity while walking at night in parks and when waiting at bus stops or platforms in isolated areas' (Lynch and Atkins, 1988, ref, in Yanuz and Welch 2010). This can lead women to take more inconvenient routes or less frequented rides in order to avoid fear-causing situations (Hamilton and Jenkins 2000 referred in Yanuz and Welch 2010).

Also, authorities have sought to 'design out' opportunities for young people to make unstructured use of places, e.g. by the removal of seating areas and 'hanging out' space (Owens 1999, referred in Crane and Dee 2001).

The protectors

When concentrating on this group, the main questions are: How are the capabilities used, and how do the specific ways of using them affect accessibility?

From previous research on CCTV, we know that a lot of factors determine consequences (Lomell 2004, Sætnan et al. 2004). One such factor is the user. Who are they? Are they from private security firms, police or PTOs? Do they operate in the field or from behind a desk? Another factor is their training. What are they trained for? Is it sufficient? A third factor is how

they view their tasks. A fourth factor is what reaction follows from observing. In other words: how do they react to what the technology tells them? As for the cameras, there are several possible reactions or outcomes. It could be conversation, expelling the perpetrator from the designated area, or handing over further actions to the police etc. When it comes to surveillance, the intensity is important. We must therefore discuss the type of surveillance used. Where are the camera and monitor placed? What is the size of the surveyed space? What are the monitoring hours? And how does the monitoring take place? Is there someone staring blankly at a screen or checking it every now and then, or, if monitoring takes place, is it one person's single task or carried out in combination with other tasks, or are the screens used pro-actively to zoom in on suspects and track them? What types of activities or looks draw attention?).

With so many factors that can vary, it is hard to estimate a specific consequence of the capacities in SECUR-ED. Studies of CCTV, that is observation studies of surveillance control rooms, have found that the operators do single out and target for closer observation those they believe to be deviant, a selection more often made on the basis of appearance alone than on behaviour. This leads to repeated targeting of groups culturally linked with criminal deviance, that is, men, particularly if they are young and / or black (Norris and Armstrong 1999:196). Most people chosen for closer observation in Norris and Armstrong's study (ibid.) were targeted 'for no obvious reason' rather than for their criminal behaviour. Still, police or security guards were seldom called upon. This illustrates the problem of judging behaviour and appearances. Relevant questions in this regard are what can be legitimately seen as 'suspicious behaviour', how behaviour is categorized and identified, and who makes this judgement call (Iphofen 2014).

Such targeting leads to categorical exclusion (Lomell 2004; Sætnan et al. 2004). Such exclusion is based on expectations about whom an individual is and what he or she will do, rather than what he or she actually does, that is, without any actual evidence of criminal wrongdoing.

Categorical exclusion is not an appreciated practice. We often think that surveillance cameras should be all-seeing, but instead they are pre-selecting. A common belief is that 'I have nothing to fear, because I have nothing to hide'. This is wrong for many reasons, and the categorical exclusion is one of them. It does not help that you have nothing to hide, as long as you 'look suspicious'. We should therefore be sceptical about categorical exclusion – and to CCTVs, as they have the potential of becoming tools of injustice through the amplification of differential and discriminatory policing if the decision whether you are 'suspicious looking' or not involves, e.g., ethnic profiling.

As an aspect of this, it is relevant to discuss the privatization of public space. The discussion is relevant because private actors tend to change the public space by establishing new activities. The presence of private actors like cafes, bars and shops turn places into areas for buying food and drinks or other goods. Shopping becomes the dominating activity, and as such participating in that activity becomes the 'ticket' to the public place. Participating, meaning presence requires the ability to take part in the activity (shopping). The place then becomes less formal than it is without shops.

On the other hand, a public space without 'suspects' may appeal to the majority. 'The prospect of a confrontation with an obstreperous teenager or a drunken panhandler can be as fear-inducing for defenceless persons as the prospect of meeting an actual robber; indeed, to a defenceless person, the two kinds of confrontation are often indistinguishable'

(Wilson and Kelling 1982). Therefore, maintaining social order can be appreciated, although actual crime rates stay the same.

5 The demonstrations

This chapter first gives a broad background to the demos by presenting the city regions where they are set, then discusses the demos from the vantage point of this report's theme, and finally identifies the demonstrated functions relevant for the subsequent analysis.

5.1 Context: the demo regions and their public transport

Public transport in urban regions is always in competition with other modes of transportation, such as walking, cycling and, mainly, cars. Its market share and patronage on a regional level are by no means to be regarded as given or stable. Competition in transportation markets on a regional level is usual a demanding issue for public transport.

A focus on social, privacy and ethical aspects in the SECUR-ED project has to take into account the competitive situation for public transport in urban regions. Measures to improve security and safety matters are to be designed with the aim of improving the competitive edge of public transport. In practice this means that no measure should be proposed or realised, which could have the effect of worsening the competitive situation for urban public transport.

Demonstrations and satellite demonstrations were carried out within the project in regions, which varied in terms of their characteristics and adjacent public transport systems. A relevant question is thus if this variation affected the demonstrations. Did regional characteristics and public transport system have any impact on the outcome of the testing?

A description of the status of public transport in the various urban regions will function as a background for considering the regional context in each area with the aim of introducing new technologies and capacities for improving security in public transportation. Examining the regional context might lead to important questions and new perspectives which are relevant and meaningful.

The status of public transport in different urban regions can be estimated on three different levels (categories) with an accompanying set of indicators. Such an analysis helps to contextualise public transport in different urban regions using the relevant results from the project's demonstration sites. Later on it will also contribute to an understanding of the context around public transport in urban regions, when the results are transferred or adapted to additional sites and urban regions. Given the need to transfer relevant results from one demonstration/satellite to another within the SECUR-ED project and to other urban regions, the status of public transport in each of the urban regions involved is covered in this report.

5.1.1 General characteristics of urban regions involved in SECUR-ED

The overall performance/market shares for public transport in urban regions vary significantly between urban regions of comparable size. But in general it can be said that market shares for public transport increase the larger the urban region is (measured by number of inhabitants). Generally speaking, public transport in minor urban regions is much more exposed to competition with other modes of transportation. While the implementation of measures for improving security in public transport for larger urban regions might be more

technologically challenging, implementing such measures in smaller urban regions must be considered even more carefully with regard to public transport's competitive edge.

Market shares for minor urban regions (< 100.000 inhabitants) can be as low as 4 per cent, for urban regions with 100.000 to 250.000 inhabitants it can be as low as 7 per cent, for urban regions with 250.000 to 500.000 inhabitants it can be as low as 8 per cent, and for urban regions with more than a million inhabitants it can be as low as 14 per cent. Public transport's market shares might vary significantly for urban regions of a comparable size by number of inhabitants due to variations of regional GDP, level of car ownership, more or less extensive access to road networks and competition by walking and cycling.

The following indicators can be used to characterise the urban regions:

- Size and extension of the urban regions (indicators to be used: number of inhabitants, inhabitants per km^2)
- Demographic attributes (indicators used: sex and age)
- Economic attributes (indicators used: regional gross domestic product (GDP) or average income in purchase power parities)
- Overall performance of public transport (indicator used: percentage of enhanced modal split)

Table 5.1 Percentage share of local trips by private motor vehicle, public transport, walking and cycling (Source: TEMS, www.epomm.eu/tems/index.phtml[2]).

	private motor vehicle	public transport	walking	cycling	Population
Berlin (2008)	31%	26%	30%	13%	3.510.000
Paris (2008)	17%	33%	47%	3%	2.210.000
Madrid (2009)	23%	38%	38%	1%	3.260.000
Milan (2005)	35%	33%	27%	5%	1.300.000
Brussels Capital region (2008)	47%	48%	3%	2%	1.140.000
Lisbon (2001)	47%	35%	1%	16%	2.800.000
Bergen (2009)	41%	16%	30%	3%	245.000
Bucharest (2007)	24%	53%	22%	1%	1.940.000
Bilbao (2006)	10%	29%	60%	1%	353.000

[2] Statistics TEMS is based upon are derived from national and local sources that might differ by design and by methods used.

Due to capacity restraints, we are not able to present all indicators. The most important indicators such as population and enhanced modal split in urban regions participating in SECUR-ED are shown in table 5.1.

As the table shows, modal share for public transport can vary significantly between regions of comparable population, like between Berlin, Paris and Madrid. It is not only car transportation public transport is competing with. The competition between public transport and walking and cycling must be taken into account when comparing the overall status of public transport...

In general the market share of public transport is lower in major urban regions in Western Europe with an average of 18 per cent, compared to major urban regions in Eastern Europe with an average of 45 per cent (source: Gilbert et al. 2008., p.71, table 2.2).

5.1.2 General characteristics of public transport in the urban regions involved

Public transport adjacent to urban regions can be characterized by several indicators and sub-indicators. Some of the indicators focus on the urban transport per se, while others focus on the public transport demand.

In order to characterize urban transport in the specific region the following indicators can be used:

- Patronage (indicators to be used: number of passengers, public transport demand per inhabitant)
- Financial situation (indicators to be used: turnover, percentage cost covered by fare revenues)
- Political responsibility (indicator to be used: responsibility for financing the operators' budget deficit)
- Type of public transport services operated (indicator to be used: bus services, light rail services, underground services and heavy rail services established).

Type of public transport services operated is directly related to the issue of public space. Metro and heavy rail are by definition highly separated transportation means in terms of space, that is, they are physically separated from other transportation means. Tram and buses are transportation means with a much higher degree and need for integration in public space.

In order to characterize urban transport in the specific region and the demands of its citizens/inhabitants, the following indicators can be used:

- Individual mobility (indicator to be used: trips made on a daily base)
- Individual time budget (indicator to be used: travel time on a daily base)
- Individual travel costs (indicator to be used: travel budget on a monthly base)

The indicators suggested above are relevant in a European context and are relatively easy to obtain via public statistics. In the tables below we show some of the numbers for Berlin-Brandenburg, Paris Ile-de-France, Madrid Community and Brussels Metropolitan. Due to capacity restraints, we are neither able to present all indicators nor all demonstration regions.

