PrivAcy pReserving Infrastructure for Surveillance

Deliverable D2.1
Contexts and concepts for SALT Frameworks

Project: PARIS
Project Number: SEC-312504
Deliverable: D2.1
Title: Contexts and concepts for SALT Frameworks
Version: v1.0
Date: 19/07/2013
Confidentiality: Public

Editors: Nathalie Trussart (CRIDS-UNamur)
Claire Gayrel (CRIDS-UNamur)
Francisco Jaime (UMA)

Contributors: Claire Gayrel (CRIDS-UNamur)
Nathalie Trussart (CRIDS-UNamur)
Fanny Coudert (ICRI-KU Leuven-iMinds)
Antonio Maña and Francisco Jaime (UMA)
Carmen Hidalgo (UMA)
Fernando Casado (UMA)
Zhendong Ma (AIT)
Bernhard Strobl (AIT)
Víctor Manuel Hidalgo (Visual Tools)
Mathias Bossuet (Thales)
Daniel Le Métayer (INRIA)
Antonio Kung and 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.	Draft	26/04/2013
V0.2	Added TOC	27/04/2013
V0.7	Added chapters 1, 2, 3.3, 3.4, 3.5, 5, 6, 7	13/06/2013
V0.8	Formatted homogeneously	13/06/2013
V1.0	Finalization of the document	31/07/2013

Approval		
	Name	**Date**
Prepared	Antonio Kung	31/07/2013
Reviewed	All Project Partners	31/07/2013
Authorised	Antonio Kung	31/07/2013

Circulation	
Recipient	**Date of submission**
Project partners	31/07/2013
European Commission	31/07/2013

Executive Summary

This public reporting document describes the approach adopted by PARIS in the task of getting an understanding of the contexts and the concepts relevant for developing SALT frameworks. (Work Package 2 – WP2, Task 1). In order to achieve this task, the following activities are performed in this deliverable.

Chapter 1 (Introduction: A Multidisciplinary Approach to Privacy) aims at providing a general introduction of the deliverable. After recalling its objectives and scope, it starts with a section which is dedicated to terminology. Some conceptual remarks needed for the well understanding of the progression of this study. First ones concern the important notion of “privacy”. Second ones concern the notion of “surveillance”. Third ones concern privacy-surveillance paradigms, where are exposed different rationales regards to the balance between surveillance and privacy. Following a section devoted to the concept of privacy-by-design, the risks and the challenges of this approach. Then, as a result of those precedent remarks, a set of remarks concerns the prism through which the SALT Framework is developed and offers the opportunity to underline the uniqueness of the SALT framework compared to other privacy frameworks used for the privacy by design of a system-to-be. Finally, a final round of remarks concern the multidisciplinary approach adopted in this text.

Chapter 2 (Privacy from Socio-Political and Ethical Perspectives) focus on different parts: one about psychosocial perspective, one about socio-political perspective and a last one regards to ethical perspectives. The section ("Privacy from a Psychosocial perspective") deals with the privacy of systems seen from psychosocial perspective. It includes different definitions of privacy relevant to the PARIS project, stressing the Altman' psychosocial model of privacy[1]. Then it discusses the different dimensions of privacy (solitude, isolation, anonymity, reserve and intimacy) and adds a classification depending on the privacy spaces (public spaces, semi-private and private spaces). Besides, this section also explains the effects of lack of privacy and the relationship between the psychological perception of privacy and the effects of the lack of privacy. Finally, this part of the document identifies the different functions and types of privacy and the relationship between them. The following section ("Privacy form a Socio-political perspective") is devoted to privacy as it is theorized from a socio-political perspective, by socio-political scholars and legal theorists. After a general overview of the main claim from the socio-political perspective, this section suggests that for the purpose of the framing of the SALT Framework, a good starting point is the study and analyse of different taxonomies, their benefits and defaults. The last section ("Privacy from an ethical perspective") follows the same structure: a general overview of the main claims regards to ethical dimensions of privacy and close the chapter with some existing manners to apprehend privacy's ethical dimensions.

Chapter 3 (Privacy from a Legal perspective - European Legal Framework for Privacy and Data Protection) aims at providing a global review of the European legal requirements in the matters of privacy and data protection, in particular in order to understand the balance between privacy public space, understood as the extent to which privacy interests are at stake when surveillance systems are deployed, especially in public spaces, and the legal 'concepts' that the SALT framework will have to integrate. In this aim, the chapter is divided in six parts. The first section will come back on the essential issues of the debate surrounding the *privacy v. public security balance* in the European Union in order to have an overview of the legal "context" within which the PARIS project intends to produce innovative solution. The second section will present the legal landscape of the protection of privacy and personal data in the Member States, which will be the occasion to identify the main relevant normative sources that may be taken into account by the SALT framework. The third section will present the caselaw of the European Court of Human Rights (ECHR) with regard to the right to private life and data protection, with specific attention on some important developments in relation to the extent of protection of private life to informational issues and public surveillance. Section four will present the core concepts and principles enshrined in the Directive 95/46, which is the main relevant EU wide instrument on the protection of personal data applicable in all Member States. Finally, because this instrument does not address the issues of protection of personal data in relation to specific surveillance technologies, we will look at European guidance with regard to videosurveillance activities (section five) and biometric technologies (section 6), which are PARIS use cases, and how these matters are dealt with in two Member States, Belgium and France.

[1] Irwin Altman, *The environment and social behavior: Privacy, personal space, territoriality and crowding* (Monterey (Ca.): Books/Cole, 1975).

Chapter 4 (Accountability by Design – a Way to Ensure Transparency and Trust) proceeds to a review of the state-of-the-art on the principle of accountability in view of extracting preliminary criteria for the design of an accountability-based approach for personal data governance practices within the SALT framework. In section 1, we will see that "accountability" is a concept 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 "mechanism of control" and that both approaches are of interest for the SALT Framework. As elaborated in section 2 we will see that both concepts share common features. In short, accountability relationships involve a third party external to the accountable agent and in which the latter is asked to answer the requests of the former, which may result in corrective actions taken by the agent. The review of the different initiatives in view of the introduction of an accountability-based approach within the data protection framework in section 3 shows that they approach accountability as implementation and enforcement mechanism of the existing framework, although none of the policy instruments reviewed provides for a definition of the principle of accountability. The different initiatives reviewed do however not address the specifics of surveillance practices, which means that further work is required to tailor these preliminary criteria to the context of surveillance. The next deliverable (D.2.2.) will build on the findings of this Chapter to provide a definitive list of requirements, adapted to the context of surveillance.

Chapter 5 (Privacy from a Computer Engineering Perspective) deals with the privacy of systems seen from a technological point of view. The most common principles for privacy are listed, including OECD principles. With these principles in mind, the section defines some important concepts related to ICT privacy (such as anonymity, pseudonymity, unlinkability, etc.) and privacy in video-surveillance systems. Privacy-enhancing technologies are also mentioned: encryption, access control, obfuscation, etc. Once the basis of privacy is planted (i.e., principles and concepts) this section disserts about new technologies and how they affect current systems' privacy (making a distinction between hardware and software advances), and nowadays advances in connectivity and ubiquity. Finally, it focuses on the different applications and technologies regarding to surveillance and what type of impact they can have on people. Considering PARIS project main use-cases (i.e., video-surveillance and biometrics systems) a large set of heterogeneous surveillance systems are described: imaging scanners, satellites, photography, fingerprint recognition, iris recognition, dataveillance, GPS, etc. Biometric systems functionality is also described for a better understanding of this type of systems.

Chapter 6 (Preliminary Recommendations for the SALT Framework) concludes with **recommendations** to be considered in the development of SALT Frameworks and, as a consequence, in the preparation of the next deliverable. Those recommendations are based on all previous findings identified within this report.

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-Enhanced 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

1 Introduction: a Multidisciplinary Approach to Privacy

Nathalie Trussart (CRIDS – University of Namur)

1.1 Deliverable Objectives 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 which enforces the right of citizens for privacy, justice and freedom. The methodological approach will be based on two pillars:

- A theoretical framework for relating surveillance and privacy/data protection, and integrating the concept of accountability.
- An associated process for the design of surveillance systems which takes from the start privacy (i.e. privacy-by-design) and accountability (accountability-by-design).

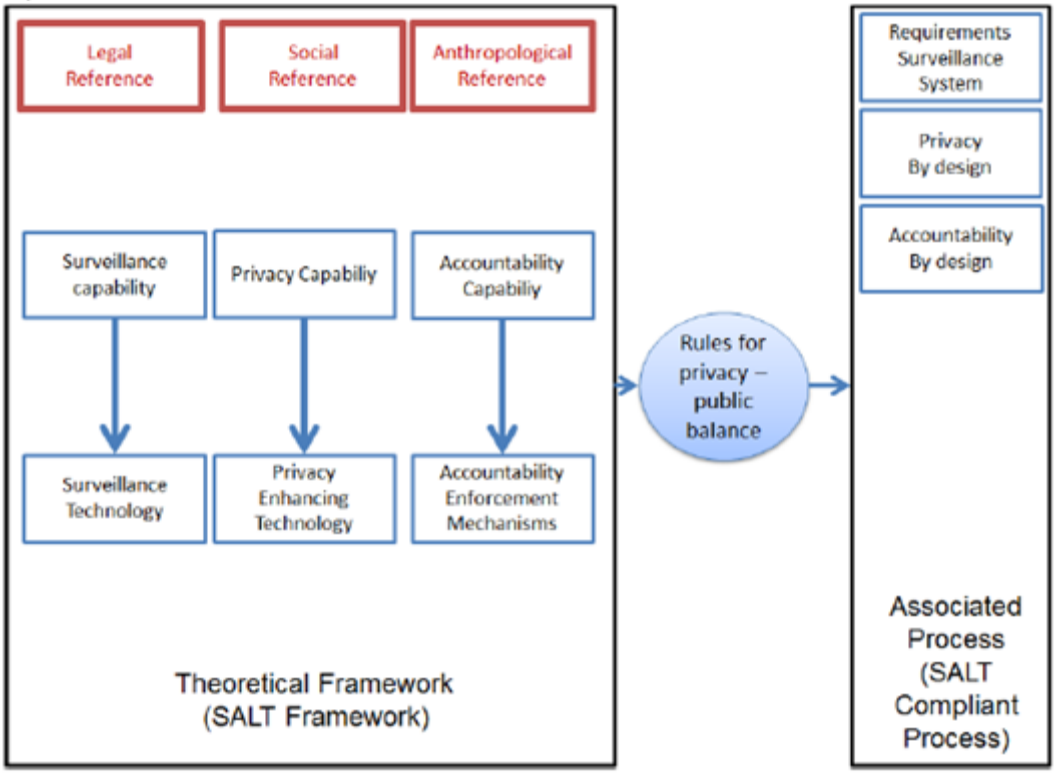

Figure 1 PARIS Methodological Approach

The following objectives will be addressed during the PARIS project:

- 01: Definition of a **S**ocial, **A**nthropological, **L**egal and **T**echnical or **SALT framework** for an evolving understanding of the concept of privacy in a surveillance system, while fully integrating the concept of accountability.
- 02: Development of **a SALT framework management tool**. This tool allows for a digital reference and representation of a SALT framework. It is used by stakeholders as a reference, including for the design of surveillance systems. It includes mechanisms for creating and updating a SALT framework.

- 03: Definition of **a SALT compliant process** for surveillance. It uses a reference SALT framework and integrates process activities and process artifacts for privacy-by-design and accountability-by-design.
- 04: Provide **evidence of the value of SALT compliant process for surveillance in two cases**. A laboratory demonstration will show how a surveillance system can be developed using a SALT compliant process for video data lifecycle management based applications and for biometrics based applications.

The aim of this deliverable D21 is to contribute to the making of the theoretical framework above cited as the first objective of the PARIS project.

This theoretical framework, while being conceived through a triple prism - (1) a **S**ocio-political and ethic**A**l prism, (2) a **L**egal prism and (3) a **T**echnological prism – , is the **SALT** framework which is at the heart of this project. A SALT framework describes a consistent socio-political, ethical, legal and technological skeleton concerning the balance between privacy and surveillance.

This study, carried out in Work Package 2, in the scope of Task 1 on "Concepts and Contexts", aims to help the characterisation 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, technical privacy's dimensions and the concept of accountability. This aim is achieved through a well documented overview of the current European landscape recorded about the relationship between privacy and surveillance. The materials used for this task consist in scientific literature, laws, institutional and policy documents, and studies (co-)funded by the European Commission.

1.2 Terminology

For the well understanding of the progression of this study, we have to start with some conceptual remarks. First ones concern the important notion of "privacy". Second ones concern the notion of "surveillance". Third ones concern privacy-surveillance paradigms. Fourth ones concern the critique addressed to the privacy-by-design concept for adopting a techno-centric perspective. And finally, as a result of those precedent remarks, the last set of remarks concerns the prism through which the SALT Framework is developed.

1.2.1 Privacy

The notion of "privacy" is used through this document in a very generic sense as long as it is not precisely specified otherwise. Indeed, as we consider several perspectives, the notion of "privacy" has different specifications and characterisations. Thus, for example, inside the legal practice, as well as from the theoretical legal perspective, the notion of "privacy" is well distinguished from the one of "data protection". Nevertheless, this single distinction is not relevant from ethical and social perspectives for which several other distinctions are identified. As this document will show, these different disciplinary perspectives bring different distinctions which intersect and partially overlap while bringing interesting nuances. At each step, a point is

made about the main characterisations of privacy which are highlighted by the relevant discipline. And finally, the conclusive part of this document aims at gathering those dimensions of privacy which were provided through this study and gives a provisional list of criteria which should be taken into account in the design of the SALT framework. A series of recommendations for the integration of those dimensions in a SALT framework are gathered, while paving the way for the preparation of the next deliverable (D 2.2).

A second remark has to be made about this notion of privacy and the way this study carve a pathway through its conceptual muddle. The aim of this report is not to provide a definition of privacy. Nevertheless, as the aim of this study is to provide a well documented set of privacy's dimensions which may be of interest in the making of the SALT framework, several definitions, dimensions and classifications of privacy are presented. Despite the differences between the proposals presented in this study, the chosen authors share the common convictions that **privacy counts**, that **privacy is in danger** and that **privacy should be protected**. Although, in this task, their strategies are different, their enterprise in defining or describing privacy is sustained by these common assumptions.

This "privacy counts"[2] thesis may seem obvious. However, it still faces another one, the "**privacy is dead**" doctrine for which struggling to protect privacy is a vain activity which comes too late: the body (of privacy) is cold[3]. "You have zero privacy anyway. Get over it!"[4]: that is its most popular motto and (re)appears regularly when a new breach into our privacy is discovered[5]. For our purpose – to make clear the standpoint adopted in this document and the choices made among the numerous literatures relating to privacy issues – there is no need to

[2] Despite, or precisely because, the critiques surveillance studies address to the concept of privacy, I consider them as being part of those who share this "privacy counts" thesis, even though they precisely critics the concept of privacy because it is too narrow and leaves aside crucial issues. What is at stake in this general assumption is the critique which targets the propensity of privacy protection policy to reduce any issue to informational terms and to the definition of successful privacy governance in terms of the application of the 'fair information principles (FIPS)' doctrine for which any surveillance must involve a moment of capture of personally identifiable data. For more details of the arguments in favor of the defence of privacy and an interesting response to the critiques addressed by scholars working in the field of Surveillance Studies, see this enlightening paper: Colin Bennett, "In the defense of privacy. The concept and the regime", *Surveillance & Society*, 8 (4) (2011): 485-96.

[3] A longer development about the "privacy is dead" thesis is provided here: Serge Gutwirth et al., "Deliverable D1: Legal, social, economic and ethical conceptualisations of privacy and data protection," in *PRESCIENT. Privacy and emerging fields of science and technology: Towards a common framework for privacy and ethical assessment* (EC: Seventh Framework Programme, March 2011).