Table 5.2 Total journeys by public transport per inhabitant and year in 2011 (Source: EMTA barometer 2011, www.emta.com[3])

	Total journeys by public transport per inhabitant and year
Berlin-Brandenburg	186
Paris Ile-de-France	349
Madrid Community	230
Brussels Metropolitan	163

The table shows that the number of yearly journeys by public transport per inhabitant is by far the highest in Paris. There the total journeys are 349 per inhabitant. Also in Madrid the number is high, there the total journeys by public transport is 230 per inhabitant. The Berliner travel the least by public transport; 186 total journeys per inhabitant and year.

Table 5.3 Coverage by fare revenues in 2011 (Source: EMTA barometer 2011, www.emta.com)

	Coverage by fare revenues
Berlin-Brandenburg	46,2%
Paris Ile-de-France	39,6%
Madrid Community	44,0%
Brussels Metropolitan	46,3%

Table 5.3 shows that Berlin and Madrid have approximately the same coverage by fare revenues; Berlin with 46.2 percentages and Madrid with 44.0 percentages. Paris has a coverage on 39,6 percentages. The figures are interesting as they indicate the need of regional authorities support. The lower the coverage by fare revenues, the more the PTO depends on public authorities. A low coverage by fare revenues can thus limit the PTOs latitude.

Table 5.4 Public transport demand per inhabitant per public transport mode in 2004 (Source: EMTA barometer 2004, www.emta.com)

	Public transport demand per inhabitant (million passenger-km/1000 inhabitants)
Berlin-Brandenburg	Bus: 0.4, Metro: 0.4, Heavy Rail: 0.7, Tram: 0.09
Paris Ile-de-France	Bus: 0.4, Metro: 0.6, Heavy Rail: 1,3, Tram: 0.01
Madrid Community	Bus: 1,1, Metro: 0.6, Heavy Rail: 0.6
Brussels Metropolitan	Bus: 0.1, Metro: 0.2, Heavy Rail: 0.13

[3] The EMTA Barometer 2011 leaflet has been published in full version in December 2012.

Table 5.4 shows that the public transport demand per inhabitant varies the most for bus and heavy rail when comparing the regions. We find the highest demand for buses in Madrid, while Paris has the highest demand for heavy rail. The demand for metro varies less.

While buses in general are more integrated in the urban space, heavy train is separated from other transport. The distribution of demand thus indicates different challenges according to accessibility.

5.1.3 The context of involved urban regions and their public transport systems

Urban regions and their public transport systems involved in the SECUR-ED's demonstrations and satellites can be contextualized according data shown in Table 5.5. In the table, the phrase 'rail' refers to heavy rail.

With the exception of Bergen and Bilbao all urban regions involved in SECUR-ED's demos and satellites are regions with more than a million inhabitants, even if every region's size of population varies according to different definitions of its geographical size (for example Berlin vs. Berlin-Brandenburg and especially Paris vs. Ile-de-France including Paris).

Almost by definition public transport in European urban regions of this size achieves higher market share compared to minor urban regions like Bergen. Amongst the project's demos and satellites, public transport in Bergen is exposed to a tougher competition especially by car transportation.

But then there are huge differences between the bigger urban regions participating in SECUR-ED.

5.1.3.1 Paris

Ile-de-France including Paris is by far the biggest urban region participating in the project with about 12 million inhabitants (2012). With 349 total journeys per inhabitant a year and high modal split shares public transport here enjoys a very favourable market position. Best modal split shares for public transport are achieved for transport within the community of Paris and for commuting from the surrounding region to Paris. Demand for public transport is supported by high urban densities in Paris and the outstanding centrality of Paris within the region. About 82 per cent of public transport demand per inhabitant measured in passenger kilometres is realized by metro and heavy rail. The question of integration of public transport in the public space is mainly connected to the development of bus and tram systems accounting for 18 per cent of public transport demand per inhabitant.

Table 5.5 Characteristics of urban regions and their public transport systems involved in the SECUR-ED's demonstrations and satellites (Source: epomm/tems)

Urban region	Population	Modal split share public transport (percentage)	Modal split share private motor vehicle (percentage)	Total journeys by public transport per inhabitant and year	Public transport demand per inhabitant (mio passenger-km/1000 inhabitants)
Berlin (2008)	3.510.000	26	31	186 (Berlin-Brandenburg, 2011)	Bus: 0,4, Metro: 0,4, Rail: 0,7, Tram: 0,09 (Berlin-Brandenburg, 2004)
Paris (2008)	2.210.000	33	17	349 (Paris Ile-de-France, 2011)	Bus: 0,4, Metro: 0,6, Rail: 1,3, Tram: 0,01 (Paris Ile-de-France, 2004)
Madrid (2009)	3.260.000	38	23	230 (Madrid Municipality 2011)	Bus: 1,1, Metro: 0,6, Rail: 0,6 (Madrid Community, 2004)
Milan (2005)	1.300.000	35	33	n.a	n.a
Brussels Capital region (2008)	1.140.000	48	47	163 (Brussels Metropolitan, 2011)	Bus: 0,1, Metro: 0,2, Rail: 0.13 (Brussels Metropolitan, 2004)
Lisbon (2001)	2.800.000	35	47	n.a.	n,a,
Bergen (2009)	245.000	16	41	n.a.	n.a.
Bucharest (2007)	1.940.000	53	24	n.a.	Trip shares within PT*: 35,8 % bus, 30,2% metro, 30,2% tram, 3,8% rail
Bilbao (2006)	353.000	28	10	n.a	Trip shares within PT*: 46,4 % bus, 46,4% metro, 1% tram, 1% rail

5.1.3.2 Madrid

The Autonomous region of Madrid and Berlin-Brandenburg are both of comparable size of 6,0 and 5,9 million inhabitants (2012). Figures available indicate a more favourable position for public transport in the autonomous region of Madrid with 230 total journeys per inhabitant a year compared to 186 in Berlin-Brandenburg. Within the community of Madrid public

transport with 38 per cent actually enjoys a significantly higher market share than what is achieved in Berlin with 26 per cent. Also the community of Madrid public transport enjoys a very favourable market position comparable to that in Paris. Best modal split shares for public transport are achieved for transport within the community of Madrid and Berlin, and for commuting from the surrounding region to Madrid and Berlin.

In the autonomous region of Madrid about 52 per cent of public transport demand per inhabitant measured in passenger kilometres is realized by metro and heavy rail. The question of integration of public transport in the public space is mainly connected to the development of bus and tram systems accounting for 48 per cent of public transport demand per inhabitant.

5.1.3.3 Berlin

In Berlin-Brandenburg about 69 per cent of public transport demand per inhabitant in passenger kilometres is realized by metro and heavy rail. The question of integration of public transport in the public space is mainly connected to the development of bus and tram systems accounting for 31 per cent of public transport demand per inhabitant.

5.1.3.4 Milan

The province Milan including the community of Milan accounts for about 3.1 million inhabitants (2012); the community of Milan about 1.3 million inhabitants (2012). The suburban area of Milan (Provincia di Milano) has 3.5 million inhabitants.

5.1.3.5 Lisbon

The region of Lisbon including Lisbon accounts for about 3,1 million inhabitants (2012)); the community of Lisbon about 0,6 million inhabitants (2012).

With 35 per cent modal split share in the community of Lisbon public transport here enjoys a favourable market position.

Public transport faces tough competition from car transportation. Walking as mode of transport is of minor importance, while cycling is of some importance.

5.1.3.6 Brussels

Brussels Metropolitan area accounts for about 1.1 million inhabitants (2012). Figures available indicate a position for public transport in the Brussels Metropolitan region with 163 total journeys per inhabitant a year, in size comparable with Berlin-Brandenburg. But contrary to Berlin-Brandenburg public transport seems to be in exclusive competition with car transportation in the Brussels Metropolitan region. Walking and cycling as modes of transport are of minor importance.

In the Brussels Metropolitan region about 77 per cent of public transport demand per inhabitant is realized by metro and heavy rail. The question of integration of public transport in the public space is mainly connected to the development of bus and tram systems accounting for 23 per cent of public transport demand per inhabitant.

5.1.3.7 Bergen

Bergen community counts about 245.000 inhabitants. The ratio between the market share for car transportation and public transport is the highest in favour of car transportation amongst the demos and satellites in SECUR-ED. In Bergen community about 5 per cent of public transport demand per inhabitant is realized by heavy rail.

5.1.3.8 Bucharest

Bucharest community has about 1,9 million inhabitants (2012). With 53 per cent modal split share in the community of Bucharest public transport enjoys a very favourable market position. About 34 per cent of public transport demand per inhabitant measured in passenger trips is realized by metro and heavy rail. The question of integration of public transport in the public space is mainly connected to the development of bus and tram systems accounting for 66 per cent of public transport demand measured in passenger trips per inhabitant.

Public transport faces competition from car transportation. Walking as mode of transport is of major importance, while cycling is not important.

5.1.3.9 Bilbao

Bilbao community has about 350.000 inhabitants (2013). Bilbao metropolitan region is about 0,9 million inhabitants. With 28 per cent modal split share in the community of Bilbao public transport enjoys a relatively strong market position. About 50 per cent of public transport demand per inhabitant measured in passenger trips is realized by metro and heavy rail. The question of integration of public transport in the public space is mainly connected to the development of bus and tram systems accounting for 50 per cent of public transport demand measured in passenger trips per inhabitant.

Within Bilbao community walking as mode of transport is the major competitor, while cycling is not important.

5.2 What do the demonstrations tell us about privacy, societal and ethical aspects?

In this section we take a close look at the demonstrations in order to see which, if any, privacy societal and / or ethical issues were considered. Ideally, all demonstrations should have been looked at, but for the time being neither are all the demonstration satellites finished nor are all demonstrations reports prepared. We therefore concentrate on the flagship demonstrations and to them add the satellite demonstrations in Bergen and Lisbon. We start by presenting each demonstration and then discuss the findings.

We start with the flagship demonstrations before we move on to the demonstration satellites.

5.2.1 The Berlin demonstration

Aim and scenarios

The demonstration in Berlin provided security training for employees. Employees are seen as a key part of security, it is therefore relevant to include training in the security effort. The training is separated into different training progress for different groups of employees,

resulting in security awareness training programs for front-line employees, passengers and top management and other training programs for 1) security employees, 2) operators in control centres, 3) security managers, 4) police and railway staff and 5) security awareness. In addition, the demonstration contains standard and emergency operating procedures (SOP & EOPs), field level security plans and decision-making models for threat, emergency and crisis situations, and table top exercises for police and railway staff. The training programs answer a number of threats, varying from criminal activities such as pick-pocketing, vandalism, evasion of fare payment and public disorder, to anonymous bomb threats, suspicious objects, assaults with cold weapons and dispersion of toxic material. Altogether six scenarios were pictured: 1) assault with neither physical violence nor theft, i.e. aggressive behaviour and / or use of abusive language, 2) sabotage in the shape of cutting energy supplies and interfering with signalling or power equipment, 3) criminal damage like tag, graffiti and small scale arson, 4) threat events like anonymous calls, suspicious object and suspicious vehicle, 5) illegal activities in the transport system, for example consuming illegal products, illegal sales, production and sale of counterfeit tickets and trafficking, and 6) behavioural and public disorder offences like noncompliance with animals rules and smoking rules, drunkenness and vagabonds.

For all the training programs the objective is to improve job performance and, for the groups it is relevant to, raise the level of competence and ensure better courses of action. In the table top exercises the purpose is to encourage discussion among stakeholders and developing awareness of coordination and planning requirements.

The demonstration is further described in the SECUR-ED report D45.1 Detailed Scenarios for Berlin demonstration.

Privacy, societal and ethical issues

Early in the project, according to D11.2 Measures to Improve Security and Privacy, legal, societal and ethical concerns were said to be related to the legal competence of security staff as defined by legislation. Further on, customer respect needs to be ensured, and the access to data and images need to be controlled. When commenting on the demonstrations, AG Ethical said partly the same, revealing the need to respect legal provisions regarding the privacy and personal data protection of passengers and staff alike. Privacy and personal data must be protected also when actors, trainers and trainees are involved. In order to avoid privacy issues linked to CCTV usage, it was decided not to introduce any CCTV system in the demonstration. Instead, pre-recorded video clips simulating real CCTV pictures were used in the training systems. The clips involved only actors and not real passengers.

In the ethical review checklist one possible risk was ticked off, and that was psychological harm on participants. Psychological harms are for example, according to the checklist, lowered self-esteem, emotional distress, embarrassment, misperceptions of the purpose of the project that raise false expectations of gain to participants, or induce unnecessary fear. A respondent commented that ‘training can always be a cause for psychological harm’. The formulation refers to training in general, thus indicating that the respondent had no specific risk in mind. This led us to think that the probability for psychological harm was low. It was explained that ‘experienced trainers will ensure that possible harm will be prevented through detailed briefing and continuous reassurance during training sessions’.

The checklist asked if the measure / set of measures involved automated processing of data that relate to living individuals which can directly or indirectly be identified. The answer was

'yes'; pre-recorded images were an input for one of the scenarios, and streaming / living coverage without recording during demonstration for observational purposes. Participants were informed about this and that the data should be kept until the end of the demonstration. The before-mentioned decision was made that only pre-recorded video clips simulating real CCTV pictures were to be used.

The experimentation report (D45.5 Experimentation report for Berlin demonstration) documents that a repeated feedback was that the training was interesting. As feedback on the training programs for security managers, it was also commented that training has to be adapted to the local culture and procedures. What does not appear in the documents is that trade union involvement was critical to the training programs due to the planned CCTV usage. At the mid-term conference, the need to involve trade unions was presented as a 'lesson learned'. This experience is a reminder that privacy issues in regard to security efforts in public transport can also affect employees in public transport

5.2.2 The Madrid demonstration

Aim and scenarios

The Madrid demonstration aimed at enhancing cooperation between stakeholders. In Madrid the exchange and coordination of information is challenging due to a complex map of operators offering various modes of transport. In order to improve coordination among PTOs, the Regional Transport Consortium (CRTM) has created an Integrated Public Transport Management Centre (CITRAM). CITRAM coordinates the information on infrastructure and services of different modes of transport that operate in the region of Madrid. Focused on real time information, the centre manages the status of public transport as a whole and provides a coordinated, integrated response to all public transport stakeholders (customers, transport operators, emergency services etc.). Using CITRAM, the Madrid Region Organising Authority is able to make decisions faster and more effectively when coordinating the operation of the entire transport system.

The demonstration consisted of four scenarios. In all scenarios information systems played a vital role: cooperation should improve with the help from an interoperable incident management tool, a CCTV system and communication between control centres in case of incidents.

The first scenario tested procedures and legacy technologies. The second scenario tested how an incident management system (GEIS) and a geographical information system (SGRAF) would allow interoperability among different stakeholders like PTA, PTO, IMs, emergency services etc. Specific PIS (SGIP) was applied. In the third scenario an intermodal CCTV was added to the second scenario, thus testing the efficiency of decision-making procedures. Also here specific PIS (SGIP) was applied. The fourth scenario tested the interoperability between CCTV on board and the PTA in the specific cases of night buses.

The three first scenarios were planned in two different sessions. The first session aimed at showing how different stakeholders should react in case of incidents, while the aim of the second was to explain all technological aspects about scenarios 1, 2 and 3.

The first session took place at Moncloa interchange and its surroundings. A bus was 'set on fire by terrorists', and it caused collapse of the main access to the interchange. Some passengers were injured and in need for medical attention, while other passengers who were

not injured still had to be evacuated. Dealing with this meant that stakeholders had to be informed, passengers had to get medical assistance and / or be evacuated, and other buses and underground lines had to be directed away from the interchange and to a temporary substitution 'interchange'. The passengers were informed by this on screens at stops and on buses. The actions were in accordance with CITRAM Rolling Stock Procedures, Communications Network Procedure and Emergency Service Procedure.

The fourth scenario, aiming at enhancing the cooperation between stakeholders in case of common incidents, was divided into two sub scenarios. The incident in sub scenario one was a robbery in a shopping area at the interchange. More precisely, a passenger was waiting in line in order to buy ticket, when a stranger passed by and grabbed her wallet from her purse. The passenger was alerted by another passenger who saw what happened, and they alerted an employee who in turn notified a security officer. The Emergency Procedure was activated and the control centre at the interchange notified the Municipal Police and CITRAM. As the robber got on an EMT bus, CITRAM informed EMT's CRA, who activated the alarm. When the bus was located, the protocol with the Municipal Police was activated. The Police met the bus, the bus stopped and the police detained the robber.

The incident in sub scenario two was vandalism in an EMT urban bus line in the Plaza de Castilla Interchange. A small group of passengers started to vandalize and harass other passengers. The bus driver activated an alarm that warned both the EMT Control Centre and CITRAM. The Municipal Police got a notice from the EMT Control Centre. When the bus was located, the police was notified again. CITRAM informed the Interchange Control Centre, who supports the Municipal Police. When the disturbers left the bus at the interchange, the interchange was warned by CITRAM. The interchange tracked the disturbers and informed the police about their locations.

The demonstration is described in detail in the demo description (SCR-WP42-D-CTM-002-06-D42.1 Detailed description for Madrid demo).

Privacy, societal and ethical issues

Like for the other demonstrations, an ethical review checklist was filled in as a part of the preparation of the demonstration. For the Madrid demonstration, the questions about risks were reported to be 'unlikely', that is, not relevant, as all the participants were actors. The participants being actors was also reported as a reason that it was not necessary with an informed consent. Still, the demonstration was handled according to Spanish law. Among others, that involved explaining which organisation was responsible for implementing the measure(s) and / or the documentation, that participation was voluntary and that CCTV images were processed according to EU directives and Spanish Law.

The AG Ethical pointed at two specific issues met with the Madrid demonstration, concerning 1) the respect of privacy and fundamental rights while using CCTV (fixed and on-board), and 2) the respect of the rights of employees and actors / volunteers that take part in the demonstration as participants. Both issues were handled according to law. The demonstration was notified to the Spanish data protection authority (AEPD), which oversees and guarantees the fundamental rights of citizens regarding their personal data. The mentioned issues were also discussed in AG Ethical meetings, where the Madrid demonstration was represented with one ethical contact and one independent ethical expert from the Madrid Data Protection Agency.

Privacy, societal and ethical issues in regard to the Madrid demonstration have been discussed, in particular at AG Ethical meeting #. Madrid responses suggested all participants to be 'actors' and this precluded risk assessment. AG advised that even if participants are 'actors' risk still needs to be assessed and addressed. In fact, participants will be staff 'volunteers' and unknown passengers. There was discussion on ensuring that the staff could genuinely volunteer, that no undue pressure to participate would be placed on them. There was need for clarification of the unknown passengers. In all cases the need for fully informed consent was clarified as was the need for protection for the collection and holding of personal data. There was also discussion on the nature of the 'public space' to be observed and the form consenting could then take..

5.2.3 The Milan demonstration

Aim and scenarios

The Milan demonstration aimed at improving security operations. That involves monitoring threats and protecting vehicles in depot, improved reaction and event management and improved procedural coordination of stakeholders. It was organized in four scenarios. Scenario 1 tested capacities for tracking persons. A person at Pagano station was seen as behaving suspiciously. The person bought a ticket to the airport. He went by the underground to Cadorna station, from where he took the train to the airport. The capacities involved were CCTV analogue tracking, video analytics tracking, ticketing system, RFID sensors and CBRNE sensors. These were integrated in a security operation control centre (SOCC).

Scenario 2 tested the following capacities: thermal and PTZ cameras, intrusion detection and PTZ auto tracking, on-board empty vehicle detection and CBRNE sensors. Like for scenario 1, the capacities were integrated in a security operation control centre.

The scenario was divided in two parts. The first part dealt with an intruder at a train entering the depot. He made a graffito and left an unknown device on the external body of the train. He tried to run away, but was stopped by security guards who were able to locate him due to different sensors in the depot. An integrity check, made by R sensors, identified the unknown device and the train was moved on a dead track and security procedures started. The second part of the scenario dealt with an intruder climbing over the fence into the depot area. The intruder was detected by a perimeter protection system, consisting of thermal cameras equipped with video analysis and positioned around the entire perimeter of the depot. Security guards were alerted and went to the place where the intruder was located. The intruder headed towards the train, noticed first by the PTZ cameras and then by thermal cameras. Security guards were guided by the SOCC to the intruder.

Scenario 3 aimed at improving efficiency in rescue operations by coordinating all activities and actors though a control system. What happened was that a train stopped in a tunnel just after leaving the station of Abbiategrasso. Smoke filled the tunnel and the driver was unable to reach the station. First responders were contacted and the train, the tunnel and the station had to be evacuated. The driver sent an alarm through a mobile application to the control centre and then he got the passengers off one by one, walking towards the station. Two passengers became ill and collapsed to the ground causing crowding. More people became ill and also panicked.