[4] In 1999, the chief executive officer of Sun Microsystems, Scott MacNealy made this declaration in front of a group of reporters and analysts. (Sprenger s.d.). If at this time, it was a shocking statement – Jodie Bernstein, director of the Bureau of Consumer Protection at the US Federal Trade Commission, said that McNely's remarks were out of line: "Millions of American consumers tell us that privacy is a grave concern to them when they are thinking about shopping online" – nowadays, things look like getting worse. (Couts s.d.)

[5] A very recent resurgence of this slogan stands to designate the news revealed by the Washington Post in June 2013: "The U.S. government is accessing top internet companies' servers to track foreign targets. (...) GCHQ, Britain's equivalent of the NSA, also has been secretly gathering intelligence from the same internet companies through an operation set up by the NSA". See: Barton Gellman and Laura Poitras, "U.S., British intelligence mining data from nine U.S. INternet companies in broad secret program", *The Washington Post*, 2013, June 6. http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html See the use of the motto: (Dignan s.d.)

enter in the details of its proponents' similar remarks[6], which go from spelling end of privacy to actively blurring the private and public divide[7]. Nevertheless, it is worth noting the existence of this doctrine.

1.2.2 Surveillance

The notion of "surveillance" that is taking into account as a start in this deliverable is a generic one. It is not restricted to security situations, neither to the only cases of video surveillance and biometrics which are under focus in this study, except as otherwise specified.

The main argument in favour of a broader definition of "surveillance" is the large amount of practices which implies surveillance and which, while not being linked to security, *stricto sensu*, are likely to cause harms to privacy. Those practices of surveillance have existed for a long time, e.g. records of people by and for administration purposes. New ones, with new specificities (technologically speaking), implies new possible and actual harms to privacy.

> "Understanding surveillance society as a product of modernity helps us avoid two key traps: thinking of surveillance as a malign plot hatched by evil powers and thinking that surveillance is solely the product of new technologies (and of course the most paranoid see those two as one). But getting surveillance into proper perspective as the outcome of bureaucracy and the desire for efficiency, speed, control and coordination does not mean that all is well. All it means is that we have to be careful identifying the key issues and vigilant in calling attention to them"[8].

[6] Few examples among others:

- Marc Zuckerberg, the billionaire founder of Facebook, is accredited with having said that people no longer have an expectation of privacy on line as the rise of social networking online shows, that means that privacy is no longer a social norm. See: (Johnson 11 Jan 2010)
- Eric Schmidt, Google's chief executive officer, spoke in those terms about its company's aspirations: "When we talk about organizing all of the world's information, we mean all". See: Randall Stross, "Google anything, So Long as It's Not Google"", *The New York Times*, 28 Aug 2005.
- "Sir David Omand, the former Whitehall security and intelligence co-ordinator, sets out a blueprint for the way the state will mine data - including travel information, phone records and emails - held by public and private bodies and admits: "Finding out other people's secrets is going to involve breaking everyday moral rules. (...) Modern intelligence access will often involve intrusive methods of surveillance and investigation, accepting that, in some respects this may have to be at the expense of some aspects of privacy rights". See: (Travis s.d.)

[7] Danah Boyd, Microsoft's social media expert, "argued strongly that privacy is not dead and has no diminished in importance, but rather that the distinctions between private and public are different in the network age. (...) she contrasts what she calls personally identifiable information with personally embarrassing information and notes that these need to be treated differently because the consequences of exposure are different." Actually, companies might try to convince their users they care about their privacy, while adding privacy options which protect them from any embarrassing situation – personally embarrassing information -, they are more interested in personally identifiable information for marketing purposes. See: (Thompson s.d.) . For more details about the market use of personally identifiable information: Louise Story, "To Aim Ads, Web is keeping Closer Eye on You", *The New York Times*, 2008: http://www.nytimes.com/2008/03/10/technology/10privacy.html?pagewanted=all.

[8] Surveillance Society Network, *A report on the Surveillance Society. For the UK Information Commissioner (U.K.: Information Commissioner's Office, 2006),* 2. Available at: http://www.ico.gov.uk/about_us/research/reports_to_parliament.aspx.

Some authors, like Michel Foucault[9] or Ulrich Beck[10], to mention only two among others, have extensively documented this understanding of surveillance as a product of modernity.

Based on this historical perspective, the *Report on the Surveillance Society for the UK Information Commissioner* suggests this definition of surveillance:

> "Where we find purposeful, routine, systematic and focused attention paid to personal details, for the sake of control, entitlement, management, influence or protection, we are looking at **surveillance**."[11]

And the Report goes on with the definition of those characteristics:

> "To break this down:
>
> - The attention is first *purposeful*; the watching has a point that can be justified, in terms of control, entitlement, or some other publicly agreed goal.
> - Then it is *routine*; it happens as we all go about our daily business, it's in the weaves of life.
> - But surveillance is also *systematic*; it is planned and carried out according to a schedule that is rational, not merely random.
> - Lastly, it is *focused*; surveillance gets down to details. While some surveillance depends on aggregate data, much refers to identifiable persons, whose data are collected, stored, transmitted, retrieved, compared, mined and traded.
>
> The personal details in question may be of many kinds, including CCTV images, biometrics, such as fingerprints or iris scans, communication records or the actual contents of calls, or most commonly, numerical or categorical data."[12]

In this study, this broad definition offers a sufficient generic scope likely to accommodate different species of surveillance technology[13], regarding different characteristics that must be specified before any examination:

- the type of surveillance's practices (watching, listening, following, etc.);

[9] Michel Foucault, *Discipline and Punish:The birth of the prison.* (New York: Random House, 1975).

[10] Ulrich Beck, *Risk Society: Towards a New Modernity* (London: Sage, 1992).

[11] Surveillance Society Network, *A Report on the Surveillance Society. For the UK Information Commissioner* (U.K.: Information Commissioner's Office, 2006), 4. Available at: http://www.ico.gov.uk/about_us/research/reports_to_parliament.aspx.

[12] Ibid., 4.

[13] For taxonomy and mapping of surveillance technologies, see: Alberto Crespo García et al., "D1.3. Report on Technology Taxonomy and Mapping", *PACCT: Public perception of security and privacy: Assessing knowledge, Collecting evidence, Translating research into action*, June 2012.

For a complete description of smart surveillance systems, see: Michael Frieddewald and Rocco Bellanova, "Deliverable 1.1: Smart Surveillance - State of the Art," in *SAPIENT. Supporting fundamental Al rights, Privacy and Ethics in surveillance Technologies* (EC: Seven Frameworks Programme, January 2012).

For details about the development and use, by both authorities and private actors in Europe, of surveillance systems and technologies for fighting crime and violence, see: Trilateral Research and Consulting LLP, "Deliverable D1.1: Surveillance, fighting crime and violence," in *IRISS: INcreasing Resilience in Surveillance Societies* (EC: Seventh Framework Programme, 2012), Available at: http://irissproject.eu/wp-content/uploads/2013/06/IRISS-D1-MASTER-DOCUMENT-10-June-2013.pdf.

- the type of surveillants[14] (public authorities, private actors, etc.);
- the target of the surveillance (people or objects, particular individuals, groups or social categories of persons, etc.);
- the technology used (video surveillance, imaging scanners, fingerprint recognition, etc.)[15] ;
- the purpose of the surveillance (crime control, marketing, etc.);
- the locations and perimeters kind of surveillance (transport facilities, public space, communication facilities, etc.);
- the publicity/visibility of the surveillance (do the surveilled know precisely when, where, why and how they are under surveillance?);
- etc.

Starting from this generic definition of surveillance will allow, in further steps of the PARIS project, to characterize, among those technologies of surveillance, on the one hand, the ones which are chosen as case studies and, on the other hand, the other ones for which the SALT Framework is also relevant.

1.2.3 Privacy-Surveillance Paradigms

The two last set of remarks regarding privacy and surveillance tend, both, to avoid fixing those terms into absolute values that are inversely proportionate to each other. Indeed a rapid overview of the literature regards to privacy and surveillance shows a wide range of possible definitions and theories which are not necessarily in opposition. Instead they can and they should take turns each other regards to different situations and to different privacy problems which can occur in one single situation. The inversely proportionality between surveillance and privacy is characteristic of **a trade-off-paradigm of privacy and surveillance** in which an increase of one part necessarily results in a decrease of the other part: more privacy is seen as being only achievable by less surveillance and more surveillance is seen as being only achievable by less privacy.

By **privacy-surveillance paradigms**, I refer to a set of assumptions about their relations and their definitions. These assumptions collectively set the agenda of argumentation, policies and research and yet are often not made explicit. A paradigm produces an approved and common understanding about the nature and scope of a particular problem.[16] Those paradigms do not

[14] Surveillants and surveillers are neologisms coined by surveillance studies scholars with the aim of offering a generic identity for those actors of surveillance system whose actions are not reduced to the only one of watching.

[15] A complete list of technologies of surveillance is developed thereafter in this deliverable (Section 4.7).

[16] The notion of privacy paradigm is interestingly used in Colin Bennett and Charles Raab, "The privacy paradigm," in *The Governance of Privacy. Policy instruments in Global Perspective*, ed. Colin Bennett and Charles Raab (Cambridge (MA): MIT Press, 2006), 3-28. A similar set of paradigms as general worldviews is developed in Wolfgang Hofkirchner, *Twenty questions about a Unified Theory of Information. A Short Exploration into Information from a Complex System View* (Litchfield Park (AZ): Emergent Publications, 2010), 37. This attempt of categorization is based on a similar one made about the relationship between security and privacy in the PACT project: Anthony Amicelle et al., "D1.1. Report on Theoretical Frameworks and Previous Empirical Research," in

pretend to describe reality as it is – reality is of course much more complex –, neither grant an exhaustive categorization, but rather provide a way to organize and discuss relevant assumptions, arguments and theories underlying such privacy-surveillance paradigms, included the problems they address and the errors they induce. This discussion is beyond the scope of the present document. This is also the case for the necessary clarification of the links between security, surveillance and privacy. Nevertheless, this overall explicit categorization may be a useful tool in order to have common milestones when the relationships between privacy and surveillance are at issue.

Here are the three main privacy-surveillance paradigms.

- **A Trade-off Surveillance-Privacy Paradigm.**
    - **a. Surveillance Prevalence Paradigm.**

      Needs for surveillance explain, causally determine and dominate the scope of privacy.

        - **i. Example of arguments used in this paradigm** [17]:
            - **The Nothing-to-hide argument:**

              "If you are not a criminal or terrorist, then you got nothing to fear from application of surveillance technology and therefore nothing to hide."
            - **The All-or-Nothing fallacy:**

              "For protecting security, we need to reduce/abolish privacy because the latter shields criminals and terrorists."
            - **The Pendulum Argument:**

              "Times of exception, such as terror and war, require the curtailment of civil liberties."
    - **b. Privacy Prevalence Paradigm.**

      Needs for privacy explain, causally determine and dominate the scope of surveillance.

        - **i. Example of arguments used in this paradigm** :
            - **The privacy-first-Argument:**

              "Privacy or other values are absolute and need to be protected even if this results in less security"
- **The Privacy-Surveillance as Dualistic Paradigm.**

  Surveillance and Privacy are seen as causally independent and have an autonomous existence.

    - **i. Example of arguments used in this paradigm** :

PACT. Public perception of security and privacy. Assessing knowledge Collecting evidence, Translating research into action (EC: Seventh Framework Programme, 2012), 120-4.

[17] Those arguments are all developed by the legal theorist, Daniel Solove, about Security and Privacy. Daniel J. Solove, *Nothing To Hide. The False tradeoff between privacy and security* (New Haven: Yale University Press, 2011).

"Privacy and surveillance technologies can both be achieved. They are not causally connected."

- **The Privacy-Surveillance as Interconnected Paradigm.**

  Surveillance and Privacy are different and connected, they depend on each other and constitute each other mutually.

  i. **Example of arguments used in this paradigm** :

  "A society that respect privacy of the weak and bases itself on equality can enhance and secure stability and social peace, which can further enhance basic rights. Privacy enhances security and security should be understood and implemented in a way that enhances privacy."

1.3 Privacy-by-Design

That categorization being showed, it is worth adding a remark about the dualistic paradigm. Indeed, some scholars in the field of security studies[18] noted that the concept of **privacy-by-design**, which is at the core of the PARIS project, was one of its examples. They quote extensively the Ontario's Information and Privacy Commissioner, Ann Cavoukian who has pioneered this concept:

"Adding privacy measures to surveillance systems need not to weaken security or functionality but rather, could in fact enhance the overall design (…) privacy must be proactively built into the system, so that privacy protections are engineered directly into the technology (…) The effect is to minimize the unnecessary collection and uses of personal data by the system, strengthen data security, and empower individuals to exercise greater control over their own information. The result would be a technology that achieves strong security and privacy (…) By adopting a positive-sum paradigm and applying a privacy-enhancing technology to a surveillance technology, you develop, what I may call 'transformative technologies'. Among other things, transformative technologies can literally transform technologies normally associated with surveillance into ones that are no longer privacy-invasive, serving to minimize the unnecessary collection, use and disclosure of personal data, and to promote public confidence and trust in data governance structures (…) I am deeply opposed to the common view that privacy is necessarily opposed to, or an obstacle to, achieving other desirable business, technical or social objectives. For example:

- Privacy versus security (which security? Informational, personal or public/national?)
- Privacy versus information system functionality
- Privacy versus operational or programmatic efficiency
- Privacy versus organizational control and accountability
- Privacy versus usability

The zero-sum mentality manifests itself in the arguments of technology developers and proponents, vendors and integrators, business executives and program managers – that individual privacy must give way to more compelling social, business, or operational

[18] Anthony Amicelle et al., "D1.1. Report on Theoretical Frameworks and Previous Empirical Research," in *PACT. Public perception of security and privacy. Assessing knowledge Collecting evidence, Translating research into action* (EC: Seventh Framework Programme, 2012), 123-4.

objectives. At the same time, defenders or advocates of privacy are often cast, variably, as Luddites, technological alarmists, or pressure groups largely out of touch with complex technological requirements and organizational imperatives. Because of this prevailing zero-sum mentality, a proliferation of surveillance and control technologies is being deployed, without appropriate privacy checks and balances."[19]

After noting that privacy-by-design mainly means the creation of privacy-enhancing technologies (PETs), the critics quote another scholar, from the field of Surveillance Studies[20], for whom privacy-by-design and its dualistic paradigm are "a technocratic approach to managing information that fails to grasp how power shapes the agenda and overall context in which struggles over technological design occur"[21]. According to these authors, this dualistic paradigm is based on a belief in a technological fix to societal problems.

Indeed, in the last ten years, a range of scholars in the emerging field of Surveillance Studies have raised criticisms with respect to Privacy enhancing technologies (PETs) and/or the privacy as confidentiality paradigm. These critiques have focused on describing modern day conditions in order to show that the computer scientists' conception of privacy through data or communication confidentiality has been mostly techno-centric and has used to displace end-user perspectives.

1.3.1 Techno-Centricity

Techno-centricity is generally defined as a viewpoint which is mainly involved in understanding how technology influences human action, taking a largely functional or instrumental approach.[22] Within such approaches, people – engineers are not the only ones who may be attached implicitly to this viewpoint - tend to assume unproblematically that technology is largely neutral, exogenous, homogenous, predictable, and stable, performing as intended and designed across time and place. This perspective tends to put technology in the centre, blend out cultural and historical influences, and products technologically deterministic claims.