The capacities involved were evacuation modelling, crowd movement detection, emergency light paths and QR code information for First responders. The capacities were integrated in a security operation control centre.

Scenario 4 aimed at demonstrating the possible visualization and coordination of local procedures of different stakeholders through the implementation of a local System of Systems in Milan area. Focus is on a global OCC that coordinates, exchanges information and integrates systems with all other local ones. The OCC will be the SECUR-ED control centre. The scenario summed up the previous three, meaning that it involved the capacities in all three.

Privacy, societal and ethical issues

During the planning of the demonstration, the AG Ethical pointed at ethical issues found in scenario 1, which addresses the tracking of a person exhibiting suspicious behaviour in the PT network. Initially, tracking was planned using Bluetooth and Wi-Fi (in addition to CCTV and RFID), but that was rejected because of the risk of infringing the legislation concerning privacy and personal data protection. ATM filed a request to the Italian privacy authorities to perform the demonstration, and the privacy authorities then stated that showing video sequences of passengers in public required a written consent. Otherwise, all faces should be masked. The latter was done in the demonstration video. Further on, the privacy authorities stated that video tracking, as other investigation activities, shall be performed only upon a judicial decision. A real-time tracking on live picture flows did not correspond to an authorised usage of the technology in the current state of legislation. Still, permission was given to test the capacities in the scenario. In the ethical review checklist, ATM stated how data would be made accessible to data subjects and otherwise secured, as required by law.

As the demonstration took place, all people that during all the tests or demonstration had access to the depot, were made aware of the risks present in the workplace. This was done through a specific document named ‘Report on workplace risks’, which was read and signed by all people in the demo. All partners involved in scenario 2 were appointed ‘Responsible of Privacy’. For scenario 1 and 3, the persons who were recorded in the demo video had to sign a release to show their face and, since the station was closed to public, all the people involved in the event have been required to sign it. The persons who recorded the demo video first signed the document authorizing their image utilization in accordance with ethics rules. The ticket seller and the suspect in scenario 1 were actors. All others present were masked in the video, following privacy rules on the request of the Data Protection Authority. Participants were wearing a high visibility life vest.

After the demo its results have been documented in D44.5 Consolidated results for Milan demonstration. Chapter 8.5 in that report presents what is called ‘Ethical results’. The first part of the chapter looks at possible impact from the capacities on fundamental human rights and / or citizens civil liberties. The comments point at the use of fixed basic CCTV as regulated by law. That is also the case for person tracking in video. For both the ethical aspects are not specified, but are said to be the same as for the legacy CCTV. Regarding the ticketing system and the RFID ticket tracking, it is commented that passengers, in a hypothetical application, must be aware of the activities of tracking. For chemical, explosive and radiological detection, persons must be aware of the scanning by the sensors; how they work and why.

For several of the capacities no particular ethical aspects are seen. The evacuation modelling is said to have no impacts on ethical aspects since it is a simulation. The comment on the QR code information to first responders stated that the QR coded information cannot be read without the required tool, which means that personal data are protected.

The second part of chapter 8.5 deals with privacy and personal data protection issues. Several comments concern information; citizens must be aware that they can be tracked, scanned, or recorded, and that the information is stored according to law. Possible privacy issues are noted when a ticket is associated to a person.

The third part of chapter 8.5 deals with acceptability from society at local and wider level. Good acceptability is expected for fixed based CCTV, while it may be problematic when it comes to ticketing systems and RFID ticket training. For the chemical and explosive, radiological and crowd detection no particular problems of acceptability is expected. For chemical and explosive and radiological detection, this is explained by the improved perceived security and that it does not require passengers' time. For the same reasons it is assumed to have positive impact on the use of mass transit systems.

5.2.4 The Paris demonstration

Aim and scenarios

The Paris demonstration addresses a wide range of security challenges, from major threats such as terrorism, to the everyday security situation such as theft, aggression, traffic, etc. The demonstration tests capacities that respond to the daily security challenges such as panic and the safety of passengers in case of major incidents. The aim of the capacities tested is to ensure minimal impact on the existing urban transport system (service performances, freedom of movement, privacy, etc.) and to take into account the specific environment.

The scenarios dealt with different attacks. While the cyber-attack is directed at critical network and IT systems, the other attacks are directed at interchange nodes. The attacks are connected to each other as the first is a preparation for the others. The demonstration involves both operational and technology capacities that first detect the threat and then support emergency procedures. The latter involves informing passengers, crisis management, and the function of a security organisation

Scenario 1 simulated a cyber-attack aiming at make staff lose confidence in the information displayed by the PIS; display a fake event on social networks in order to encourage passengers to travel to a specific location; display wrong information on the PIS of a Large Multimodal Hub, claim attacks on PIS and social networks etc, and make the video surveillance system of Large Multimodal Hub unusable. What happened was that a person entered a data room in the RATP infrastructure and by the use of stolen passwords he infiltrated a malware which gave free access to the passenger information system (PIS) and CCTV system. A communication module made him able to remotely control the system via his smartphone and for example display wrong messages on the screens of the PIS network.

Scenario 1 is supposed to create panic and disorganization. By that, it prepared the ground for scenario 2, toxic attack and 3, radiological attack. In scenario 2 the perpetrator entered metro line 1 and abandoned a parcel which contained a bomb that would spread Toxic Industrial Material (TIM) gas. The primary objective is to kill and harm people. Scenario 3, the radiological attack, took place at the same time. While the perpetrator in scenario 2 left his

parcel on the station platform, the perpetrator in scenario 3 entered the infrastructure via an entrance dedicated to technical staff and infiltrated the targeted station's technical area. He then entered the ventilation plant where he left a parcel containing an IRD (Improvised Radiological Device) filled with radioactive material that would be released through the working ventilator. The IRD was remotely activated and the perpetrator escaped via the suburban network.

Scenario 4 consists of video tracking, and it is the perpetrators from scenario 2 and 3 that are tracked. The first perpetrator escaped via a metro line, got off at an interchange and took the train to Luxembourg. There he left the station and returned to BFM by bus. The second perpetrator escaped by a suburban line to Paris Saint-Lazare railway station, which he left and then walked to the metro station interchange area and took another metro line to BFM. The aim of the scenario was to track previously identified individuals and investigate, hypothesise their next actions and apprehend him / her before successful escape or further actions were taken.

Scenario 5, explosive attack, builds on the previous scenarios. The two perpetrators from scenario 2 and 3 travelled to BFM using each their way. They are carrying two explosive devices ready to be blown: an explosive belt and an IED (Improvised Explosive Device). BFM is on red code security, which means that security controls have been installed and teams of security agents with dogs are patrolling the station.

The demonstration is further described in D43.1 Detailed Scenarios for Paris Demonstration.

Privacy, societal and ethical issues

A chapter in the report deals with laws and directives that ensure ethics and privacy. The chapter states what has been done in order to make the demonstration in accordance with legislation. The report chapter refers to French law and European decrees and states all legal and ethical requirements were taken into account and complied with. In addition, an ethical code is followed, reminding every employee and RATP partners about their respective rights and duties; a TIC (Technologies of Information and Communication) chart is used, specifying the rights, duties and responsibilities of every user of RATP communication and IT tools; and a GSM chart is used, specifying the characteristics of each RATP professional mobile and office phone. All employees of the RATP Group review the code and charts in order to ensure that they are understood and respected.

According to the AG Ethical (D01.8 Ethical Management report (Period 2)), a specific issue met with the Paris demonstration was the use of the CCTV tracking feature. The issue is dealt with in the following way: RATP security officers and law enforcement representatives will be re-located in a single control room to coordinate a security response, the tracked persons shall be actors and selected by law enforcement representatives at the operational control centre (OCC).

Another adjustment was installation of new cameras. The cameras already in use were designed for transport operations only, and to use them for the purpose of tracking persons would have violated the rules.

A computerised video tracking system was planned. The system should make possible automatically recognising of people similar to criminals. Practical reasons made this difficult, and a semi-automatic system was therefore implemented. This system was able to follow a person on a route covered via several CCTV cameras, after the person first was designated on a screen along the route.

5.2.5 Bergen satellite demo

Aim and scenarios

The Bergen satellite demonstration aimed at improving how members of the staff, mainly drivers, deal with threats. The capacities in use were training capacities, developed in the Berlin demonstration and then translated to Norwegian. The training took place in the company running the city light rail in Bergen.

Three courses were given over two days, mixing classroom lessons and field lessons. These were:

Lesson 1.3 Dealing with daily security threats Lesson

Lesson 3.3 Identifying & handling suspicious item (« NO TOUCH »-protocol)

Lesson 6.2 the operational work of security staff – field test

Lesson 3.1c - Basic awareness – front line staff

The courses were mainly chosen based on a risk assessment that showed lack of awareness and challenges related to daily threats. Examples of such threats were drunk and drugged passengers, passenger littering, vandalism, pickpockets and aggressive behaviour among others. Terrorism was not considered a threat, yet the training involved the NO TOUCH-protocol. This was due to SECUR-ED personnel highly recommending it. The demo participants would have preferred more lessons on conflict negotiation.

The demo was not built as a scenario. However, the training included practicing two situations. The first situation was to make a drunken passenger exit the train when refusing to leave at the final stop. The second situation was to handle a suspicious item left at the train. The classroom training involved talking about these threats and reflecting both on how to deal with them and how probable they were. The content of the capacity focusing on every day threats were regarded highly relevant.

Privacy, societal and ethical issues

The documentation of the Bergen demonstration does not involve an ethical review checklist or a demonstration report (at the point of time this is being written). The following discussion is therefore based on observation at day 1 of the demonstration. Besides, as this demonstration is partly a replication of the Berlin demonstration, some of the privacy, societal and ethical issues are covered there. An important issue in Berlin was about recording participants during the training. Recording was planned, but it was decided not to do it and instead use pre-recorded clips of actors. It was done likewise in Bergen, that is, there was no recording of participants.

As already mentioned, the focus on every day threats were regarded highly relevant. The relevance was confirmed by the fact that examples (of threats) presented by the instructor were recognizable to the participants, who had no problem suggesting other examples. The content of the capacity focusing on terrorism (NO-TOUCH) did not seem to be relevant, as Bergen is a small and peaceful town and the risk for terrorism must be very small. Also the participants said that. Despite that, they appreciated it as part of the course, because, as it

was said: ‘you’ll never know’. It was also pointed out that the risk of sabotage is probably higher and would therefore be a more relevant topic than terrorism.

5.2.6 Lisbon satellite demo

Aim and capacities

The aim of the Lisbon demonstration was to improve the dealing with threats as graffiti, crowd panic, stoning and abandoned luggage in altogether four scenarios. Graffiti is a problem as it might reduce the experience of travelling, and besides involves huge costs for the owner of the vehicles.

One scenario consisted of intruders making graffiti. While a woman distracted the security guard, other persons enter. The intruder and perimeter detections system triggers an alarm on the control centre, which in turn alerts the rest of the system (security guards). The security officers confirmed the presence and activities of the graffiti performers, and, communicating with the control centre, requested police support. The control centre contacted the police, who arrived and detained the intruders.

Another scenario consisted of a gang robbing passengers. As the gang entered, security staff informed the control centre. Staff in the vehicles informed the control centre via mobile phone. For passengers, a special app is developed in order to make it possible for them to inform the control centre about threats.

A third scenario tested capacities for detecting and handling abnormal crowd movements at station. The crowd could grow as passengers arrived from trains, metro, ferry, buses and taxis. Imagining the crowds are hooligans, there was a risk of clashes between groups of supporters. Also capacities for detecting explosive materials in the trains and among the football fans were tested. Both events are about early detection of risk scenarios: clashes between fans, related acts of vandalism or attacks between groups of fans using dangerous materials. This scenario involved CCTV, crowd detection programs, and communication systems. The most important thing is to ensure fast communications and coordination.

A fourth scenario dealt with abandoned luggage. The luggage contains a device that triggers the explosive detection system, alarming the control centre. The Police is notified, and they isolate the area and make a secure perimeter. They find the suspicious luggage, and by the use of a sensor system it is confirmed that it contains explosive. It turns out that it is fairy lights and fireworks.

Privacy, societal and ethical issues

In the ethical review checklist for the Lisbon demonstration, no specific privacy, societal or ethical issues were pointed out as problematic. An informed consent was to be used. Personal data were not retained, and the data retention policy is in accordance with the law. The data protection authorities were involved. To the question if the demonstration involved automated processing off data that could lead to direct or indirect identification of individuals, the answer stated that the recorded images would not be linked to other systems and could therefore not be used for direct identification. Indirect identification was possible and could happen in accordance with the law. The images were not meant to identify individuals. Confidentiality was guaranteed.

Still, the demonstration made use of capacities that clearly involved privacy, societal and ethical issues. However, not much of the discussion specific for Lisbon is documented, and we will therefore discuss it at a general level in Chapter 7.

5.3 Summing up demonstrations and tools, processes and systems

The demonstrations are summarised in the table below for the analyses to be made in Chapter 6. In the table the large number of tools, processes and systems deployed in the project are summarised under eight functions.

Table 5.6 Functions in the demonstrations

Demos	Madrid	Paris	Milan	Berlin	Lisbon	Bergen
Functions						
Information management	X	X	X		X	
Video analytics	X	X	X		X	
CBRNE sensors		X	X		X	
Cyber defence (mass transport critical systems)		X			X	
Training and preparedness	X			X		X
Protection of non-public spaces			X		X	
Apps as info receivers		X				
RFID, apps and other new info sources			X			

The table shows that the Paris and Milan demos – together with satellite Lisbon –worked with the widest scope of functions. Berlin and Bergen both have a singular focus on training and preparedness, which was not part of the other three mentioned demos. Madrid can be described as taking an intermediate position both with regard to number of functions and in including training as one of them.

The novelty of mobile apps features in two of the functions. This is because apps can serve both as info source, such that people report security relevant observations, and as info receiver, where security info is transferred e.g. to apps in the phones of PT staff.

6 Analysis of problem areas identified in connection with security relevant functions in the demos

In the present chapter we perform the main task of D46.6 as identified in the DoW, viz. to consolidate knowledge on the societal aspects related to the use of the technologies, systems and procedures tested during the demonstration experiments (cf. Chapter 3). Both to more specifically identify topics of potential such relevance, and subsequently to analyse them more in-depth, we first need to operationalize the DoW task in terms of societal and ethical issues. This is done in Section 6.2.1. Then based on this understanding of the report's main theme, in Section 6.2.2 we translate the functions identified in Section 5.3 into problem areas. Then follow a sequence of sections each analysing a problem area in terms of the identified societal and ethical issues.

6.1 Framework for analysis

6.1.1 Defining societal and ethical issues for analysis of the demo results

A first question is then how the first bullet in the DoW (see Section 3.1), impact on human rights, relates to the following three. In the human rights domain, as discussed in Section 4.1.2 there exist legally binding provisions within UN, The Council of Europe, and EU. The right to privacy or private life appears at all these levels, clearly underscoring the importance of the second DoW bullet. The EU provisions also explicitly mention protection of personal data, which we elect to see as part of privacy.

Another area has to do with access to public transport of different groups. One example is the rights of people with disabilities discussed in Section 4.2.1. We summarise these concerns under 'access to mass transport for all groups'.

In our judgment this exhausts the problem areas where human rights and mass transport overlap with sufficient frequency to merit inclusion in our analysis model.

Based on the above review and a task internal workshop we decided to operate with the following list of social/ethical issues in our analysis model:

- impact on privacy (incl. data protection)
- access to mass transport for all groups
- impact on use of mass transport
- consent
- risks for violation of proportionality
    - illusory security trap
    - slippery slope
    - function creep
        - example: capabilities in combination, data fusion – 1+1=3
        - example: automated analysis
- Synergies including securitisation.

The first two items have already been discussed in connection with human rights.

The content of the third issue is that, on the one hand (perceived) insecurity, on the other negative effects of security systems (e.g. perceived invasion of privacy) may cause people to abstain from public transport. This in turn is likely to have detrimental effects on social welfare and sustainability when people have to choose among other modes of transportation.

Consent, which should be informed and voluntary, is an important prerequisite, e.g., for collecting personal information in many settings.

According to the list the risks for violation of proportionality presents a multi-faceted issue area. The core meaning of proportionality, as discussed in Section 4.1.2 for privacy but here applied for all types of impact, is that the generalised costs, e.g. in terms of invasion of privacy or limited access for certain groups, for a security measure should be proportionate to the gains.

Debates on proportionality seldom reach complete unanimity, and the first example – illusory security trap – could provide a good example. Let us consider aviation security with regard to passenger screening, even though such mass screening approaches are patently untenable in a mass transport setting. The counter argument then goes that very few terrorists are discovered, while the costs in terms of privacy, waiting time, and direct operational cost are immense. The counter-counter argument goes, however, that in the absence of these measures, many terrorist attacks would have been levelled at civil aviation, which are now deterred by the security measures.

The meaning of 'slippery slope' is that acceptance of, e.g., one invasion of privacy may lead to other invasions being seen as logical given the first.

Function creep means that a capability motivated by one task once in place gets used in other ways as well. Data fusion and other forms of automated analysis have a potential for function creep since additional capabilities can be realised at low cost; many types of data are already brought together and additional analysis can be performed without hiring and training additional staff as would be the case if the analyses were made manually.

Function creep is also related to the final issue area: synergies including securitisation. Securitisation means that security is used to motivate measures where the real motive is at least partly something else. For example, better entrance controls can be motivated by security while avoiding financial losses by preventing people from entering without a valid ticket may be the real reason. But conversely security-relevant capabilities may also be 'sold' with non-security arguments. This is when proportionality threatening function creep may occur. This said, exploiting synergies – also involving security – is fundamentally a sound and essential economic principle.

6.1.2 From functions to problem areas

In Section 5.3 we summarised the technologies, systems and procedures tested during the demonstration experiments under eight functions, However, going directly from functions to social/ethical issues turned out not to provide a sufficiently sharp focus for analysis, since a function can play different roles in different contexts. Therefore, again building on WP54 experience, we bundled functions into *problem areas* as shown in Table 6.1. In the table, **X** denotes the core function for the problem area – we found these to be unique; x are supporting or in other ways related as explained in what follows. Video analytics features in as many as four of the problem areas; this indicates that analysing this at function level is particularly difficult, different problem areas pulling the function in different directions.

Table 6.1 What problem areas arise from what functions? (**X** = core function for problem area)

Problem areas	Big Data	Detection and tracking of individuals	Decentralisation of security information	Protection of non-public spaces	Training and preparedness
Functions					
Information management	**X**		x		
Video analytics	x	**X**	x	x	
CBRNE sensors		x			
Cyber defence (mass transport critical systems)			x	x	
Training (preparedness)					**X**
Protection of non-public spaces				**X**	
Apps as info receivers			**X**		
RFID, apps and other new info sources	x	x			

Given the limited interaction with other functions already noted for training and preparedness, in this case analysis at function level presents no particular problems. In Table 6.1 we apply the term problem area to that function for the sole reason of being able to pursue the whole analysis in problem area terminology. .

Also in the case of protection of non-public spaces we let the same phrase denote a function and a problem area. Here, however, the problem area involves two functions in addition to the like-named one. Hence, here the function protection of non-public spaces is distinct from the problem area with the same name.

In the following sections each problem area will be analysed in terms of the key ethical/societal issues identified in Section 6.1.1. Table 6.2 provides an overview of these analyses. A brief summary is provided in Section 6.7.

Table 6.2 Societal issues per problem area as discussed in text (**X** = identified as most important issues)

Problem areas **Societal/ethical issues**	Big Data	Detection and tracking of individuals	Decentralisation of security information	Protection of non-public spaces	Training and preparedness
Privacy (incl. data protection)	**X**	**X**	x	x	
Access for all groups	x	x			x
Consent	x				
Impact on use		x			
Proportionality - illusory security		x			
- slippery slope	**X**		x		
- function creep	**X**				
Synergies incl. securitisation	x		x		

6.2 Big Data

One recurring aspect in the capacities used in the demonstrations is gathering or recording of information connected to individuals and their movements, by different means. Large amounts of data can be gathered as a result of some of the functions involved in SECUR-ED, in particular video and new information sources like RFID (as smart tickets), smart phones and other ICT devices. The core function is, however, information management, the ability to make use of these huge amounts of data.