Facing techno-centricity, there is **human-centricity**, a view which focuses on how humans make sense of and interact with technology in various circumstances. In human-centric accounts,

[19] Ann Cavoukian, *Privacy by Design. Take the Chalenge* (Ontario (Canada): Information and Privacy Commissioner of Ontario, 2009), 51. Available at: http://www.ipc.on.ca/images/Resources/PrivacybyDesignBook.pdf

[20] Surveillance Studies is a cross-disciplinary initiative to understand the rapidly increasing ways in which personal details are collected, stored, transmitted, checked, and used as a means of influencing and managing people and populations. See one its promoters, in the editorial he wrote for the first issue of the first volume of the journal created in 2002 entirely dedicated to Surveillance Studies: David Lyon, "Editorial. Surveillance Studies. Understanding visibility, mobility and the phenetic fix", *Surveillance and Society*, 1 (1) (2002). The objective of these studies is to critically understand the implications of current day surveillance on power relations, security and social justice.

[21] Dwayne Winseck, "Netscapes of power. Convergence, network design, walled gardens, and other strategies of control in the information age," in *Surveillance as social sorting*, ed. David Lyon (New York: Routledge, 2003), 176-98.

[22] For a well documented reading of the techno-centric view, see: W. J. Orlikowski, "Sociomaterial practices: Exploring technology at work.", *Organization Studies*, 28 (2007).

technology is understood to be different depending on meanings human attribute to it and through the different ways people interact with it. This approach takes cultural and historical contexts into consideration, but has a tendency to minimize the role of technology itself. [23]

Besides these two positions in dichotomy, there is also a mediate position for which the materiality of technology and the human processes, where those processes are inseparably individual and collective at the same time, are **constitutively entangled**[24]. "Social practices in space subject to surveillance are constituted by existing surveillance practices and by PETs, whereas PETs are the products of humans, their own social practices and conceptions of how surveillance is made effective and can be countered."[25]

Among computer scientists, some authors have also raised criticisms with respect to PETs and/or privacy as confidentiality paradigm. More exactly, these criticisms were directed against the trend, within the computer science community, to follow one single guiding principle that is that privacy equates confidentiality. That principle has gained so much importance that technical alternative privacy solutions are left over and not taken into account.[26] In addition, this trend is often accompanied by forgetfulness or contempt of other practices that are also involved in the protection of privacy, practices including, for example, that of a judge, or that of a data controller, or that of an end-user, or that of a legislator, or that of a activist of the League of Human Rights, or that of a "privacy council" in a hospital, and so on.

Discussions about PETs and privacy exclusively considered as confidentiality are beyond the scope of this chapter. The same remark applies to a discussion that would decide between Ann Cavoukian's presentation of privacy-by-design concept and criticisms that have been addressed to it. However, it is worth bearing in mind those critiques, while recalling them:

> A techno-centric proposal; a technological fix to privacy which is a societal problem; a technocratic approach to managing information that fails to grasp how power shaped the agenda and overall context in which controversies over technical design occur; an unproblematic assumption that technology is stable and performing as intended and designed across time and place; a proposal that places technology in the centre of privacy issues while blending cultural and historical influence.

Rather than considering them as describing the reality of what is a privacy-by-design process and what are its outputs, those criticisms may be seen as showing some risks any privacy-by-design process runs. In that sense, the privacy-by-design concept may gain robustness in demonstrating how it avoids these risks. This is surely a challenge for the PARIS' project.

[23] For a general presentation of this human-centric perspective, see: Ibid.

[24] For a general presentation of this inseparability and co-constitution of technology and human's processes, see: W. J. Orlikowski, "Sociomaterial practices: Exploring technology at work.", *Organization Studies*, 28 (2007). One of its promoters, see: Langdon Winner, "Do artifacts have politics?", *Daedalus*, 109 (1) (1980). And see also: Langdon Winner, "How technology reweave the fabric of society", *The chronicle of higher education*, 39 (48) (1993).

[25] Seda Gürses, *Multilateral Privacy Requirements Analysis in Online Social Network Service. PhD thesis* (Leuven: HMDB, Department of Computer Science, K.U.L., 2010).

[26] The computer scientist, Seda Gürse, reviewed and analysed these critiques addressed to privacy understood as confidentiality and proposed a classification of different types of privacy solutions through three privacy paradigms in computer sciences: privacy as confidentiality, as control, as practices. See: Ibid.

1.3.2 Privacy-by-Design: a Challenge

Indeed, from the sole point of view of rhetoric, those criticisms do not do justice to the general spirit of Privacy-By-Design as it is developed in its seven foundational principles[27] listed below:

1. *Proactive* not Reactive; *Preventative* not Remedial
2. Privacy as the *Default* Setting
3. Privacy *Embedded* into Design
4. Full Functionality – *Positive-Sum* not Zero-Sum
5. End-to-End *Security – Full Lifecycle Protection*
6. *Visibility* and *Transparency* – Keep it *Open*
7. *Respect* for User Privacy – Keep it *User-Centric*

While leaving the sole point of view of rhetoric, the critics exposed above not only identify risks any Privacy-by-Design process runs, they also identify the gap between the spirit of the Privacy-by-Design and the incorporation of Privacy-by-Design into a system-to-be.

The Paris project offers the opportunity to put these difficult challenges to the test. In that sense, it is a real scale experiment of what may be the actualisation of high privacy-by-design expectations. The first step of this real scale experiment lies in the building of the SALT framework which is characterized by its multilateral perspectives: different knowledge and practices – be they come from academic or private sectors.

1.4 The Singularity of the SALT Framework

As presented in the description of work of PARIS' project, the initial formulation of the **SALT** Framework has been at first set as referring to **S**ocio-political, **A**nthropological, **L**egal and **T**echnological dimensions of privacy. Indeed, for theoretical and methodological reasons, this wording must be specified and may be amended in the future of this project.

1.4.1 Beyond Compliance

Among the computer science community working in the research field of privacy research[28], most of the efforts have been made, during those last forty years, in addressing privacy during

[27] Ann Cavoukian, *Privacy by Design: The 7 Foundational Principles Implementation and Mapping of Fair Information Practices* (Ontario (Canada): Information & Privacy Commisionner of Ontario, Originally published: May 2010, Revised January: 2011). Those principles and many other resources regards privacy-by-design are available at: http://www.privacybydesign.ca/index.php/about-pbd/7-foundational-principles/

requirements engineering mainly with a focus on engineering security and legal compliance. That means that, for efficiency reasons, "requirements engineers have avoided the complexity of reconciling different privacy notions and solutions by implementing one selected definition of privacy in the methods they propose, e.g., privacy as data confidentiality or as legal compliance"[29]. This strategy is efficient but it does not provide the means to address some other types of privacy concerns e.g., informational self-determination, and it does not take into account other technical, social or legal mechanisms that enable different types of privacy.

By contrast, the singularity of the PARIS project lies in its aim to broaden the scope of privacy concerns taken into account, while integrating two supplementary dimensions to the usual legal and technical ones, going beyond the technical security requirements and the legal compliance[30]. It aims at integrating potential individual and collective privacy's concerns, while taking into account from the start the concept of accountability. The privacy-by-design process in which the PARIS is engaged seeks to respond to the challenges posed by such a consideration. That being said, the question arises about the knowledge which are likely to inform regarding those individual and collective dimensions of privacy which may be taken into account in the building of the SALT framework.

1.4.2 Individual and Social Privacy's Dimensions

Pragmatically, while the socio-political dimensions cover a wide range of privacy concerns regards to collective issues, the only anthropological dimensions which was hoped to address the individual privacy dimensions in the SALT Framework, have quickly appeared both too narrow and too specific to address privacy dimensions which are related to individual issues. Indeed, regards to individuals, many other dimensions of privacy are of interest and are studied by many academic disciplines (e.g. psychological or psychosocial dimensions of privacy) other than anthropology alone. Furthermore, as it will be developed in this second chapter, the claim in favour of the recognition of privacy as a social value induces to take into account privacy's value both to the individuals as well as to society. Among privacy scholars, anthropology have not yet produced this kind of interlinked insights likely to keep individual and social dimensions of privacy intertwined. Hereafter, there are several issues proper to the used that have been

[28] For more details about the development of this privacy research field among computer scientists, see: Seda Gürses and Bettina Berendt, "PETs in the Surveillance Society. A critical review of the potentials and limitations of the privacy as confidentiality paradigm," in *Data protection in a profiled world*, ed. Serge Gutwirth, Yves Poullet and Paul De Hert (Dordrecht Heidelberg London New York: Springler, 2010).

[29] Seda Gürses, *Multilateral Privacy Requirements Analysis in Online Social Network Service. PhD thesis* (Leuven: HMDB, Department of Computer Science, K.U.L., 2010), 5.

[30] Within the computer science community, it's worth noting that similar objectives – going beyond simple compliance - have already guided the development of requirements methods which are especially interesting since they often go beyond questions of legal compliance and propose new ways of approaching the privacy problems. The preliminary work in this direction is: A. K. Massey and A. Antòn, "A requirements-based comparison of privacy taxonomies", *Requirements Engineering and Law*, 2008. An interesting one which formalizes access control models using the privacy framework proposed in 2004 by the legal scholar Helen Nissenbaum: Adam Barth et al., "Privacy and Contextual Integrity: Framework and Applications", *SP '06: Proceedings of the 2006 IEEE Symposium on Security and Privacy*, May, 2006: 184-98. The thesis of Seda Gürses already mentioned is another attempt to follow a similar direction.

made by social sciences in their links with decision-making processes. They are worth underlying in order to avoid the risks identified.

1.4.2.1 The social Acceptability Paradigm

Anthropology - like other disciplines among the social sciences[31] as e.g. psychology, psychosociology, philosophy, political sciences, ethics, etc. - has been used in diverse studies and surveys about the public perception of privacy, or of privacy and security, or privacy and surveillance. Unfortunately, it is worth noting that some of these uses have been proven to be methodologically weak, their findings and conclusions being often biased, yet these are interpreted and used selectively by participants in the process of policy-making to support their different causes.[32] Among the many traits that explain this methodological weakness, there are, for example:

- the methodological opacity of surveys regards to the methodology that have been used to get and to analyze their results;
- the elusive wording of the questions that makes unsure the way the question and the response may be interpreted:
    a. asked in terms of general concepts - privacy, surveillance, security, liberty – where elusiveness and confusions – for example between technologies and practices of surveillance and/or of privacy – are common[33];
    b. asked in the form of a trade-off between privacy and other values such as security rather than put in concrete situation. Indeed, as an example of question asked you may find such a wording: “would you accept to lose parts of your privacy in order to guarantee a better security to your family?”;

[31] The category of “social sciences” is here used with ease to designate all the academic disciplines which are not included in natural and engineering sciences. More specifically, regards to the multidisciplinary perspective adopted in this PARIS project, to designate the academic disciplines which study humans in their constitutive relation to themselves or their environment: e.g. psychology, sociology, anthropology, philosophy, political sciences, etc.

[32] There is an important methodological study made by the “PRISMS Project”, in its Deliverable D7.1 “Report on existing surveys”, about the perception of the public regards to privacy. They identify and methodologically analyse existing public opinion surveys regards to privacy and security/surveillance. They compiled an inventory of about 260 surveys, from 1985 to early 2012. Nevertheless, this study reports that, among those 260 surveys, very few are of good quality regarding methodological considerations. See: Haley Watson and David (ed.) Wright, "Deliverable 7.1: Report on Existing Surveys," in *PRISMS. The PRIvacy and Security MirrorS: Towards a European framework for integrated decision making.* (EC: Seventh Framework Programme, March 2013). Available at http://prismsproject.eu/wp-content/uploads/2013/03/PRISMS-D7-1-Report-on-existing-surveys.pdf

Another interesting study was conducted within the “SAPIENT Project”, in part 4 of its Deliverable 1.1 Smart Surveillance- State of the art. This section studies citizen’s perceptions on surveillance and privacy, with a special focus on public sector practices of surveillance, where “these are framed in a discourse promoting security through surveillance”. This study analyses academic discourses and empirical researches. Specifically, it addresses methodological questions to the empirical researches,- e.g. how the public opinion is measured? How is framed the most prominent research tool used to measure them, that is the survey? How are analyzed the results of those surveys in order to decide upon the public acceptance of surveillance and of specific surveillance technologies? See: Michael Frieddewald and Rocco Bellanova, "Deliverable 1.1: Smart Surveillance - State of the Art," in *SAPIENT. Supporting fundamental Al rights, Privacy and Ethics in surveillance Technologies* (EC: Seven Frameworks Programme, January 2012), 129-84.

[33] (Harper et Singleton s.d.)

- the difficulty to get the identity of the client who command the survey and, therefore, their interests and purposes in commissioning it.
- Etc.

Another feature of the uses of social sciences in studies and surveys about the public perception of privacy is also worth noting, while being more directly link to individual traits. Indeed, the types of categorization used in order to organize the panel of respondents, while using social and anthropological traits - e.g. gender, age, ethnicity, philosophical and political views - is at risk of reproducing and/or prolonging the discrimination induced by the categorization of individuals. This is especially critical when the political or personal histories of the respondents are not taken into account to structure the surveys and to assess their results. In this case of isolation of individual traits from the context (personal, social, political...) in which they appear, those individual traits look like having a causal and explanatory strength on perception of privacy that, actually, is unjustified as soon as other elements are taken into account. Indeed, as an example we can mention that "different countries' political histories vary greatly in terms of the populations experience with different state propensities to interfere with privacy and to maintain extensive and intensive surveillance".[34] Those methodological difficulties and bias are of general nature in social sciences and are well documented.

In this context, it is worth noting that any survey which may feed or influence a decision-making process regards to privacy, including when they are parts of rhetorical campaigns led in mass-media, is at risk of falling in what has been called **the social acceptability paradigm**[35]. This latter has been identified in the well documented academic work which has been produced over those last 30 years, since in particular the widespread public campaigns in relation to nuclear energy and environmental controversies.

In such a paradigm, the discipline aims at establishing scientifically the political necessity for a public and for society of a proposed technology, mainly by showing that the public perception is in deficit regards to this technology and by proposing the manners and the tools to make it acceptable for the public (e.g. with a better communication with the public about the technology in question or with the development of educational frames about this technology). What is central in this paradigm is what has been called **the deficit model of science and technology**: the public rejection or resistance to new scientific and technological developments is sawn solely as an outcome of a lack of information or understanding or knowledge about

[34] Haley Watson and David (ed.) Wright, "Deliverable 7.1: Report on Existing Surveys," in *PRISMS. The PRIvacy and Security MirrorS: Towards a European framework for integrated decision making.* (EC: Seventh Framework Programme, March 2013). For more details about methodological remarks regards to surveys which focus on the elicitation of privacy attitudes in a variety of countries: Elia Zureilk and Lynda Hardling Stalker, "The Cross-Cultural Study of Privacy: Probelms and Proepcts," in *Surveillance, Privacy and the Globalization of Personal data: International Comparisons*, ed. Elia Zureik et al. (Montreal & Kingston: McGill-Queen's University Press, 2010), 8-30.

[35] By paradigm, I refer, as above about the privacy-surveillance paradigms, to a set of assumptions about their relations and their definitions. These assumptions collectively set the agenda of argumentation, policies and research and yet are often not made explicit. A paradigm produces an approved, common and implicit understanding about the nature and scope of a particular problem. It provides a way to organize and discuss relevant assumptions, arguments and theories underlying it, included the problems they address and the errors they induce.

these scientific and technological developments and the benefits to society and citizens associated with them. Put in short: objective knowledge belongs to the side of an already made political decision in favour of a technology and the public has only perceptions and opinions about its development in its daily life, perceptions and opinions which have to be corrected if they do not equate with the knowledge-based political decision. This paradigm has been widely analyzed and criticized in the last years[36]. One of this work's outputs is in showing that campaigns aiming simply to "inform and educate" the public of the benefits of technologies encounter with little success regarding the preliminary objectives of information, education and acceptance.[37]

1.4.2.2 Public Engagement

In order to move beyond the deficit model of science and technology, social scientists have introduced and developed new conceptions of engaging public into sciences and technologies. One line of research has been in offering a specifically well-built theoretical reasoning in stressing public attitudes to those technologies that might be considered controversial or with strong implications for citizens and societies and in highlighting alternative meanings to give to these resistance attitudes.[38] Indeed, an important theoretical and empirical work has been produced which demonstrates the links between public involvement - be it resistance or acceptance or engagement - to new technologies and the manners sciences and technological research are conducted and governed.[39] The study of the governance of science and technologies has become an important subject for theoretical and empirical work in social sciences, and more specifically in the field of research of science studies. "So successful has some of this been that in examining European funded research, the call for the public to be engaged or involved with the research and innovation process has been a critical development.