The use of, and dependence on, information and communication technologies is increasing, in public transport as for the rest of society. A common characteristic of these technologies is that they register and store personal information. The result is enormous amounts of data. The concept of 'Big Data' refers to a sort of exploitation of large bodies of data that is not possible when working with smaller data sets. This is done by combining the power of modern computing with the plentiful data of the digital era. This gives knowledge that makes us more capable of solving a lot of problems. Digital Agenda for Europe underline the need to make use of big data, and claim that it will lead to innovations in technology, development of new tools and new skills.[4] Opportunities exist in every field of society. Big data can be used at different levels: governments can use big data for traffic controlling, transport planning and modelling, route planning, congestion management, and intelligent transport

[4] https://ec.europa.eu/digital-agenda/en/making-big-data-work-europe-0

systems; operators can use it for route planning and logistics, transport management, and individuals can use big data for route planning.

Despite numerous benefits, a central objection to big data is that although it is very good at detecting correlations, especially subtle correlations that an analysis of smaller data sets might miss, it cannot tell if the correlation is meaningful (Marcus and Davies in New York Times April 6, 2014). There is also a risk of too many correlations. A thorough examination of sufficiently much big data will show significant correlations between many pairs of variables, even though there are no actual meaningful connections. Another objection against big data is that it '… is prone to giving scientific-sounding solutions to hopelessly imprecise questions.' (ibid.)

Big data is made of pieces of information put together. While each piece can document innocent and legitimate behaviour, put together the data can mistakenly indicate evil intentions. From time to time newspapers report stories about the police paying visits to individuals and / or families who appear as terrorists because of an Internet search.

Here consent is important in some cases: providers of services based on information technology sometimes require that the customers approve the sharing of personal information in order to be able to use the service fully. Smart phone applications are one example. One could argue that there are similarities between this and emerging features of public transportation in that the customer/passenger has to give consent to the demands of the service providers in order to be granted access to certain services. Personal registration of smart tickets to be able to cancel and recover the ticket value if lost is a case in point. This comparison is however not necessarily fully relevant, as we are dealing with private companies on competitive markets on one hand and public transport (PT) on the other and it is reasonable to assume that the public perception on demanded consent could differ if between the cases.

We note that the possibility to use data for ever new purposes can be tempting as means to pursue other goals, these can very well be outside the security area with traffic surveys one obvious case in point, hence exemplifying synergies emerging from the non-security side. In society at large Big Data is mainly driven by commercial interests and slippery slope type phenomena may increase the acceptance for new uses in public transport previously seen as threatening privacy. Once in place in public transport proportionality is threatened in particular due to function creep supported by the ability to combine different types of data by means of automated analysis.

Combining video and RFID or smart phone information enables linking a photographic image to other information, possibly – but not for sure since smartphones and smart-tickets may be anonymous or linked to another individual than the one carrying them – allowing identification, which then means that additional data from other sources can be invoked.

Currently the general public seems very accepting of Big Data developments. Hence the risk for such developments in PT systems negatively affecting use at large seems small. Speculatively, however, it is imaginable that a group of 'dataphobes' may emerge, who will feel unable to use PT if Big Data is utilised there. Conversely Big Data developments as defined here are not likely to make people feel safer in PT systems, since we are not including real time surveillance (cf. below). Hence Big Data is not likely to increase PT use in any group.

Arguably the most clear positive security effect of Big Data developments in PT is in forensics. Improving the forensic capabilities in PT scenarios is of course very valuable, but

Big Data based forensics is also likely to lead to false positive problems of the type mentioned above, where innocent people are found to display suspicious patterns.

A special problem with Big Data is the criteria used for singling out people (or other objects like containers) for closer inspection, which could, e.g., amount to ethnic profiling. This problem is more relevant in aviation and border security than in mass transport where the concept of closer inspection is hard to reconcile with the operational logic and where background information on travellers, if at all existing, e.g., due to personalised smart tickets, will be easy and not illegal to fake. Still this needs to be kept in mind also there.

6.3 Detection and tracking of individuals

Detection and tracking of individuals is a real time affair. Automated video analysis capacities have in some cases person tracking features. RFID poses a new generation of possible issues, different from video surveillance. The passengers would be tracked in their positions wherever identifiers are installed. Smartphones etc. have similar features but can of course be turned off. The scope for bringing even more information sources to bear is discussed under Big Data.

There is no restriction in the capacity the operators have when following such sources, while in the case of video surveillance and automated video analysis, as shown in the demos, operators still have to trigger the automated surveillance. Also RFID tracking is legally less regulated than automated video tracking.

The cross for CBRNE sensors in Table 6.1 is motivated by the non-demonstrated possibility of connecting C, E or R detection to tracking, viz. such that persons detected as suspects of carrying hazardous materials are tracked.

Tracking in real time is obviously a very privacy intruding practice. As noticed, new info sources may present legally unregulated possibilities. But slippery slope and function creep type risks for violation of privacy are less pronounced than in the case of Big Data since tracking in real time must be the result of a clear decision, manual or – theoretically – automated, which however would require explicit criteria to be formulated. The risk for ethnic profiling type practices mentioned is connection with Big Data is more realistic in connection with automated tracking, where skin colour could be a variable featuring in the decision to employ such practice. Synergy type issues do not seem likely since automated tracking of individuals is a specific capability of little relevance outside of security.

It is hard to see how automated tracking could cause significant groups of potential PT travellers to choose another alternative. For the putative ‘dataphobes’ automated real time tracking capabilities might, however, be even more disturbing than non-real time Big Data practices. On the other hand well-publicised automated real time tracking might increase the perception of security, even to the degree of illusory security.

CCTV person tracking in video raises legal social and ethical concerns, mainly regarding privacy. Two key issues that must be clarified are decision criteria and power to track persons and access to such information.

6.4 Decentralisation of security information

Decentralisation of security information can be enabled by smartphones and supported by information management. Video information supported by video analytics is a relevant type of content.

It is natural to see this as part of a broader tendency to decentralise information, thereby empowering front line employees. This could entail elements of slippery slope/synergies type. Arguably the step from traffic to security information is quite distinct, but it is possible to imagine how employees will demand more and more useful information.

There are also many advantages of such a development. However, it is important that employees are properly trained to use such information. The type of information available through smartphone in a PT system is not likely to be very privacy invading unless combined with Big Data or individual tracking capabilities as discussed above. Still it is important to include also ethical aspects in the training.

A quite problematic aspect on decentralisation is the risk that sensitive information gets into wrong hands – either via cyber-attack (hence motivating the cross for cyber defence in Table 6.1) or by stealing or simply finding a smartphone with the (in)appropriate app.

On the whole decentralisation of security information should be a quite manageable problem with proper risk analyses and measures like cyber security and staff training.

6.5 Protection of non-public spaces

Non-public spaces, e.g. depots and metro tunnels, are relatively unproblematic since uninvited members of the public present there are by definition trespassers. In Table 6.1 this area features both as a function and a problem area. The other functions marked in the table are video analytics, for fairly obvious reasons, and cyber defence, which is included since one of the demos included a scenario where access to a non-public space was a prerequisite for a cyber-attack; admittedly not a very generic argument for a cross in Table 6.1. It can be mentioned that other sensors than video, e.g. radar, can be of relevance for premises with few legitimate visitors.

Protection of non-public spaces raises few social/ethical issues. But of course privacy, e.g., of people trespassing by mistake, is relevant here too. And of course also the privacy of PT employees needs consideration.

6.6 Training and preparedness

Training and preparedness is even less problematic than protection of non-public spaces. It should however be pointed out that training has a key role in ascertaining access for all groups to PT, in the present context with regard to their needs and sensitivities with respect to security measures. Should security training fail to properly address this aspect, then it becomes a problem.

6.7 Summary

Big Data and detection as well as tracking of individuals may lead to considerable invasion of privacy. Big Data by being closely related to broad societal trends carries particular risks for violation of proportionality. The other problem areas according to the above analysis can be characterised as manageable. In terms of the societal/ethical issues identified in Section 6.1.1 the most problematic ones are privacy and the two risks for violation of proportionality referred to as slippery slope and function creep.

7 Other lessons learned from the demos – and beyond

This final chapter summarises some insights in addition to the demo-based problem area analyses in Chapter 6 focusing on the demonstrated capacities. The insights reported in Chapter 7 are inspired by other types of demo experience, as reported in Section 5.2, but enriched by the literature in the field as reviewed in Chapter 4. While Chapter 6 reports on the effects of developments enabled by emerging technologies, Chapter 7 rather deals with the insights gained in SECUR-ED on the 'eternal questions' of the field (though admittedly Section 7.3 could have been alternatively placed in Chapter 6).

One strand in the chapter deals with experimentation related issues, e.g. ethical concerns regarding actors taking part, and it ends with a tentative suggestion for best practice for ethical and societal aspects in future large-scale experimentation and demonstration projects.

7.1 Data security

Data security is an issue relevant for all demonstrations. However, data security is ensured by regulations on how it should be processed and stored, and for how long. That is, the capture, access to and distribution of recorded images has to be organized in line with legal requirements for privacy and data protection. The demonstrations did that. Experts and authorities were involved. For PTO's, with limited resources, it can probably be hard to sort out what requirements exist.

Discussions about data security tend to focus on storing, that is, for how long data can be kept. As important, however, is the question about access. Privacy is about knowledge (Burgess 2008), therefore it is also about access to information. First, it should be made clear who has access to the information. In addition, it should also be stated who makes decisions about who has access, and who controls them.

7.2 Privacy, societal and ethical aspects – who do they concern?

As already said, when the Madrid demonstration filled in the ethical review checklist they reported that some of the questions were irrelevant because the participants were actors. This makes us ask: Should the same rules be applied on everybody? Or are there different rules for actors than for ordinary people? Some of the demonstrations involved employees. From Berlin we know that when trade unions got involved in the training programs, they first protested against them. This reminds us that also employees are affected by security capacities. We can therefore ask if the rules also apply for them. Based on this, we can ask: are the rules the same for all groups involved? At least three groups of individuals are relevant to pay attention to. That is

- employees
- actors taking part in research
- the public

We discuss this in regard to the concept of consent. The discussion will be continued in Section 7.4. *Employees* have a contract with the employer. No matter how detailed the contract is, most probably it does not cover all aspects of the work life of the employee. Variations can be found depending on type of work and other factors. Some positions require for example a declaration of confidentiality, while others do not. It is reasonable to believe that in most cases, only a few aspects are made explicit. A lot of expectations concerning tasks, relations and behaviour are left to be implicit. The basic assumption is that by signing a work contract, you accept to some degree the company's policy. However, it is not clear how comprehensive this acceptance is. An important question is: Can the work contract be regarded as a free, valid and informed consent? That means: Has an employee already accepted the employer's use of his / her personal data? This was hardly debated earlier, but today the use of personal data in work life has increased. The purposes are many, like for example security, marketing, efficiency, control etc. Sometimes data on goods or vehicles end up as personal information. That is the case for example for transporters, who when monitoring their cars end up also tracking persons, due to the common practice among drivers as being likely to drive the same car day after day.