[36] We are waiting for the deliverable of the EU project PRISMS in which a part will be devoted to this social acceptability paradigm regards to privacy and surveillance technologies. There is already some important insights dealing with public acceptance and public perception of privacy, and of privacy and security in the fourth part of the deliverable 1.1 of the SAPIENT Project: Michael Frieddewald and Rocco Bellanova, "Deliverable 1.1: Smart Surveillance - State of the Art," in *SAPIENT. Supporting fundamental Al rights, Privacy and Ethics in surveillance Technologies* (EC: Seven Frameworks Programme, January 2012), 175-84.

For a general overview of the social acceptability paradigm, see: Daniel Barben, "Analyszing acceptance politics: Towards an epistemological shift in the public understanding of science and technology", *Public Undesrtanding of Science*, 19(3) (2010): 274-92.

See also studies for specific technologies, e.g. Genetically Modified Organisms: L. Levidow and Cl Marris, "Science and Governance in Europe: lessons from the case of agricultural biotechnology", *Science and public policy*, 2001: 345-60. And: Nathalie Trussart, "Publics et expérimentations", *Multitudes*, 23 (2005): 169-79. And : Tom Horlick-Jones, *The GM debate: risk, politics and public engagement* (London: Routledge, 2007). About the nanotechnologies: François Thoreau, *Embarquement immédiat pour les nanotechnologies responsables. Comment poser et re-poser la question de la réflexivité?* (Liège: Université de Liège, 2013).

[37] James Wilsdon and Rebecca Willis, *See through science: Why public engagement needs to move upstream* (London: Demos, 2004). Available at: http://www.demos.co.uk/files/Seethroughsciencefinal.pdf?1240939425

[38] See as an example of such a work: Lisa M. Pytlikzillig and Alan J. Tomkins, "Public engagement for informing science and technology policy: What do we know, what do we need to know, how do we get there?", *Review of Policy Research*, 28 (2) (2011): 197-217.

[39] For a general overview, see: Monica Kurath and Priska Gisler, "Informing, involving and engaging: Science communication in the ages of atom, bio- and nanotechnology", *Public Understanding of Science*, 18 (5) (2009): 559-73.

This has shaped how European science and technological innovation is conducted and performed through mechanisms of public engagement in science and technology policy. This deliberative and participatory approach has leg arguably to a democratising of science and technology policy".[40] Indeed, "seeking to engage and involve the public in science and technology discourse has been one strand of a potential democratising of science and technology policy".[41]

Same theoretical efforts - in moving beyond the deficit model of public and developing models of public engagement into science and technology - have been made about surveillance technologies and more especially about new and controversial surveillance technologies.[42] However, the particular argumentative setting in which surveillance technologies are deployed - i.e. with redundant links made to (national) security, war on terror [43] - has made this approach difficult to implement both into opinion 's surveys and political agenda. "For example, citing decision as being in the national interests (whether justifiable or not) means opening up such processes to public engagement or involvement difficult to achieve".[44] Some authors have argued that public resistance to implementations of new surveillance practices or technologies "will continue unless new models of public engagement are pursued" regards to new surveillance technologies.[45]

Well inspired by former works made in environmental studies, in life sciences and in sciences and technologies studies, several attempts of public engagement – participative technology assessment (PTA), interactive technology assessment (ITA), workshop around scenarios, etc. - regards to surveillance technologies have been made and several tools as be created and experimented. It is not our mandate to make a complete review of them.[46] Nevertheless, it is

[40] Michael Frieddewald and Rocco Bellanova, "Deliverable 1.1: Smart Surveillance - State of the Art," in *SAPIENT. Supporting fundamental Al rights, Privacy and Ethics in surveillance Technologies* (EC: Seven Frameworks Programme, January 2012), 178.

[41] *I*bid, 181.

[42] For a reading of European research projects which have participated in these efforts, see Michael Frieddewald and Rocco Bellanova, "Deliverable 1.1: Smart Surveillance - State of the Art," in *SAPIENT. Supporting fundamental Al rights, Privacy and Ethics in surveillance Technologies* (EC: Seven Frameworks Programme, January 2012).

[43] For more details about the historical development of this link between privacy, surveillance, (national) security, war and terror, see: Darren W. Davis and Brian D. Silver, "Civil Liberties vs. Security: Public Opinion in the Context of the Terrorist Attacks on America", *American Journal of Political Science*, 48 (1) (2004): 28-46. See also an overview of the effects beyond America: D. Bigo and A. Tsoukala (ed.), *Terror, Insecurity and Liberty: lliberal Practices of Liberal Regimes after 9/11* (London: Routledge, 2008). And also: L. Amoore and M. De Goede (ed.), *Risk and the War on Terror* (London: Routledge, 2008).

[44] Michael Frieddewald and Rocco Bellanova, "Deliverable 1.1: Smart Surveillance - State of the Art," in *SAPIENT. Supporting fundamental Al rights, Privacy and Ethics in surveillance Technologies* (EC: Seven Frameworks Programme, January 2012), 178.

[45] Ibid., 178.

[46] For a review of several of those models of public engagement, both theoretical and practical, see: Michael Friedewald, "Deliverable 2: Engaging stakeholders and civil society in the assessment of surveillance practices," in *SAPIENT: Supporting fundamentAl rights, PrIvacy and Ethics in surveillaNce Technologies* (EU: Seven Framework Programme for Research and technological development, 2012).

For a general overview and analysis of those tools which are likely to help in involving "a public" around issues relating to new technologies, see: V. Beekman and F. W. A. Brom, "Ethical tools to support systematic public deliberations about the ethical aspects of agricultural biotechnologies", *Journal of Agricultural and Environmental Ethics*, 20(1) (2007): 3-12.

worth noting that added to the traditional stakeholders taken into account regards to surveillance technologies, that those who are involved in developing, implementing and operating surveillance systems, as well as the technological, economic, political and social drivers associated with this implementation – government and public authorities, industry, academia, policy makers, NGOs, the media – there is also civil societies and citizens or groups of citizens who are targets of surveillance technologies or who simply are or may be supporting the effects of those technologies. Indeed, in the case of surveillance technologies, people who are under surveillance are not end-users. But more important is the asymmetrical stakeholder participation in different decision-making processes or Privacy Impact Assessment exercises. From a practical perspective, "not all stakeholders have the same possibility to participate in key meetings and key moments of the decision-making, and, even when they can attend, they do not have adequate resources to weight their opinions in the same way as other non-institutional actors (such as private companies)".[47] The effective participation of civil society in a decision-making process or a PIA exercise has impacts on the credibility of those processes and exercises and on the trust civil societies, citizens and consumers may place in the actors who are in charge of them[48].

It is not the mandate of the SALT Framework to respond to this challenge of engaging a public into surveillance system-to-be. Nevertheless, it is of interest for the SALT Framework to be aware of those issues concerning the asymmetrical stakeholder participation in different decision-making processes and the democratic importance of the involvement of citizens into the development of surveillance technologies in order to guarantee credibility and trust.

1.4.2.3 "ethicAl"

Those arguments presented above were sufficient to make us think about another word to anchor the **A** of the SALT Framework, regards to the knowledge likely to feed the SALT Framework. Two main constraints guide this choice. (1) The first one is to avoid the use that has been made by academic knowledge in favour of social acceptability paradigms and the methodological bias that have been induced by such a posture. (2) The second one is to inform about individual and collective dimensions of privacy.

While seeking for a new wording of the SALT framework, it is also the methodological and epistemological question about the possible academic disciplines we may use in this research that are at stake.

See also: Volkert Beekman et al., "Ethical Bio-Technology Assessment Tools for Agriculture and Food Production. Final Report Ethical Bio-TA Tools," in *Ethical Bio-TA Tools* (EC: Fifth Framework Programme, February 2006).

[47] Michael Friedewald, "Deliverable 2: Engaging stakeholders and civil society in the assessment of surveillance practices," in *SAPIENT: Supporting fundamentAl rights, PrIvacy and Ethics in surveillaNce Technologies* (EU: Seven Framework Programme for Research and technological development, 2012), 42.

[48] About the importance of trust and concerns in the relationships between privacy and security, see: Anthony Amicelle et al., "D1.1. Report on Theoretical Frameworks and Previous Empirical Research," in *PACT. Public perception of security and privacy. Assessing knowledge Collecting evidence, Translating research into action* (EC: Seventh Framework Programme, 2012).

PARIS' concern is surely to take into account both **collective and individual dimensions of privacy**. Those dimensions are not conceptualized as opposite but as relating to each other in mutually constitutive ways.[49] While institutional or organizational contexts do not determine completely the behaviour of actors, they nevertheless mark a range of options for decision-making and acting. On the other hand, people's work, lives and identities are shaped by their participation in contexts that determine what is relevant to them – many processes that imply their sense-making.

Three possible terms were proposed: agentiAl, contextuAl and ethicAl. First, **agential** was considered. In their aim of avoiding the dichotomy between society and individuals, social and political scientists propose the couple of following notions: society and agency (the capacity of an agent, an actor, to act)[50]. But it sounds quickly too specific to social and political scientists. Second, **contextual** was considered, well inspired in this change by Helen Nissenbaum's book, i.e. "Privacy in context"[51] in which she invites the reader to consider privacy in the specific context where it is an issue: an hospital is a very different context than an airport. While this focus on context of surveillance and privacy is an important feature we focus on in this project, with the only social and context dimension's, we take the risk to lose important characteristics of individual's dimensions of privacy and to make those dimensions invisible in the wording of the SALT Framework. We finally adopted **ethicAl**. While maintaining a special care for the individual's dimensions, this term allows avoiding the very old and confusing debate in sociology about the relation between individuals and society, while being ground on well documented studies which tend to include ethical concerns to privacy issues.

For all those reasons, from now on, the **SALT Framework** refers to the **S**ocio-political, ethic**A**l, **L**egal and **T**echnical dimensions of privacy.[52]

[49] This constitutive approach on collective and individual dimensions was well initiated and theorised in the pragmatist tradition of social and political philosophy, with the aim of avoiding the endless and confusing debate about the relation between individuals and society. See one of the coiners and promoters of this approach: John Dewey, *The public and its problems* (Ohio: Swallow Press, Ohio University Press, 1991).

In the sociology tradition, Anthony Giddens is also well known to have developed alternatives to the dichotomy between society and individuals, with his theory of structuration, ana analysis of agency and structure, in which primacy is granted to neither. See: Anthony Giddens, *The Constitution of Society. Outline of the Theory of Structuration.* (Cambridge: Polity, 1984).

More recently, in United-States, this approach was largely developed by post-structuralism theories. A very good example of its use in Privacy Studies is Seda Gürses' PhD thesis: Seda Gürses, *Multilateral Privacy Requirements Analysis in Online Social Network Service. PhD thesis* (Leuven: HMDB, Department of Computer Science, K.U.L., 2010).

[50] See one of the coiners of "agential" perspective: Anthony Giddens, *The Constitution of Society. Outline of the Theory of Structuration.* (Cambridge: Polity, 1984). Bruno Latour also developed agential proposals. See: Bruno Latour, *Reassembling the Social: An Introduction to Actor-Network Theory* (Oxford, UK: Oxford University Pess, 2005).

[51] See: Helen Nissenbaum, *Privacy in Context. Technology, Policy and the Integrity of Socail Life* (Standford: Standford University Press, 2010).

[52] The conduct of the following state of the art into socio-political, ethical, legal and technical aspects of privacy will be led while being aware of the criticisms addressed to this kind of study known as "ethical, legal and social aspects or implications (ELSA/ELSI) studies". Indeed, the main criticism of the ELSA approach made by social scientific disciplines is that "ethics and law have been central to ELSA research becoming institutionalised in the decision-making and policy process" because "ethics and legal approaches are perceived as giving easy answers which policy makers can utilise ", in terms of simplistic binary alternatives (i.e. ethical or not, legal or not). This criticism echoes the ones already exposed about the social acceptability paradigm. The same solution to avoid

1.5 A Multidisciplinary Approach

A rapid overview of the recent research initiatives funded by the European Commission within the Seventh Framework Programme (FP7, 2008-2013) and United States agencies such as the Defense Advanced Research Project Agency (DARPA) and the National Science Foundation (NSF) shows that the majority of the EU projects and the totality of the US ones are technical, i.e. "they focus on engineering issues and technological development and demonstrations".[53]

However, in Europe, there is also a place devoted to the analysis of the broader ethical and legal issues related to surveillance and security technologies: there is an "ethics, security and society" theme in the Security Programme under Activity 6 (Security and Society) in the current Seventh Framework Programme where several related "Science and Society" themes cover also social and individuals implications of surveillance and security technologies.[54] Among this European research landscape, yet, it is still a singularity to lead a multidisciplinary research on privacy where computer scientists and legal scholars and scientists coming from social sciences, partners coming from private and public sectors, work together as it is the case in the PARIS project. This situation requests some methodological insights in order to be able to work together.

such a risk has been proposed: the incorporation of stakeholders and publics into the research process, in order to give them the opportunity to express their views and correct the ones expressed in the studies. See: Michael Frieddewald and Rocco Bellanova, "Deliverable 1.1: Smart Surveillance - State of the Art," in *SAPIENT. Supporting fundamental Al rights, Privacy and Ethics in surveillance Technologies* (EC: Seven Frameworks Programme, January 2012), 182.

[53] See: Michael Frieddewald and Rocco Bellanova, "Deliverable 1.1: Smart Surveillance - State of the Art," in *SAPIENT. Supporting fundamental Al rights, Privacy and Ethics in surveillance Technologies* (EC: Seven Frameworks Programme, January 2012), 76.

[54] Different EU research projects which may be of interests for the PARIS project are:

- SAPIENT
- PACT
- PRISMS
- ADDPRIV
- INEX
- DETECTER
- FESTOS
- FORESEC
- ETICA
- HIDE
- RISE
- PRESCIENT
- PRACTIS

1.5.1 Privacy: a « Slippery Concept »[55]

As many scholars have already stated, privacy is "a flexible and fluid concept"[56], for which there is no single definition or meaning[57], a concept which is very difficult and challenging to define[58].

> "Attempts to define it have been notoriously controversial and have been accused of vagueness and internal inconsistency – of being overly inclusive, excessively narrow, or insufficiently distinct from other value concepts"[59].

Is privacy "a claim, a right, an interest, a value, a preference or merely a state of existence"[60]? The enterprise of defining privacy conceptually has often resulted in adding confusion to the point of, eventually, thwarting progress in helping to clarify privacy issues. The one of describing empirically the way people do experience their privacy, either individually or collectively, has not filed better results. Indeed, a lot of empirical surveys about the perception citizens have of privacy in general and of their own privacy in particular are of poor methodological quality, as a very recent study shows[61].

The difficulties are very important while attempting to grasp the parameters which make sense of privacy and privacy harms for people or groups of people and while attempting to give an account of them in order to reinforce privacy protection against possible privacy harms, risks and concerns. Taking in isolation those parameters have no utility while most of them overlap and interact with each other, are possibly in contradiction or in mutual reinforcement, are highly dependent of a political regime, a personal and/or a political history, and while their relevance concerning privacy issues is possibly changing regards to the type of surveillance technology at hand and the specific context in which they operate. Among those classical parameters, there are: class, race, sex, age, culture, country, profession, social statute, health, political regimes, legal system, economic wealth and/or (in)stability in their country, surrounded or not by trustworthy people (friends, family), etc.

Although the admission of inability to grasp the concept of privacy has become an obligatory exercise opening any study devoted to this matter, a wise first step is to start "by identifying a series of different ways that the topic of privacy is approached in the research literature".[62]

---

[55] James Q. Whitman, "The two western cultures of privacy: Dignity Versus Liberty", *The Yale Law Journal*, 113 (2004): 1153-54.

[56] (Dourish et Bell, Divining a digital future 2011, 143)

[57] Judith DeCew, "Privacy," in *The Standfordf Encyclopedia of Philosophy*, ed. Edward N. Zalta (Standford: The Metaphysics Research Lab, 2012). Available at http://plato.stanford.edu/entries/privacy/).

[58] Helen Nissenbaum, *Privacy in Context. Technology, Policy and the Integrity of Socail Life* (Standford: Standford University Press, 2010), 1-4.

[59] Ibid., 2.

[60] Ibid., 2.

[61] Haley Watson and David (ed.) Wright, "Deliverable 7.1: Report on Existing Surveys," in *PRISMS. The PRIvacy and Security MirrorS: Towards a European framework for integrated decision making.* (EC: Seventh Framework Programme, March 2013).. Available at: prismsproject.eu/wp-content/uploads/2013/03/PRISMS-D7-1-Report-on-existing-surveys.pdf

[62] Paul Dourish and Ken Anderson, "Collective Information Practice: Exploring Privacy and Security and Culture Phenomena", *Human-Computer Interaction*, 21(3) (2006): 319-42.

1.5.2 From Multi- to Inter-Disciplinary Approach

In this PARIS project, the multidisciplinary approach has been chosen in order to give to all the partners engaged the full opportunity to make visible from the perspective of its own discipline and background, the different ways that the topic of privacy has been approached. In that sense, this multidisciplinary approach is a first step before a second one which will be defined as an interdisciplinary approach and which will be useful for the second task of the WP2 devoted to the structure and dynamics of SALT Framework.

A multidisciplinary approach is defined as the presentation of privacy as it is developed inside different disciplinary frameworks.

Beside the aims of understanding each other among the different partners of the project, and to create a common vocabulary, the multidisciplinary phase is also a way to introduce ourselves to each other from the perspective and the constraints proper to our own discipline, knowledge and background. While situating the way we pose, we word and we solve problems in our own discipline, we present situated knowledge and situated practice[63] to each other. We may say that it is a polite manner to get acquainted.

An interdisciplinary approach is defined as the work between disciplines from the perspective of what may be blinding in them regards to privacy issues. The hypothesis is that the difficulties and controversies existing inside a discipline, in its aim of understanding and protecting privacy, will receive a better understanding with the help of the other disciplines. While identifying the limits of our mainstream discipline regards to privacy issues, the interdisciplinary work is needed in order to look outside our discipline and draw insights from other disciplines.

1.5.3 Benefits of this Approach

Multi-perspectivism and disciplinary perspectives are the first step before the interdisciplinary work. The emphasis on **disciplinary** practices serves for reminding several traits of this research:

- A State of the art: **research literature.**
- A research practice and its **internal controversies** or **different points of view on privacy issues and privacy impacts**.
- A research practice **among other research practices**.
- Researches practices **among other kind of practices** through which privacy or privacy impacts make sense.

The advantages of this approach are:

- It helps **avoiding the temptation of grasping an essence of privacy**, a core concept with stable characteristics and to keep an elusiveness for the privacy concept. More about the advantages of this elusiveness is expressed thereafter.

[63] The concept of situated knowledge was coined by the feminist philosopher Donna Haraway. See: Donna Haraway, "Situated Knowledges: The Science Question in Feminism and the Privilege of Partial Perspective", *Feminists Studies*, 14 (3) (1988): 575-99.

- It **makes less evident the "implicit feeling" or "common sense"** most of us share about privacy and attempt to produce a rationale and reflexive knowledge on what is and what might be privacy in order to ensure it a better protection.
- It makes **visible the constraints and values which animate a specific disciplinary construction of privacy,** without giving any privilege to one discipline to the exclusion or detriment of others.
- It helps avoiding the **methodological and political risks** already mentioned above such as a technocentricity posture or the participation to the social acceptability paradigm.

1.5.4 Elusiveness and Undecidability

Starting from a multi-perspectivism approach does not solve the problem of how to articulate the different conceptions of privacy. This problem of articulation induces more precise questions, like:

- **WHAT**: what is holding the articulation (e.g. what technical system? A decision-making process? A practice of judging?)?
- **WHO**: who is in charge of articulating these different conceptions (e.g. a legislator? A judge? A computer scientist?)? And for which purposes (e.g. a decision-making process? An impact assessment? A judging practice?)
- **HOW**: What are the **procedures, the constraints, the criteria** adequate to reach this articulation with regard to the specific practice of the person (or people) who are in charge with this articulation?
- **SCOPE**: What are the scopes of the articulation and what are the zones which should not be articulated, regards to the responses to the previous questions? Those zones are the **zones of undecidability.**

Let's illustrate this with an example.

In 1992, "the European Court of Human Rights (ECtHR) has ruled that it is neither possible or necessary to determine the content of privacy in an exhaustive way. Furthermore, **maintaining flexibility in a conceptualisation of privacy could ensure that a wide range of issues** such as integrity, access to information and public documents, secrecy of correspondence and communication, protection of the domicile, protection of personal data, wiretapping, gender, health, identity, sexual orientation, protection against environmental nuisances and so on **are covered by the law**".[64]

The argument in favour of the elusiveness of the concept of privacy is, in this case, expressed from the perspective of a judging practice (WHAT), which involves for the judge (WHO) the responsibility to "qualify" in law (HOW) what is privacy and what is a privacy harm. Regards to this practice, the judge has to articulate different dimensions of privacy and has to leave some of those dimensions out of the scope of his/her practice of judging. The borders between the articulated zones and the zones of undecidability are not framed once for all, rather their

[64] Niemietz vs. Germany and Pretty vs. UK, Judgement of 16 December 1992.

possible redefinition, regards to novelty (the case, the issues, the technology involved and so on) is part of the practice of judging.

Those zones of undecidability are also of interests for the SALT Framework. There are several reasons for this:

- In order to avoid for the system (the SALT Framework management tool) to take the place of decision-making processes that it is devoted to help finalizing and that is in charge of possible redefinition of the borders between zones which has to articulated and those which has to remain undecidable.
- In order to be able to adapt e.g. to the emergence of new surveillance technologies, new negative impacts on privacy, new public claims regards to their privacy, new rules regards to privacy.

For any practice which is engaged in its protection, privacy has become a "key lens through which many new technologies, and most especially new surveillance technologies, are critiqued."[65] "The notion of privacy remains out of the grasp of every academic chasing it. Even when it is cornered by such additional modifiers as 'our' privacy, it still finds a way to remain elusive", says Serge Gutwirth who explains why privacy is substratum of democracy and "of contemporary Western Society because it affects self-determination; the autonomy of relationships, behavioural independence; existential choices and the development of one's self; spiritual peace of mind and the ability to resist power and behavioural manipulations." [66]

Many scholars have argued in favour of the elusiveness of the privacy's concept for the main reason that its inherently heterogeneous, fluid and multiple dimensions "may be necessary to provide a platform from which the effect of new technologies can be evaluated" and, therefore, the relevant protection be identified and created. "This potential necessity is supported by the fact that different technologies impact upon different types of privacy, and further technological changes may introduce or foreground previously unconsidered privacy dimensions".[67]

1.6 Deliverable Structure

This public reporting document describes the approach adopted by PARIS in the task of getting an understanding of the contexts and the concepts relevant for developing SALT frameworks. (Work Package 2 – WP2, Task 1). In order to achieve this task, the following activities are performed in this deliverable.

[65] Rachel L. Finn, David Wright and Michael Friedewald, "Seven Types of Privacy," in *European Data Protection: Coming of Age*, ed. Serge Gutwirth (Dordrecht: Springer, 2013), 4.

[66] Serge Gutwirth, *Privacy and the Information Age* (Lanham/Boulder/New York/Oxford: Rowman 1 Littlefield Publishers, 2002), 30.

[67] Rachel L. Finn, David Wright and Michael Friedewald, "Seven Types of Privacy," in *European Data Protection: Coming of Age*, ed. Serge Gutwirth (Dordrecht: Springer, 2013), 26.

Chapter I (Introduction: A Multidisciplinary Approach to Privacy) aims at providing a general introduction of the deliverable. After recalling its objectives and scope, it starts with a section which is dedicated to terminology where conceptual remarks needed for the well understanding of the progression of this study are made. First ones concern the important notion of "privacy". Second ones concern the notion of "surveillance". Third ones concern privacy-surveillance paradigms. Different rationales are exposed regards to the balance between surveillance and privacy. Following a section devoted to the concept of privacy-by-design, the risks and the challenges of this approach. Then, as a result of those precedent remarks, a set of observations concerns the prism through which the SALT Framework is developed and offers the opportunity to underline the uniqueness of the SALT framework compared to other privacy frameworks used for the privacy by design of a system-to-be. Finally, a final round of remarks concern the multidisciplinary approach adopted in this text.

Chapter II (Privacy from Socio-Political and Ethical Perspectives) focus on different parts: one about psychosocial perspective, one about socio-political perspective and a last one regards to ethical perspectives. The section ("Privacy from a Psychosocial perspective") deals with the privacy of systems seen from psychosocial perspective. It includes different definitions of privacy relevant to the PARIS project, stressing the Altman' psychosocial model of privacy[68]. Then it discusses the different dimensions of privacy (solitude, isolation, anonymity, reserve and intimacy) and adds a classification depending on the privacy spaces (public spaces, semi-private and private spaces). Besides, this section also explains the effects of lack of privacy and the relationship between the psychological perception of privacy and the effects of the lack of privacy. Finally, this part of the document identifies the different functions and types of privacy and the relationship between them. The following section ("Privacy form a Socio-political perspective") is devoted to privacy as it is theorized from a socio-political perspective, by socio-political scholars and legal theorists. After a general overview of the main claims from the socio-political perspective, this section suggests that for the purpose of the framing of the SALT Framework, a good starting point is the study and analyse of different existent taxonomies, their benefits and defaults. The last section ("Privacy from an ethical perspective") follows the same structure. It begins with a general overview of the main claims regards to ethical dimensions of privacy and of the context of the use of ethics at the European Union level. The chapter closes with some existing manners to apprehend privacy's ethical dimensions and existent ethical framework which are of interest for the integration of ethical issues in the SALT framework.

Chapter III (Privacy from a Legal Perspective) aims at providing a global review of the European legal requirements in the matters of privacy and data protection, in particular in order to understand the balance between privacy public space, understood as the extent to which privacy interests are at stake when surveillance systems are deployed, especially in public spaces, and the legal 'concepts' that the SALT framework will have to integrate. In this aim, the chapter is divided in six parts. The first section will come back on the essential issues of the debate surrounding the *privacy v. public security balance* in the European Union in order to have an overview of the legal "context" within which the PARIS project intends to produce

[68] Irwin Altman, *The environment and social behavior: Privacy, personal space, territoriality and crowding* (Monterey (Ca.): Books/Cole, 1975).

innovative solution. The second section will present the legal landscape of the protection of privacy and personal data in the Member States, which will be the occasion to identify the main relevant normative sources that may be taken into account by the SALT framework. The third section will present the caselaw of the European Court of Human Rights (ECHR) with regard to the right to private life and data protection, with specific attention on some important developments in relation to the extent of protection of private life to informational issues and public surveillance. Section four will present the core concepts and principles enshrined in the Directive 95/46, which is the main relevant EU wide instrument on the protection of personal data applicable in all Member States. Finally, because this instrument does not address the issues of protection of personal data in relation to specific surveillance technologies, we will look at European guidance with regard to videosurveillance activities (section five) and biometric technologies (section 6), which are PARIS use cases, and how these matters are dealt with in two Member States, Belgium and France.

Chapter IV (Accountability by Design – a Way to Ensure Transparency and Trust) proceeds to a review of the state-of-the-art on the principle of accountability in view of extracting preliminary criteria for the design of an accountability-based approach for personal data governance practices within the SALT framework. In section 1, we will see that "accountability" is a concept 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 "mechanism of control" and that both approaches are of interest for the SALT Framework. As elaborated in section 2 we will see that both concepts share common features. In short, accountability relationships involve a third party external to the accountable agent and in which the latter is asked to answer the requests of the former, which may result in corrective actions taken by the agent. The review of the different initiatives in view of the introduction of an accountability-based approach within the data protection framework in section 3 shows that they approach accountability as implementation and enforcement mechanism of the existing framework, although none of the policy instruments reviewed provides for a definition of the principle of accountability. The different initiatives reviewed do however not address the specifics of surveillance practices, which means that further work is required to tailor these preliminary criteria to the context of surveillance. The next deliverable (D.2.2.) will build on the findings of this Chapter to provide a definitive list of requirements, adapted to the context of surveillance.

Chapter V (Privacy from a Computer Engineering Perspective) deals with the privacy of systems seen from a technological point of view. The most common principles for privacy are listed, including OECD principles. With these principles in mind, the section defines some important concepts related to ICT privacy (such as anonymity, pseudonymity, unlinkability, etc.) and privacy in video-surveillance systems. Privacy-enhancing technologies are also mentioned: encryption, access control, obfuscation, etc. Once the basis of privacy is planted (i.e., principles and concepts) this section disserts about new technologies and how they affect current systems' privacy (making a distinction between hardware and software advances), and nowadays advances in connectivity and ubiquity. Finally, it focuses on the different applications and technologies regarding to surveillance and what type of impact they can have on people. Considering PARIS project main use-cases (i.e., video-surveillance and biometrics systems) a large set of heterogeneous surveillance systems are described: imaging scanners, satellites,

photography, fingerprint recognition, iris recognition, dataveillance, GPS, etc. Biometric systems functionality is also described for a better understanding of this type of systems.

Chapter VI (Preliminary Recommendations for the SALT Framework) concludes with **recommendations** to be considered in the development of SALT Frameworks and, as a consequence, in the preparation of the next deliverable. Those recommendations are based on all previous findings identified within this report.

2 Privacy from a Socio-Political and Ethical Perspectives

2.1 Introduction

With the objective of helping in the characterisation and definition of relevant criteria that have to be considered in the making of the SALT Framework, this chapter provides a state of the art analysis of different conceptions on privacy and its relations to surveillance technologies from the perspectives of different social sciences. The chapter is structured in three sections. The first one focuses on psychological and psycho-social perspectives on privacy. The second one is devoted to the socio-political perspective on privacy. The third one deals with ethical perspectives on privacy.

2.2 Privacy from a Psychosocial Perspective

Carmen Hidalgo, Antonio Maña, Fernando Casado and Francisco Jaime (University of Malaga)

One of the main goals of this deliverable is providing knowledge for the future creation of SALT frameworks from multidisciplinary perspectives. The psychological sciences are of interest in the aim of completing a wide understanding the balance between privacy and surveillance technologies. Therefore, in this section we will concentrate on the psychological perspective, but not in isolation, but with the aim of using this perspective in an integrated way with other perspectives and in relation to the project objectives.

2.2.1 Definitions

Nowadays there is a considerable level of confusion and ambiguity for psychologists who work in the research field of privacy[69]. Attempts to understand and analyse privacy are focused on several single perspectives, as diverse as anthropology, ethology, politics, sociology, law, and psychology. As a result, there are many different definitions of privacy found in the literature.