Here, the most relevant issue is surveillance. Surveillance can violate privacy, and the use of cameras is therefore regulated by law. It is the duty of the one in charge of the surveillance (here: the employer) to operate according to the rules. A general rule is that surveillance on the workplace is only allowed when it is necessary in order to prevent and reveal crimes or to protect life and health. Shops and offshore oil platforms are examples of workplaces were surveillance is allowed. Still, there are limitations: the camera shall not be directed at the individual employee, and it shall not be used in areas where the employees withdraw from work, for examples where employees have lunch. However, it can be difficult to decide when surveillance is necessary. Questions to be discussed are: What is the risk of the occurrence of the specific crime? To what extent and in which ways will cameras help?

The principle of proportionality might help to decide when surveillance is necessary. We will discuss that later, as that principle counts in all cases, independent of who (which groups) are being surveyed.

When it comes to *actors*, it is a question whether or not they are to be considered as employees or as participants in a research project. Normally, employees are paid while participants in research project are often not. For both employees and participants an informed consent is required. But unlike employees, participants in research projects can withdraw their consent at any time, without giving any reasons. It is important to note that using actors or volunteers does not make questions about consent, risks etc. irrelevant.

When discussing privacy issues in regard to security in public transport, the concerns most often relate to the travellers. It is their rights and attitudes that are in focus. They do not necessarily give a written consent. Again, it can be questioned what should count as a consent. A general view is that if an individual knows that an area is surveyed, he or she gives consent to surveillance when voluntarily entering the area. Publicly available information on the presence of surveillance is therefore important. It is also important to have an option to enter or not.

7.3 Individualized security information to passengers

SECUR-ED partners asked the AG Ethical to comment on the ethical and societal aspects linked to a dedicated passenger information system that would provide individualized security information to passengers in case of emergency. It was suggested to develop such a system, and even though SECUR-ED decided not to do it, the partners still wanted to know if doing it would be legal and ethical, and if so, what were the limitations that had to be taken into consideration. The answer is presented in the report D35.2 AG Ethical Review of Privacy and Ethical Matters. The AG Ethical members made several points. For one thing, there is a risk that the traditionally vulnerable are being made more vulnerable, as not everybody possesses a mobile phone. Following from that, to use mobile phones for informing means that not all will get the same information. This is problematic, as access to security information should not depend on whether or not one owns a mobile phone. Another concern, according to the AG Ethical, is whether the public would 'feel safer' knowing the information would be available if necessary, or if they would be frightened by the possibility of receiving such information on an individualized basis. Yet another thing is that the ability to provide individualized information might lead to the collection of additional personal data which poses a risk to individual privacy both for legitimate data collection agencies and / or the enhanced hacking possibilities. Illegitimate access is expected to create panic and / or steer people to crisis sites rather than away from them. In addition, it is difficult to know whether or not individuals are travelling at specific moments, and it should therefore be clarified on what assumptions the information should be given.

Within AG Ethical, no shared opinion on the legitimation of an individualized security information system exists. Although some matters could be saved, and despite some possible benefits, all in all, most of the members concluded are that it is not possible to claim enhanced safety from such a system and it should not totally replace traditional passenger information systems.

7.4 Privacy – whose responsibility?

The right to privacy is stated in both national and international laws. The laws state that as a general rule, the actor who wants to register information has to ask for consent from the persons he or she wants information from. This means that actors who want to register information are given an explicit responsibility. They are responsible for informing and offering the option of 'yes' or 'no' to registering, and by doing so, they ensure individuals' privacy. By requiring consent, the laws give the individual control over personal information.

Despite this, every now and then information is used with questionable motives and legitimacy, that is, without consent. One therefore might ask whether or not the consent really is securing privacy in sufficient ways, or if it is more of an illusory protection. Some even declare that consent is dead (Ustaran 2013). The claim is based on people's lack of understanding of what they actually give their consent to, the relative disadvantages by not giving consent, and the risk of function creep among others.

As a response, many urge individuals to take more responsibility themselves in order to ensure their 'own' privacy. Privacy protectors encourage more awareness about privacy issues; insurance companies tell us what we can do in order to avoid identity thefts; our PCs

command us to change passwords; we are advised about how to behave on social media and so on. In other words: in different ways individual responsibility and activity is called for.

The arguments vary. For instance, when it comes to privacy on the Internet, it is claimed that the Internet belongs to everybody and therefore it is everybody's responsibility to make it safe.[5] It is not only *one* part's responsibility. Hackers and cybercriminals can be compared to epidemics, and as with past epidemics, what is required is a combination of collective and individual action. The individual action should be 1) technological, that is, ensuring privacy by settings, and 2) expressed in engagement, putting privacy issues on the agenda in public debate.

Some also hold industry partners responsible, and claim that privacy and security is shared between government, industry and individuals.[6] This is in accordance with the law, which puts the actor who registers information in charge of consent and data security.

Another option, also focusing on a third part (neither government nor individual) is 'privacy by design'. It is based on the view that ensuring privacy should not be left to legislation and regulatory framework; rather, it must be the default mode of operation. That can be accomplished by practicing seven principles:

1. Proactive and not reactive
2. Privacy as default setting
3. Privacy as embedded into design
4. Full functionality positive –sum, not zero-sum
5. End-to-end security, full life cycle protection
6. Visibility and transparency
7. Respect for user privacy

These are guidelines both for organizations that develop technologies and organizations that use technologies. By following them, the chance of misuse is reduced.

No doubt there is a lot of effort one can make to secure personal information. It is however important to underline that privacy is seen as a human right, and that violating privacy is a crime where proscriptive legislation exists. This means that privacy cannot be the individuals' responsibility. It is the government's responsibility.

7.5 Real versus perceived security

It can be dangerous to travel. The threats are numerous and vary from terrorist attacks to impolite teenagers: your plane could crash, the train could derail, and your wallet could get stolen while you are waiting for the bus and so on. It is in the interest of the PTOs to make travelling as safe and secure as possible. This is not to say that they are the only responsible party. The development towards more secure mobility is due to the effort from authorities and producers (of vehicles, ITS etc.) as well. Still, the PTOs do a lot to make travel secure. During SECUR-ED, a lot of capacities have been developed and tested, and they serve as examples of steady work in order to increase security.

[5] http://www.wired.com/2013/10/internet-privacy-and-security-a-shared-responsibility/

[6] http://www.forbes.com/sites/larrymagid/2013/02/12/online-privacy-and-security-is-a-shared-responsibility-government-industry-and-you/

Travel must not only be secure, or as secure as possible, it must also be perceived as secure. This is pointed out because it is no necessary coherence between real and perceived risk. According to Schneier[7] we 'misunderstand' threats in four ways:

1. We over-react to intentional actions, and under-react to accidents, abstract events, and natural phenomena.
2. We over-react to things that offend our morals.
3. We over-react to immediate threats and under-react to long-term threats.
4. We under-react to changes that occur slowly and over time.

This means that we worry more about anthrax than influenza, despite the fact that the annual death toll of anthrax is close to zero while it for influenza is a quarter-million to a half-million people. It also means that we react more when we feel insulted or disgusted. It shows that we do not respond (merely) rationally to threats, and following from that, we may not be able to consider security in the optimal ways.

For PTOs, and other actors who operate in this market, it is not enough to maintain the real security. Because they depend on passengers (like other actors depend on patients, customers, pupils etc.), they need that the latter feel safe in order to make their service attractive. In other words: the real security must be accompanied by a perceived security.

Naturally it happens that the perceived security is in accordance with the real security. But also the opposite is possible. When implementing a security capacity, there is a chance that nothing changes. In addition, at least four consequences are possible: the actual security is improved or not, and the perceived security is increased or not. That means that two different incongruities can occur: when the level of security has not increased but is still perceived as it has, and when the actual level of security has increased, while not perceived so. It is shown in the following table:

Table 7.1 Actual and perceived level of security

		Perceived level of security	
		Increased	Constant / decreased
Real level of security	Increased		Lack of trust and / or knowledge
	Constant / decreased	False security[8]	

The real level of security can increase without a corresponding increase in perceived level of security. One reason is that when someone is paying attention to security, we are reminded that threats actually exist. Armed policemen with dogs can make a place safe, but at the same time the sight of them can be pretty frightening. There are also other consequences not appreciated when an increase in security level takes place. One reason is that the capacities used can be regarded as too intrusive. That was the case with the body scanner. Body scanners are more efficient than metal detectors, and the passengers no longer need to have the hands of the guard on their body. Still, in many places it is rejected because passengers felt exposed and were concerned about their privacy. For example, women

[7] https://www.schneier.com/blog/archives/2006/11/perceived_risk_2.html
[8] Or 'illusory security' in the terminology of Section 6.1.1...

claimed that they have been intentionally picked for random controls and that employees shared their pictures with friends. Kastrup Airport (among others) refuses to use a body scanner showing genitalia until some sort of filter is installed.

Another reason capacities are not appreciated can be cost. The prize can be paid both in money, time and practicalities. Yet another reason can be people's evaluations of the relevance. It is reasonable to believe that efforts directed at threats that are hardly seen and rarely occur are less appreciated than those directed at visible, often experienced threats. Critics also claim that we are being manipulated (reference). Security is a big industry, and following from that, actors exist that have an interest in presenting the world as a dangerous place.

When the actual level of security is consistent, or even decrease, it can simultaneously be perceived as having increased, this is when false security occurs.

7.6 Acceptance of surveillance

With expanding use of technologies that require, use and store personal information, we hear many warnings against giving away personal information too easily. The warnings come from authorities as well as academics and activists.