Even from a psychological point of view, we find different definitions of privacy relevant to this project:

- "Freedom to choose what, when and to whom one communicates" and "personal control over personal information"[70].
- "Control of personal space"[71].
- "A voluntary and temporary condition of separation from the public domain"[72].

[69] Darhl M. Pedersen, "Model for types of privacy by privacy functions," *Journal of Environmental Psychology,* 19 (1999): 397-405.

[70] Alan Westin, *Privacy and Freedom* (New York: Atheneum, 1967).

[71] Jeffrey D. Fisher, Paul A. Bell & Andrew Baum, *Environmental Psychology*, 2nd Edition (New York: Holt, Rinehart & Winston, 1984).

[72] Patricia B. Newell, "A Systems Model of Privacy," *Journal of Environmental Psychology*, 14 (1994): 65-78.

- "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"[73].
- "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)"[74].

Some of these definitions are of special interest for PARIS project, such as "control of personal space and visual exposure". It is important to know how the loss of control over personal spaces affects to people, and how it feels to be observed.

A relevant psychosocial model of privacy was proposed by Irwin Altman[75]. In this model, privacy is defined as: "selective control of access to the self or to one's group". It addresses two key aspects of privacy: (i) *control of social interaction*; and (ii) *control of offered information*. Privacy is a boundary control process in which an individual regulates with whom contact will occur, and how much and what type of contact it will be, as well as how much and what type of information you want to share with others. Altman does not propose only a theory of private spaces but a broader theoretical perspective on social interaction, beyond the traditional concept of privacy as isolation or seclusion. He also proposes an adequate theory of privacy to analyse other social spatial behaviours such as crowding, territoriality and personal space. Altman's model highlights the dialectical process that is established among the person, its needs and its expectations. The definition of the SALT framework needs to consider the different processes of privacy because it is important to know the process control or regulation limits of people, together with the optimal level of access to the self and cultural, social, personal and environmental mechanisms. Gifford[76] reflects Altman's theoretical model, and defines it as a three dimensional process:

- **Process control or regulation limits**. People not only seek the exclusion of others, but also seek other people to engage in interaction.
- **Optimization process**. Privacy can be understood as a mechanism to achieve certain goals in social interaction. Altman believes that the ultimate goal of privacy is an optimal level of access to the self, choosing to be alone or in company when desired.
- **Multi-instrumental process**. The mechanisms for privacy are multiple and including: cultural, social, personal and environmental mechanisms.

2.2.2 Dimensions of Privacy

Alan Westin[77] suggested five types or dimensions of privacy: solitude, isolation, anonymity, reserve and intimacy. These dimensions can be classified in two groups:

- Control of interaction from the person. This group includes two dimensions:

[73] Sandra S. Petronio, *Boundaries of privacy: Dialectics of disclosure* (Albany, New York: SUNY Press, 2002).

[74] John Archea, "The places of architectural factors in behavioral theories of privacy," *Journal of Social Issues*, 33 (1977): 116-137.

[75] Irwin Altman, *The environment and social behavior: Privacy, personal space, territoriality and crowding* (Monterey (Ca.): Books/Cole, 1975).

[76] Robert Gifford, *Environmental Psychology: Principles and Practice,* 4th edition *(*Canada: Optimal Books, 2007).

[77] Alan Westin, *Privacy and Freedom* (New York: Atheneum, 1967).

- **Solitude**: refers to placing yourself in a situation where other people can't see or hear what you are doing.
- **Isolation**: involves using physical distance to separate oneself from others to obtain privacy.

- Selective control the information into interaction situations. This group contains three dimensions, of which the first two are the most relevant to the design of surveillance systems.
  - **Anonymity**: is seeking privacy by going unnoticed in a crowd of strangers.
  - **Reserve**: is controlling verbal disclosure of personal information to others (especially to strangers).
  - **Intimacy:** a form of privacy as a reference to the group. Pedersen[78] distinguishes:
    - **Intimacy with family**: refers to being alone with members of one's family to the exclusion of other people.
    - **Intimacy with friends**: is like intimacy with family except that the reference group is friends.

As with many other security concepts, we observe a difficulty for researchers in separating the concepts and objectives (e.g. avoiding that others know about your acts) from the ways or mechanisms used to achieve such goals (e.g. using physical distance to separate oneself from others). This distinction is a very necessary step, because it is the only way to capture and analyse the motivations behind the concepts.

Private space, semi-private space and public space

Each space can be characterized by the degree of privacy it offers. That is, each environment offers a different level of control to regulate the interaction. Zimring[79] proposed a theoretical distinction among **private spaces** that allows a high degree of privacy (are areas where accessibility is determined by one person or a small group of people, they are characterized by intimacy) **semi-private o semi-public spaces** (are accessible to members of the public, they are characterized by a certain intimacy which might be experienced therein) and **public spaces** (social spaces that are open and accessible to all). Visual exposure of people, their identification and their relationship with the different spaces in which they are, will condition the acceptance of different IT-empowered surveillance.

The public space can take many different forms, can be a gathering place defined by its social function, a civic space, a community space, a virtual space… The strength of the public space is its potential in reaching out and involving a wide and diverse group of people. From psychosocial theories of privacy, a public space is a space in which it is not possible to apply direct and effective control of our interaction with others, unlike a private space in which interaction regulation strategies are more varied and effective.

[78] Darhl M. Pedersen, "Psychological Functions of Privacy," *Journal of Environmental Psychology*, 17 (1997): 147-156.

[79] Craig Zimring, "The built environment as a source of psychological stress: Impacts of buildings and cities on satisfaction and behavior," in *Environmental Stress,* edited by Gary W. Evans (New York: Cambridge University Press, 1982).

In an empirical study, Krämer[80] extended this theoretical distinction, performing a classification of spaces depending on the degree of privacy:

- **Public spaces:** street, station, airport, university, beach, shopping mall, bank, hospital, sport club, supermarket, café, pub, market square, post office, swimming pool, hairdresser´s, sport ground, etc.
- **Semi-private spaces:** park, cinema, specialist's shop, museum, office, concert hall, library, theatre, school, art gallery, church, hall, meeting room, etc.
- **Private spaces:** one's home, friend's house, bathroom, private office, car, bedroom, etc.

It is important for the PARIS project to understand the extent to which people are willing to lose some of their privacy in different places in relation to their safety. The new configurations of the borders between public and private are shaped by the interactions among social and anthropological practices, legal norms, and technology creating four main streams. Therefore this concept of public space and privacy must be seen through this multidisciplinary perspective. The SALT framework is precisely the mechanism that PARIS will develop in order to provide comprehensive descriptions of such concepts as public space and privacy which are of major interest regarding the balance between privacy and surveillance infrastructure.

2.2.3 Psychological Effects of Lack of Privacy

Although, not much work is available dealing with the perception of privacy in the framework of IT systems, and more specifically, IT-empowered surveillance[81], we can find interesting studies that provide analyses about the psychological perception of privacy and the effects of the lack of privacy.

Traditionally, lack of privacy appeared to depend on the cognitive appraisal made by the person whose space has been invaded. Consequently, when there was an obvious legitimate reason for the invasion, no ill effects were reported[82]. This is a crucial finding for PARIS because it highlights the importance of informing the subjects of surveillance about the goals and limitations of the system, and indicates that providing adequate information is crucial in developing non-intrusive systems.

[80] Beatrice Krämer, "Classification of generic places: explorations with implications for evaluation," *Journal of Environmental Psychology*, 15 (1995): 3-22.

[81] Actually, there is an important study made by the "PRISMS Project", in its Deliverable D7.1 "Report on existing surveys", where they identify and analyse existing public opinion surveys regards to privacy and security/surveillance. They compiled an inventory of about 260 surveys, from 1985 to early 2012. Nevertheless, this study reports that, among those 260 surveys, very few are of good quality regarding methodological considerations. Available at http://prismsproject.eu/wp-content/uploads/2013/03/PRISMS-D7-1-Report-on-existing-surveys.pdf

[82] Stephen Worchel & Steven M. Yohai, "The role of attribution in the experience of crowding," *Journal of Experimental Social Psychology*, 15 (1979): 91–104.

The discomfort of an invasion of privacy initiates a variety of conscious and unconscious behaviours that attempt to regulate personal boundaries[83]. These may take the form of movement away from the invasive individual or group to increase interpersonal distance, reorientation of the face or body to reduce visual contact, or complete retreat to another environment, all of which represent types of avoidance behaviours[84]. For PARIS, this indicates that the psychological effects of a surveillance system that represents a privacy breach must be taken into account in order to design systems that are non-intrusive and that perform their function without affecting the observed subjects.

Baum & Greenberg[85] have shown that the potential for spatial invasion can influence the choice of seating, with those anticipating the invasion choosing seats in a corner or along a wall, making use of the physical environment to help regulate privacy. Other findings suggest that individuals will avoid invading the personal space of others[86] or will engage in submissive gestures or verbalized apologies to minimize the impact of invasion[87]. This is relevant for PARIS, since it shows that people will protect their privacy, while reacting against systems that do not respect their privacy. Even if, as we have already pointed out, in some cases the will to lose parts of privacy in favour of the surveillance system is conditioned by the legitimacy and importance of the surveillance goals, in some other cases, a badly designed surveillance system may result in reactions that may defeat the original goal of the surveillance system. As an example, consider a very intrusive surveillance system in a supermarket, designed with the goal of increasing the revenues by avoiding shoplifting. If the perception of the privacy invasion is such that customers decide to shop somewhere else, the system will not achieve the goal of increasing the revenues, even if it totally prevents shoplifting.

Privacy regulation may also involve the use of physical barriers to reduce the amount of stimulation as well as reduce the uncertainty associated with exposure, giving the individual a sense of control over an environment[88]. Again, we can obtain interesting conclusions for PARIS from this study: The provision of user-control mechanisms can increase the users' perception of the system legitimacy and efficiency.

The effects of lack of privacy may be permanent, we must be careful. "The social media and online data collection are conditioning our privacy and a lot of it is our own fault. Six in 10 think people should stop sharing so much of their personal thoughts and experiences online; they

[83] Irwin Altman, "Privacy regulation: culturally universal or culturally specific," *Journal of Social Issues*, 38 (1977): 66-84.

[84] Matthew L. Fried & Victor J. DeFazio, "Territoriality and boundary conflicts in the subway," *Psychiatry*, 37 (1974): 47–59.

[85] Andrew Baum & Carl I. Greenberg, "Waiting for a crowd: The behavioral and perceptual effects of anticipating crowding," *Journal of Personality and Social Psychology*, 32 (1975): 671–679.

[86] John C. Barefoot, Howard Hoople, & David McClay, "Avoidance of an act which would violate personal space," *Psychonomic Science*, 28 (1972): 205-206.

[87] Michael G. Efran & J. Allan Cheyne, "Affective concomitants of the invasion of shared space: Behavioral, physiological, and verbal indicators," *Journal of Personality and Social Psychology*, 29 (1974): 219- 226.

[88] Virginia W. Kupritz, "Privacy management at work: A conceptual model," *Journal of Architectural and Planning Research*, 17 (2000): 47–63.

believe society needs to re-establish its privacy boundaries. Concern is most pronounced for the millennial generation: 7 in 10 believe today's youth have no sense of personal privacy"[89].

2.2.4 Functions of Privacy

The terms privacy needs and privacy functions have been used synonymously. Westin[90] described four functions of privacy:

- **Personal autonomy:** refers to the desire to avoid being manipulated, dominated, or exposed by others.
- **Emotional release:** release refers to release from the tensions of social life such as role demands, emotional states, minor deviances, and the management of losses and of bodily functions.
- **Self-evaluation:** refers to integrating experience into meaningful patterns and exerting individuality on events.
- **Limited and protected communication**: limited communication sets interpersonal boundaries and protected communication provides for sharing personal information with trusted others.

Altman[91] organized privacy functions ranging from the interpersonal aspect to the self, being the relationship between the self and other people the middle point: i**nterpersonal functions, the relationship between self and others, self-identity.** Newell[92] proposed that privacy provides for the maintenance and development of the individual as a system.

Pedersen[93] identified five privacy functions: **autonomy, confiding, rejuvenation, contemplation, and creativity.** He examined the relationships between their types and functions.

This is interesting for PARIS to identify the relation between the types of privacy and the privacy functions model, and thus obtaining more accurate information to develop SALT frameworks. The model secures the link between the types of privacy people need and the way they are used. He suggested that autonomy, a function, is reasonably supported by all six types but is supported best by intimacy with family and intimacy with friends. This model represents a significant extension of Westin's[94] theory of privacy.

2.3 Privacy from a Socio-Political Perspective

Nathalie Trussart (CRIDS – University of Namur)

[89] Havas Worldwide, *This Digital Life*. *Prosumer Report,* vol. 13 (2012): 10-21.

[90] Alan Westin, *Privacy and Freedom* (New York: Atheneum, 1967).

[91] Irwin Altman, *The environment and social behavior: Privacy, personal space, territoriality and crowding* (Monterey (Ca.): Books/Cole, 1975).

[92] Patricia B. Newell, "A Systems Model of Privacy," *Journal of Environmental Psychology*, 14 (1994): 65-78.

[93] Darhl M. Pedersen, "Model for types of privacy by privacy functions," *Journal of Environmental Psychology,* 19 (1999): 397-405.

[94] Alan Westin, *Privacy and Freedom* (New York: Atheneum, 1967).

The claim of privacy as a social value is the keystone of the socio-political perspective on privacy. Indeed, different scholars, from political sciences and social sciences, have advocated the recognition of the social and political values of privacy, while addressing a challenge both to the conception of privacy as an individual right and/or value and to the one of its consequential turn of mind, that is the balancing relationships between privacy – conceived as an individual interest and/or value and/or right – and other social values such as (national) security. As Colin Bennet and Charles Raab put it: "The conception of privacy as an individual right could be challenged by an emergent recognition of privacy as a social value".[95] Accepting to reduce privacy to "only" an individual right and/or value and/or interest, especially in our current context overloaded of discourses in favour of security and safety[96], and to balance privacy against other social values such as (national) security, is a very risky posture. Indeed, privacy, while being conceived only as an individual interest and/or right and/or value and not as a social value, is at risk of becoming the loser in the balance against social values.

2.3.1 General Overview

Priscilla M. Regan was one of the first who identifies why the protection of privacy is important to society. In her book, *Legislating Privacy*: *Technology, social values and public policies*, published in 1995, her arguments are clear.

> "Privacy has a value beyond its usefulness in helping the individual maintain his or her dignity or develop personal relationships. Most privacy scholars emphasize that the individual is better off it privacy exists. I argue that **society is better off as well when privacy exists**. I maintain that privacy serves not just individual interest but also **common, public and collective purposes**. If privacy becomes less important to one individual in one particular context, it serves, to several individuals in several context, it would still be important as a value because it serves other crucial functions beyond those that it performs for a particular individual." [97]

She unfolds the social importance of privacy in three dimensions: (1) a **common** value; (2) a **public** value; (3) a **collective** good.

> The **common** value of privacy. "Some rights, which protect individual interests, are regarded as so fundamental that all individuals in common have a similar interest in them...in much the same way that people of different religious beliefs have a common interest in a right to free conscience, people of different privacy beliefs or preferences have a common interest in a right to privacy".

[95] Colin Bennett and Charles Raab, *The governance of privacy. Policy instruments in Global Perspective* (Cambrige (MA): MIT Press, 2006), 49.

[96] For more details about the historical development of this link between privacy, surveillance, (national) security, war and terror and its reinforcement after 9/11, see: Darren W. Davis and Brian D. Silver, "Civil Liberties vs. Security: Public Opinion in the Context of the Terrorist Attacks on America", *American Journal of Political Science*, 48 (1) (2004): 28-46. See also an overview of the effects beyond America: D. Bigo and A. Tsoukala (ed.), *Terror, Insecurity and Liberty: Illiberal Practices of Liberal Regimes after 9/11* (London: Routledge, 2008). And also: L. Amoore and M. De Goede (ed.), *Risk and the War on Terror* (London: Routledge, 2008).