But at the same time, individuals seem to be rather careless about personal information. In general, they do little to protect their privacy. Even those who say they are aware of privacy do not necessarily take precautions. It turns out that many are privacy pragmatists (Westin, referred in Kumaragu and Cranor 2005), and willing to trade personal information for benefits (Ravlum 2005, Oliver and Lunt 2002). Studies show out that the more people know about how the information will be used, the less willing they are to share such information (Olivero and Lunt 2004). Some individuals seem to care more about privacy than others. Based on a survey on costumer behaviour, Westin classified individuals as 'privacy pragmatists', 'privacy fundamentalists', and 'privacy unconcerned' (Westin 1991, referred to in Kumaraguru and Cranor 2005), thus showing how different individuals deal with privacy. This and similar classifications have been criticized for taking too few factors into consideration (Perri6 2002).

An often heard phrase is: '*I don't care about privacy because I've nothing to hide'*. It is normally stated by persons who do not fear surveillance, and / or see how advantageous use of personal information can be. The reasoning of the argument is that use of personal information is no privacy violation if a person has nothing sensitive, embarrassing, or illegal to conceal. Consequently, criminals involved in illicit activities have something to fear, while the vast majority of people do not. Privacy rights experts, warn against such an attitude. The problem, it is claimed, is the underlying assumption that privacy is about hiding bad things, and that it views privacy as form of concealment or secrecy (Solove 2007). However, this view ignores the fact that surveillance can create chilling effects on free speech and free association, and even inhibit people from engaging in legal activities (ibid.). In this way, it harms society.

7.7 Cultural differences

Capacities cannot be regarded isolated from their context. That counts both for training, procedures and technologies. Neither of them are exclusively defined by intrinsic features. Instead, they can be used and understood in several ways. Also the public's acceptance of them may vary. Take for instance camera surveillance. The same camera can be placed at different places and the signs informing about them can look differently. Also companies' policy and practice regarding cameras vary; in some cases they are used to constantly monitor while in other cases nobody watches. To what degree the cameras are accepted depend probably who you ask, that is, the acceptances vary according to gender, age, perceptions of risk, and so on.

Limited attention has been given to the context of the capacities in SECUR-ED. A few times it has been pointed at the significance of culture. One example is a comment regarding the Berlin demonstration, stating that cultural context is important.

We talk about cultural differences. But we cannot take for granted that cultural differences exist, and we therefore start by asking: Are there cultural differences regarding privacy and security?

Apparently there are. One divide is claimed to be between Europe and USA. In 2010, The Economist[9], under the headline 'The clash of data civilisations', points at sharply differing attitudes towards privacy in Europe and USA. The article states that 'European regulations are inspired by the conviction that data privacy is a fundamental human right and that individuals should be in control of how their data are used. America, on the other hand, takes a more relaxed view, allowing people to use a patchwork-quilt of consumer-protection laws to seek redress if they feel their privacy has been violated. Companies that handle users' data are largely expected to police themselves.' In America it is up to the individual to protect his or her privacy, and privacy is usually regarded as a matter for contractual negotiation (Hessler and Freerks, 1995). This can also be put another way: While there in Europe is an interest in personal dignity, Americans worship liberty; it is to secure 'the blessings of the liberty' versus the guarantee to everyone's 'honour' (Whitman 2004). The consequence is that Europeans and Americans react differently to privacy threats. However, not everybody shares this point of view, and changes on both sides that narrow the gap are expected to come. Still, examples of differences, at least what we think of as differences, can be listed: Americans talk openly about salaries, which is not seen as good etiquette in Europe, Americans are puzzled by Europeans' relaxed attitudes towards nudity, and Europeans cannot understand how merchants can be permitted access to the entire credit history of customers who have never defaulted on their debts (Whitman 2004).

Cultural differences seem to exist also between nations. Many will probably question the Norwegian practice with public tax rolls. Until recently registers of persons' income, tax and capital were published in newspapers, and the same information could be searched for at the Internet. Only the last years this search has required username and password. Similarly Whitman (2004) claim that we cannot assume that we all consider privacy the same. He states that 'We have intuitions that are shaped by the prevailing legal and social values of the societies in which we live.' (Whitman 2004:1160). That means that our intuitions reflect our

[9] (www.economist.com/node/16377097?stiry_id=16377097)

knowledge of, and commitment to, the basic legal values of our culture. Legislation is not separated from culture, nor is history.

Using the latest ESS dataset (from 2012), we can see national differences in trust in national institutions. The respondents indicated their trust at a scale from 1 = no trust at all, to 10 = complete trust. The table shows the number for countries involved in SECUR-ED demos, except that there were no numbers available for Romania and Turkey.

Table 7.2 Trust in legal systems. Percentages.

	No trust at all	1-3	4-6	7-9	Complete trust
Belgium	6.4	21.9	41.0	30.1	0.8
France	5.3	21.0	43.1	29.3	1.3
Germany	3.4	15.7	34.9	41.8	4.2
Italy	16.1	21.8	34.1	25.5	2.6
Norway	0.9	4.3	22.1	64.6	8.0
Portugal	15.6	34.3	40.1	9.8	0.4
Spain	17.7	30.7	36	14.6	1.0

N= 53 149

Individuals were asked do what degree they trusted their country's legal system. The legal system is relevant here, as our right to privacy is enshrined in law. The table shows huge variations in trust in legal systems. Italy, Portugal and Spain have little trust, especially the two latter. Norway distinguishes itself with a very high trust, compared to the others. Belgium, France and Germany are in the middle, Germany having the most trust of those three.

Table 7.3 Trust in the Police. Percentages.

	No trust at all	1-3	4-6	7-9	Complete trust
Belgium	2.2	10.5	33.6	51.8	5.9
France	3.2	11.4	39.7	42.3	3.4
Germany	1.4	6.7	27.8	56.3	7.9
Italy	5.3	10.0	33.9	42.9	7.8
Norway	0.5	4.3	24.3	62.6	8.2
Portugal	5.9	15.8	41.6	34.2	2.4
Spain	5.1	11.5	38	39.8	5.7

N=53 854

In general, the trust in the police is higher than in the legal system. Again Norway has a high trust, but so have also Germany and Belgium, although they are not at Norway's level. Italy, Portugal and Spain have little trust.

Table 7.4 Trust in ones country's parliament

	No trust at all	1-3	4-6	7-9	Complete trust
Belgium	5.8	17.4	48.3	27.8	0.8
France	10.3	28.6	55.9	14.1	1.2
Germany	6.2	24.2	44.5	23.3	1.7
Italy	22.1	33.1	35	8.8	0.9
Norway	1.5	9	37.9	46.7	4.8
Portugal	25.7	41.7	28.2	4.2	0.2
Spain	21.9	29.1	37.1	10.9	0.9

N=53 210

The table shows that Italy, Portugal and Spain have little trust. Also France has little trust, but slightly more than the former three. Norway is still the one with most trust. Belgium, and Germany form a middle group.

Table 7.5 Trust in European Parliament

	No trust at all	1-3	4-6	7-9	Complete trust
Belgium	6.5	16.2	45.7	31.1	0.7
France	10.2	25.5	48.7	13.6	1
Germany	8	28.7	44.8	17.7	0.8
Italy	14.5	21.9	41.3	20.5	1.8
Norway	3.9	16.8	57	22	0.4
Portugal	20.4	33.7	39.1	6.6	0.3
Spain	16.9	25.4	43.9	13.7	0.9

N= 48.345

Norway still has more trust than the others, but the difference to the other countries are not that striking. Norway is not so positive anymore. Also France has little trust.

Except for when it comes to the European Parliament, the pattern is that Norwegians have remarkable high trust in the national institutions, while the Italians, Portuguese and Spanish have the lowest trust. Belgium, Germany and France are in the middle.

7.8 Towards a best practice

This section is a tentative suggestion for best practice for ethical and societal aspects in future large-scale experimentation and demonstration projects.

Our overall impression of the demonstration activities and social/ethical issues is that the project and project partners have a well-informed perspective on current legislation to be followed. However there are other aspects on privacy, ethical and societal aspects discussed in this document that are challenging to approach for partners in a large and complex project. New technologies and new extended use of security systems are evaluated. These technologies, uses and capacities are in part previously unseen in wide use.

In the end it is hard to predict the reaction by the public, and the reaction at several different points in time is of interest: what it would have been if some of these capacities would have already been implemented in society today, the public perception when implemented at a time years ahead, or the long term perception after long use.

We suggest that, as a future best practice, the involved partners should be given privacy, ethical and societal support in terms of an enhanced advisory function, by allocating resources on assessment early in a project process and considering what authorities should be involved in a project.

- Support through project actors could be given through enhanced documented assessment from advisors, early on and as a project unfolds. It can also be produced by design in project planning, striving to have ethical focal issues discussed and formulated in the project planning phase.
- If issues on privacy, ethical and societal aspects issues are being part of an early defined evaluation process, our assessment is that it would constitute support for partners involved in a project.
- Governmental authorities are likely to be challenged by new aspects regarding privacy, ethical and societal aspects on new technologies and new extended use of security systems. Our suggestion is therefore, in the planning phase for a project, to analyse what authorities could be possible to build a working relationship with as representatives for relevant social/ethical perspectives. Expected outcome and effects could be e.g. to enhance the project's ability for promoting discussions to support other partners and to raise the awareness in authorities for possible future challenges. In that way, pitfalls could be avoided during the project and at that the same time the involved actors would be more prepared for future possible difficulties.
- Surveillance at workplaces requires dialogue about the use of cameras, including whose security will be ensured, how use will be logged, who has access and how this will be managed.

It should also be noted that capacities like those tested in SECUR-ED represent possibilities to improve security and mobility. Security measures aim to reduce risks. Still, the operator's main task is to ensure mobility. That is a basic premise for every effort. Implicit is that lack of security and safety hinder mobility. Incidents makes the traffic stop, and controls leads to delays. Efforts that reduces stops and delays, even though their main goal is to reduce risks, thus have mobility as a side effect.

Taken to their respective extremes privacy and security are incompatible. However, a balance can be struck and on the whole SECUR-ED has accomplished this.

In projects, one tool is advisory groups like AG Ethical. In the field, it can be done by paying attention, following legislation, advices and assessments. That does not mean that one does not have to take precautions. It is necessary to be aware that:

- Privacy and accessibility are not only a matter of legislation
- Effort can have long term consequences that is hard or even impossible to predict based on a small scale pilot test
- The understanding, use and acceptance of capacities may vary according to context. Especially public acceptance is an important element for actors selling products or services to individuals.

- End of Document –