[97] Priscilla M. Regan, *Legislating Privacy: Technology, Social Values, and Public Policy* (Chapel Hill: University of North Carolina Press, 1995), 221. I highlight.

> The **public** value of privacy. "A public value of privacy, then, is derived from its importance to the exercise of rights that are regarded as essential to democracy, such as freedom of speech and association, and from its importance as a restraint on the arbitrary power of government".
>
> Privacy as **a collective good**. "No one member of society can enjoy the benefit of a collective goof without others also benefiting". It is the case for clean air, for national security and for privacy.[98]

In the same line of though, **Arthur Cockfield** contends that both, privacy as an individual right and as a social value have to be preserved.

> "Judges, lawyers and policy-makers need to take into account more explicit account of the individual rights aspect of privacy as well as the social value or privacy, that is, **society's interest in preserving privacy apart from a particular individual's interest**. Both of these aspects of privacy are critical to the functioning of our democratic state (...) Even if privacy becomes less important to certain individuals..., it continues to serve other critical interests in a free and democratic state (e.g. the need to protect political dissent) beyond those that it performs for a particular person".[99]

Cockfield also contends about the risky balance between privacy and social values such as (national) security and takes this risk as a reason of major importance for advocates in favour of privacy as a social value.

> "The traditional understanding of privacy often focuses on the individual rights aspect of privacy by emphasizing privacy as an individual's claim against state interference. This understanding generally leads to legal analysis that sees privacy as an interest which competes with security, sometimes resulting in calls for the need to dilute privacy to protect the public against criminal and/or terrorist activities".[100]

Alan Westin, in his seminal work published in 1967, supports also the defence of privacy as a social good which is necessary in democratic societies.

> "The importance of that right to choose, both to the individual's self-development and to the exercise of responsible citizenship, makes the claim for privacy a fundamental part of civil liberty in democratic society. If we are switched on without our knowledge or consent, we have, in very concrete terms, lost our rights to decide when and with whom we speak, publish, worship, and associate. Privacy is therefore **a social good in democratic societies**, requiring continuous support from the enlightened public."[101]

Stephen Margulis, on his side, offers a short classification of the social dimensions of privacy.

[98] Ibid., 220-31.

[99] Arthur J. Cockfield, "Protecting the Social Value of Privacy in the Context of Dtate INverstigations Using New Technologies", *U.B.C. Law Review*, 40 (1) (2007): 41. I highlight.

[100] Ibid., 42.

[101] Alan Westin, "Social and Political dimensions of Privacy", *Journal of Social Issues*, 59(2) (2003): 431-53. I highlight.

> "Privacy is social in two senses: the socio-psychological and the social-political. This duality is a bridge between socio-psychological privacy as social behaviour and socio-political privacy as a social issue."[102]

Regards to the socio-political dimensions of privacy, Margulis takes up the classification of Regan, that is: privacy as (1) a common value, (2) a public value and (3) a collective good. Regards to the socio-psychological dimensions of privacy, he identified three dimensions:

> "(a) Privacy's foci are **interpersonal communication and social interaction**. This view of 'social' predominates... There are two less frequent referents. (b) **How we experience, understand, react to, and enact privacy** are products of our social and cultural development ... (c) Privacy is an **attribute** not only of individuals but also **of groups** and, for some theorists, **organizations**."[103]

Daniel Solove shares with Cockfield the necessity to challenge the balance paradigm between privacy and other social values.

> "Privacy is often cast as an individual right and balanced against the greater social good, which results in privacy being frequently undervalued in relation to many conflicting interests." [104]

That is the main reason for him to advocate in favour of privacy as a social value.

> "When privacy protects the individual, it does so because it is in society's interest (...) The value of privacy should be understood in terms of its contribution to society".[105]

For **Julie Cohen**, as for the aforementioned scholars, privacy is a fundamental value for both individual and society, **a value which underlies other values such as autonomy and anonymity**.

> "A degree of freedom from scrutiny and categorization by others promotes important non instrumental values, and serves vital individual and collective ends (...) Informational autonomy comports with important values concerning the fair and just treatment of individuals within society (...) A realm of autonomous, unmonitored choice, in turn, promotes a vital diversity of speech and behaviour. The recognition that anonymity shelters constitutionally-protected decisions about association – decisions that otherwise might be chilled by unpopularity or simple difference – is part of our constitutional tradition (...) The autonomy fostered by informational privacy also generates more concrete collective benefits. Development of the capacity for autonomous choice is an indispensable condition for reasoned participation in the governance of the community and its constituent institutions – political economic and social (...) Examination chills experimentation with the unorthodox, the unpopular, and the merely unfinished. A robust and varied debate on matters of public concern requires the opportunity to experiment with self-definition in private, and (if one desires) to keep distinct social, commercial, and political associations separate from on another". [106]

[102] Stephen T. Margulis, "Privacy as a Social Issue and Behavioral Concept", *Journal of Social Issues*, 59 (2) (2003): 243-61.

[103] Ibid. I highlight.

[104] Daniel J. Solove, *Understanding Privacy* (Cambridge (MA): Harvard University Press, 2008), 78-79.

[105] Ibid., 173.

[106] Julie E. Cohen, "Examined Lives: Informational Privacy and tge Subject as Object", *Standford Law Review*, 52 (5) (2000): 1423-6.

Valerie Steeves makes the observation that, in Alan Westin's seminal work, privacy is defined, of course, as a social value, but also as informational control and that there is something wrong with this definition of privacy as informational control. More than forty years after the publication of Alan Westin's book, *Privacy and Freedom*, both the theoretical work and the legislative activity, which were boosted by his claim in favour of privacy as a social value, have done little to constrain the collection of massive amounts of personal information on the part of government and of corporations. Steeves argues that the reason is that advocating privacy as a social value is not enough, this avocation must by accompany with reliable conceptualisations of privacy which goes beyond the sole "information control" definition.

> "Sociologists have been particularly critical of Westin's conceptualization of privacy, arguing that as 'appealing and seemingly intuitive as this concept is, it plainly doesn't work".[107]

Among the criticisms addressed by sociologists to Westin's concept of privacy as "information control", Steeves quoted these ones:

- "data protection has been unable to stop the rollout of technologies like closed-circuit television cameras in public places, remote-activated location devices in cell phones, iris scans in school cafeteria lunch lines, and security cameras in bathrooms, hotel rooms, and school buses,
- In spite of concerns that the surveillance these technologies enable may have deleterious effects on our social and political relationships.
- The conceptualization of privacy as informational control has also arguably displaced broader – and potentially more empowering – discourses rooted in a human rights model that seeks to protect human dignity and democratic freedoms in the surveillance society."[108]

Steeves' concern is about a reconceptualization of privacy in which there is a place for normal social interactions through which people negotiate their privacy and the borders between their different privacy's spheres and what does not concern those spheres.

> "The gap between the goal of data protection legislation and the reality of life in surveillance society is not just a matter of poor implementation. I suggest it reflects the fact that **we rely upon a definition of privacy that is problematic** because it strips privacy out of its social context (...) goes back to the source and revisit Westin's theory of privacy with a view to recapturing the social elements of the privacy equation. I argue that, although Westin's theory is rich in sociality, he limits his insights into the social nature of privacy by focussing on the flow of information rather than on **the social interaction of persons seeking or respecting privacy**. In addition, **Westin equate perfect privacy with social withdrawal**; from this perspective, any social interaction becomes a risk to privacy, making privacy not only asocial, but also antisocial." [109]

Steeves goes on, in her very interesting paper, and proposes an alternative framework that conceptualizes privacy as a dynamic process of negotiating personal boundaries in intersubjective relations.

[107] Valerie Steeves, "Reclaiming the Social Values of Privacy," in *Lessons from Identity Trail*, ed. I. Keer (Oxford: Oxford University Press, 2008), 191.

[108] Ibid., 192.

[109] Ibid., 192-93. I highlight.

> "In doing so, I am not arguing in favour of a collective right versus an individual right. Rather, I am suggesting that by placing privacy in **the social context of intersubjectivity**, privacy can be more fully understood as a social construction that we create as we negotiate our relationships with others on a daily basis. This conceptualization frees the policy questions from the narrow procedural considerations of data protection, and reinvigorates our ability to question – and limit – the negative impact of surveillance on our social and democratic relationships".[110]

As those different authors show us, and in a very explicit manner in the case of Steeves, the general claim in favour of privacy as a social value must be sustained by a conceptualization of privacy. Regards to the kind of conceptualization proposed, the effects are very different. In fact, the way privacy is conceptualised allows identifying very different kind of harms or concerns.

This is worth emphasizing for the construction of the SALT framework which may be very different regards to the kind of taxonomy or conceptualization of privacy retained for its construction. Indeed, as a short term research aim, the reading of different existent taxonomies of privacy reveals that, while planning the construction of the taxonomy which will be relevant for the SALT Framework, it is necessary to be transparent in the methodological design of the taxonomy and reasons for choosing certain criteria rather than others.

For this reason, the next subsection identifies different taxonomies of privacy which are of interest for the construction of the SALT Framework. In the next deliverable (D 2.2), a detailed analysis of their content still must be done regards to different details such as, for example,

- the types of categories retains in the taxonomies. For example, a taxonomy which takes into account as a relevant criteria the intellectual property rights regime over information is very different than one which takes into account the social context of intersubjectivity;
- their purpose. Indeed, the purpose of the taxonomy is not trivial. Helping Law enforcement or helping the design of a system-to-be which integrates Privacy-By-Design principles are two very different purposes. Regards to the kind of purpose, some common criteria to the analyzed taxonomy may be relevant (or not) for the SALT Framework;
- the sources used. For example, legal sources or theoretical rationales built on the study and analyze of new and emerging technologies provide very different perspective on privacy;
- the consequences and the types of consequence of the breaking of the criteria used in those different taxonomies. For example, the consequence may be law pursuit or a psychological effect on individuals.
- criticisms that have been addresses to those different taxonomies.

2.3.2 Privacy Frameworks Regards to Socio-Political Issues

[110] Ibid., 193. I highlight.

This subsection identifies existent taxonomies of privacy which are of interest for the SALT Framework and which may be studied in more details during the next step of this project and more specifically regards the two specific surveillance technologies that are at the core of the PARIS project: CCTV and biometric surveillance technologies.

The following privacy frameworks were chosen among many others possible ones because of the different focus they put on privacy.

2.3.2.1 Finn, Wright and Friedewald: Seven Types of Privacy

In their paper, *Seven Types of privacy*[111], those authors propose to extend the definition of privacy – using in a way this notion as a springboard or a lever – to any "specific elements of privacy which are important and must be protected", attempting "to capture the complexity of privacy issues within frameworks that highlight the legal, socio-psychological, economics or political concerns"[112] that surveillance technologies present. They define their approach as **pro-active and protective** regards to privacy, "over-arching protection that should be instituted to prevent harms"[113], offering "a forward-looking privacy framework that positively outlines the parameters of privacy in order to prevent intrusions infringements and problems."[114]

They identify their **taxonomy of types privacy** by contrast with **taxonomy of privacy harms** which they identify as being the result of a reactive posture regards to privacy, a "reactive highlighting of concerns or intrusions"[115]. According to these authors, most privacy "scholars' focus on the ways in which privacy can be infringed and the legal problem which must be solved is largely reactive. They focus on specific harms which are already occurring and which must be stopped."[116] Indeed, starting from the many dimensions of privacy, many scholars have tried to generate taxonomies of privacy problems, harms or intrusions. Among those scholars, Finn, Wright and Friedewald identified Daniel Solove's taxonomy of privacy problems[117] and Debbie Kaspar's typology of privacy intrusions[118] as the figures of reactive posture regards to privacy.

They illustrate this difference between a **taxonomy of privacy harms** and a **taxonomy of types of privacy** with an analogy with "the difference between outlawing murder and adopting a right to life (...) a positive right to life forces individuals, governments and other organisations to evaluate how their activities may impact upon a right to life and introduce protective measures." [119]

[111] Rachel L. Finn, David Wright and Michael Friedewald, "Seven Types of Privacy," in *European Data Protection: Coming of Age*, ed. Serge Gutwirth (Dordrecht: Springer, 2013), 3-32.

[112] Ibid., 3.

[113] Ibid., 6.

[114] Ibid., 3.

[115] Ibid., 3.

[116] Ibid., 6.

[117] Daniel Solove, *Understanding Privacy* (Cambridge (MA): Harvard University Press, 2008).

[118] Debbie V.S. Kaspar, "The Evolution (or Devolution) of Privacy", *Sociological Forum*, 20 (1) (2005): 69-92.

[119] Ibid., 6.

It's worth noticing that the seven types of privacy retained in this taxonomy expand a former categorization of four types of privacy identified in 1997 by Roger Clarke[120]. The main argument formulated by Finn, Wright and Friedewald in favour of the partial reworking and the expansion of this previous categorization is that the coming of new and emerging technologies and applications has meant to have new impacts of privacy in such a way "that previously unconsidered types of privacy now need to be addressed in order to adequately protect individuals' rights, freedoms and access to goods and services".[121]

Clarke identified those four types of privacy:

1. Privacy of the person
2. Privacy of personal behaviour
3. Privacy of personal communication
4. Privacy of personal data

Finn, Wright and Friedewald, while reworking Clarke's first classification, defined those seven types of privacy:

1. Privacy of the person
2. Privacy of personal behaviour and action
3. Privacy of personal communication
4. Privacy of personal data and image
5. Privacy of thoughts and feelings
6. Privacy of location and space
7. Privacy of association

2.3.2.2 Steeves: Privacy in Intersubjective and Social Interactions

As exposed above, Steeves offers an alternative framework that conceptualizes privacy as a dynamic process of negotiating personal boundaries in intersubjective relations. Her framework is particularly interesting for the construction of the SALT Framework for two main reasons. (1) First she gives an important focus on surveillance in public space. (2) Secondly, her main concern is to keep vivid the intersubjective negotiation between people regards to their personal privacy's boundaries.

Steeves' privacy framework is based on a critic of Westin's privacy concept conceived as informational control. About it, she argues that:

> "Once the focus shifts to the flow of information, privacy is no longer grounded in the social interaction of subjects, but becomes located in the individual's unilateral control over keeping information on the internal side of the boundary (...) From this perspective, privacy is no longer asocial – it is antisocial. Because disclosure is dependent on the trustworthiness of intimate others and the sensitivity of the

[120] Roger Clarke, "Introduction to Dataveillance and Information Privacy, and Definitions of Terms", *Xamas Consultancy*, 1997: Available at: http://www.rogerclarke.com/DV/Intro.html.

[121] Rachel L. Finn, David Wright and Michael Friedewald, "Seven Types of Privacy," in *European Data Protection: Coming of Age*, ed. Serge Gutwirth (Dordrecht: Springer, 2013), 28.

generalIpublic to respect the individual's reserve, any social interaction poses a risk to privacy, and privacy can only be fully protected by a withdrawal from others."[122]

The table below shows the way she represents Westin's privacy concept.

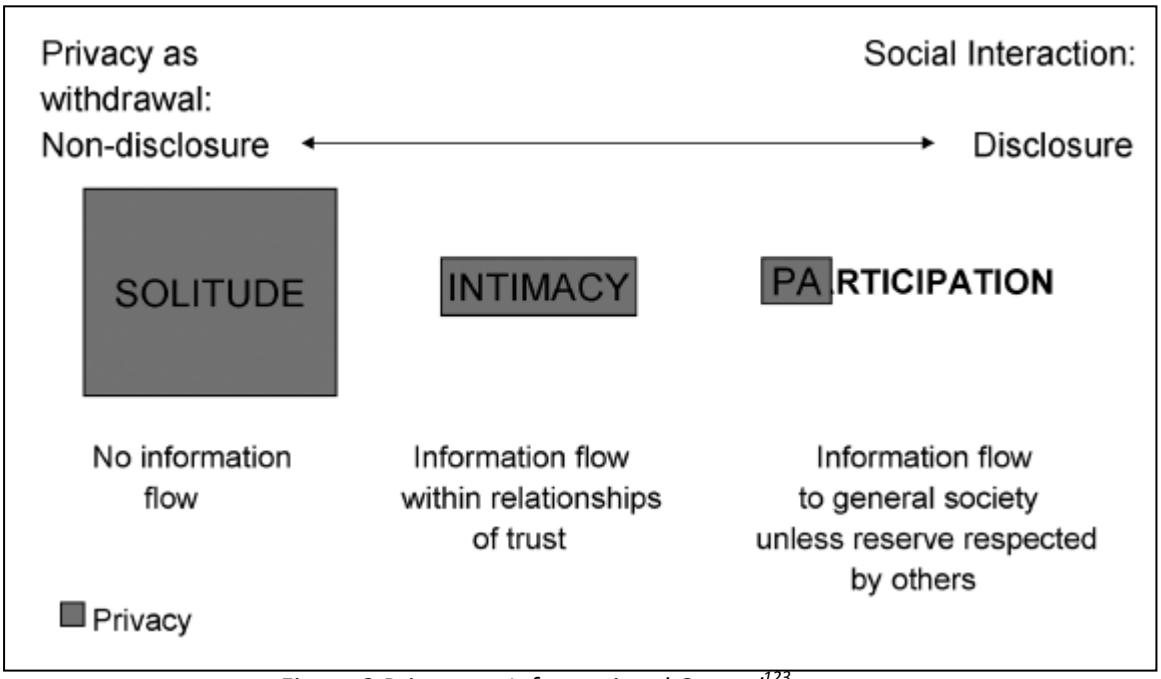

Figure 2 Privacy as Informational Control[123]

And as a corrective to Westin's theory of privacy - based on a definition of privacy as informational control - she draws on Irvin's Altman's work on territoriality and Georges Mead's work on social interactionism. As the table below shows it, the alternative privacy's framework she proposes is based on the boundaries people negotiate throughout a range of social interactions, in situations of low to high contact with others.

[122] Valerie Steeves, "Reclaiming the Social Values of Privacy," in *Lessons from Identity Trail*, ed. I. Keer (Oxford: Oxford University Press, 2008), 201.

[123] This table is taken from : Ibid., 201.

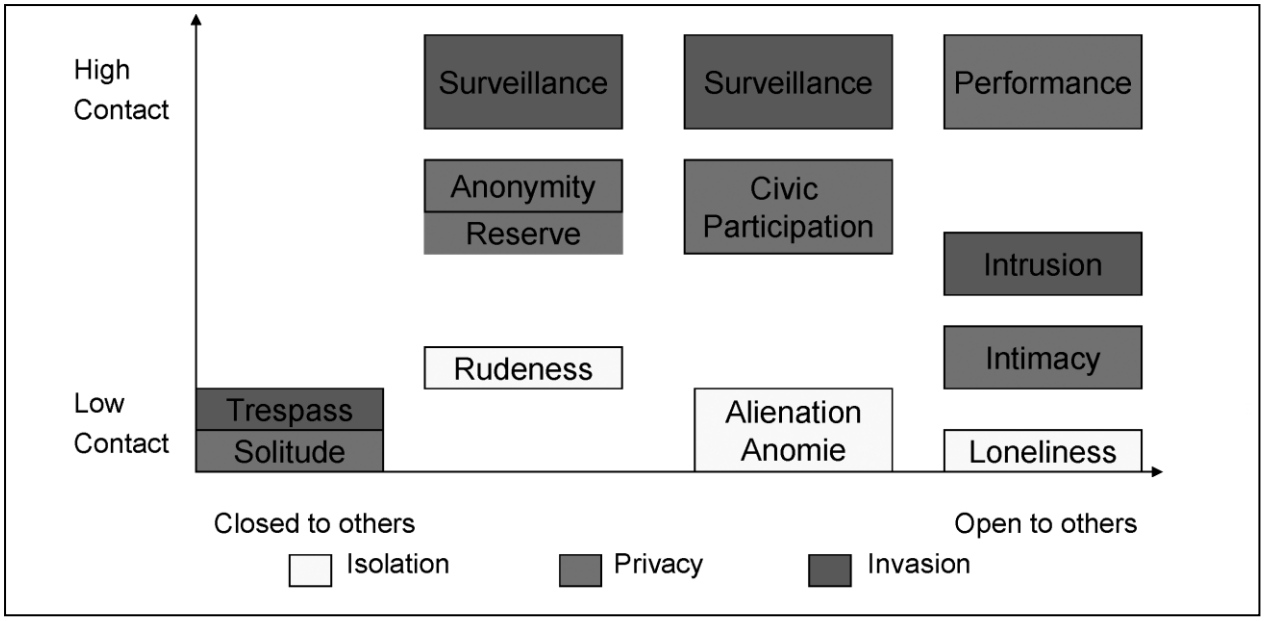

Figure 3 Privacy as Boundary[124]

2.3.2.3 Solove: A taxonomy of Privacy Problems

Daniel Solove created a taxonomy of privacy problems that is devoted to provide a useful tool for further development of legislative protection of privacy. Indeed, as he wrote it, his "taxonomy aims to carve up the landscape in a way that the law can begin to comprehend and engage."[125] He explained clearly, extensively and in different documents, the method he used and dedicated a full chapter to his taxonomy of privacy in his famous book "Understanding Privacy".

Privacy is best understood as a « family of different yet related things."[126] Solove arrives at this conclusion by outlining a taxonomy of privacy problems that must be addressed, regardless of whether they conform to a precise definition of privacy. The criteria retained for the choice of privacy problems that are accounted is that they have achieved a significant degree of social recognition. Even if those problems are "identified through a bottom-up cultural analysis, he said, using historical, philosophical, political, sociological, and legal sources", his primary focus is on "the law because it provides concrete evidence of what problems societies have recognized as warranting attention."[127]

His taxonomy is an extension of the four categories of privacy torts that were articulated by William Prosser in 1960[128] :

> "1. Intrusion upon the plaintiff's seclusion or solitude, or into his private affairs.
> 2. Public disclosure of embarrassing private facts about the plaintiff.
> 3. Publicity that places the plaintiff in a false light in the public eye.
> 4. Appropriation, for the defendant's advantage, of the plaintiff's name or likeness."[129]

[124] This table is taken from Ibid., 208.

[125] Daniel J. Solove, *Understanding Privacy* (Cambridge (MA): Harvard University Press, 2008), 102.

[126] Ibid, 9.

[127] Ibid., 102.

[128] William L. Prosser, "Privacy", *California Law Review*, 48 (1960): 383.

Solove discerned the need to expand upon these four categories of privacy torts for different reasons. First, the epoch has changed and new technologies are likely to produce new kind of harms. Second, Prosser focused only on tort law and it is not enough according to Solove. "A new taxonomy to address privacy violations for contemporary times is sorely needed."[130] This new taxonomy "focus on activities that can or do create privacy problems. A privacy violation occurs when a certain activity causes problems that affect a private matter or activity."[131] Those activities which structure his taxonomy in four main categories, each including sub-categories, are:

- *information collection*, such as surveillance or interrogation,
- problems associated with *information processing*, including aggregation, data insecurity, potential identification, secondary use and exclusion,
- *information dissemination*, including exposure, disclosure breach of confidentiality, etc.
- *Invasion*, such as issues related to intrusion and decisional interference.[132]

2.3.2.4 Nissenbaum: Contexts of Privacy

In his book, "Privacy in context"[133] , Helen Nissenbaum invites the reader to consider privacy in the specific context where it is an issue: a hospital is a very different context than an airport. In different context, privacy responds to different kind of norms. What is appropriate, regards to privacy, in a context, can be a violation of privacy in another context.[134]

It is worth noting that the privacy framework proposed by Nissenbaum has been used by requirement engineers who have developed a requirement method which formalises access control models.[135]

2.3.2.5 Extended Version of Privacy Impact Assessment

Several scholars have worked upon an extended version of privacy impact assessment (PIA). Indeed, different forms of privacy impact assessment are proposed – existing guidelines, analyses and recommendations for legal enforcement purpose – and form a continuum which is bordered by two extremities we may be called, for ease purpose, a limit version of PIA and an extended version of PIA. As a caricature we may say that the limited version of PIA is limited by the legal requirement regards to privacy and may adopt the minimal form of an administrative

[129] Daniel J. Solove, *Understanding Privacy* (Cambridge (MA): Harvard University Press, 2008), 101.

[130] Ibid., 101.

[131] Ibid., 102.

[132] Daniel J. Solove, "'I've got nothing to hide' and other misunderstanding of privacy'", *Sans Diego Law Review*, 44 (2007): 758.

[133] See: Helen Nissenbaum, *Privacy in Context. Technology, Policy and the Integrity of Socail Life* (Standford: Standford University Press, 2010).

[134] In 1985, J.H. Moor already argued in favour of the need to consider ethics in context. See: Moor, J. H. What is computer ethics? In T.B. Bynum (ed.) Computer & Ethics (Oxford: Blackwell, 1985), 266-275.

[135] Adam Barth et al., "Privacy and Contextual Integrity: Framework and Applications", *SP '06: Proceedings of the 2006 IEEE Symposium on Security and Privacy*, May, 2006: 184-98.

questionnaire which looks like a check-list of different question (YES/NO choice or Multiple choice form). On the other extremity, there is the extended version which includes legal requirements, socio-political and ethical requirements. This extended version is defined as a process. A complete analysis of the current existent forms of PIAs has been provided by the PIAF project.[136] Another analysis has been made by Roger Clarke.[137] Charles Raab and David Wright have also provided very interesting proposals regards to extended version of PIA, and more specifically about a version of PIA which might assess the impact of surveillance on broader range of individual and societal values (such as autonomy and dignity) as well as on other rights and freedoms that are not generally taken into account in minimal version of PIA.[138] A very well documented and argued overview is also extensively presented in the book edited in 2012 by Paul De Hert and David Wright: *Privacy Impact Assessment*.[139]

We suggest taking these studies about extended version of PIA into consideration in the next step of the project, while the different features retained by different versions of PIA might be of interest for the design of the SALT Framework. Different reasons exist.

A first reason regards the arguments express in favour or in disfavour of specific features. They provide a good methodological transparency.

A second reason is about the “extension” of the concept of privacy taken into account and which goes beyond the sole legal compliance.

A third reason that can be put forward is that in order to make those proposals of Privacy Impact Assessments, a same kind of preliminary work that the one we have to process for the design of the SALT Framework had to be done, that is identifying the privacy features to be taken into account for such an assessment. Of course, several dimensions retains for an extended version of PIA are at first sight not relevant for the SALT Framework, as for example, the institutional environment and the stakeholders specific to this environment.

A last reason lies in the process through which those two privacy tools – a SALT system and a PIA -, which are different regards their tasks, objectives and actors, operate. Indeed, they appear at different stages of the process and the Salt Framework occurs far before any PIA. Nevertheless, as an anticipatory posture, the SALT Framework may already be “PIA compliant”. In that sense, taking into account extended version of PIA is of interest for the SALT Framework regard to the anticipatory perspective they offer on what may be guaranteed in privacy matter.

[136] Paul De Hert, Dariusz Kloza and David Wright, "Deliverable D3: Recommandations of a privacy impact assessment framework for the European Union," in *PIAF: Privacy Impact Assessment Framework* (Brussels-London: European Commission - Directorate Generale Justice, 2012).

[137] Roger Clarke, "An evaluation of privacy impact assessment guidance documents", *International Data Privacy Law*, Vol.1 N°2 2011, 111-120. Available at: http://rogerclarke.com/DV/PIAG-Eva.html.

[138] Charles Raab and David Wright, "Surveillance: Extending the Limits of Privacy Impact Assessment," in *Privacy Impact Assessment*, ed. David Wright and Paul De Hert (Dordrecht Heidelberg London New York: Springer, 2012), 363-83.

[139] David Wright and Paul De Hert (eds.), *Privacy impact assessment* (New York: Springer, 2012).

2.4 Privacy from an Ethical Perspective

NathalieTrussart (CRIDS – University of Namur)

Generally speaking, ethics can be defined as "a philosophical inquiry in concepts involved in practical reasoning, i.e. concepts related to the ways in which human beings choose among possible different courses of actions, according related criteria such as good/bad or right/wrong."[140] As a discipline, ethics contains three main streams:

(1) *Meta-ethics* investigates "where our moral principles come from."
(2) *Normative ethics* tries "to come up with moral standards for right and wrong behaviour."
(3) *Applied ethics* focus "on specific moral issues within a given context and practical case".[141]

"Provided that there are events which are actions (i.e. events that are controlled, at least in part, by an agent, who contributes to cause them according to some intentions), ethics investigates"[142], related to the three main streams identified above:

(1) "the notions involved in actions, say, ethical principles such as good and evil, right and duty, virtues, obligations, free will, etc., their foundation and their rationale;
(2) Claims made in these terms, their soundness and consistency;
(3) And practical problems which involve the ethical principles and the assessment, of their rationale behind each option of action".[143]

Different ethical theories exist in order to identify and to respond to ethical issues arising from scientific and technological innovation, while the first of them has been developed as bioethics in the field of medicine and medical research.[144] These different ethical theories can be set along a continuum bounded by two limits that are presented later in this section:

(1) *An essentialist conception of ethics* which assesses innovations with a normative frame based on universal and prescriptive principles.
(2) *A pragmatist conception of ethics* which defines ethics as a "savoir-faire", a capacity to make moral choice when faces with situations raising unprecedented ethical dilemmas or challenges.

A wide range of values may all legitimately contribute to an ethical decision and determining ethical issues regards to surveillance technologies is a value-laden operation that critically depends on the ethical perspective chosen by those who will carry it out.

It is not our mandate to make a complete review on the many approaches of ethics. Nevertheless, regards to the aim of this text of indentifying relevant criteria for the design of an

[140] Silvia Venier and Emilio Mordini, "Deliverable 4. FInal Report - A Privacy and Ethical Impact Assessment Framework for Emerging Sciences and Technologies," in *PRESCIENTproject. Privacy and emerging fields of scienbce and technoolgy: Towards a common framework for privacy and ethical assessmenttechnologies: Five case studies* (EC: Seventh Framework Programme (FP7), 2012), 61.

[141] Ibid..

[142] Ibid.

[143] Ibid.

[144] For more detailed analysis of biomedical ethics, see: T. L. Beauchamp and J.F. Childress, *Principles of biomedical ethics (6th ed.)* (New York: Oxford University Press, 2008).

ethical-based approach within the SALT framework, the focus is placed on (1) several ethical approaches that may be of interest for extracting ethical issues relating to surveillance technologies and (2) on several existent ethical frameworks. Different key sources are identified along this section and listed at this end with the recommendation to analyze them in details during the next step of this research. The next deliverable (D 2.2) will build on the findings of this Chapter to provide a definitive list of requirements, adapted to the context of surveillance.

2.4.1 General Overview

In this subsection, different ethical aspects are stated. First, a general remark about ethics and surveillance technologies. Second, the presence of ethics in the official texts at the European Union (EU) level. And third, a general overview of two main approaches and tools for identifying ethical issues regards to technology.

2.4.1.1 Surveillance Technologies: a Challenge for Ethics

If generally speaking, what is an "ethical issue" is in itself an issue, the question remains largely open regards to surveillance technologies. This is true for different reasons.

A first reason is related to surveillance technologies itself. The argument is also true for ICT's technology at large. Indeed, "**the development of new ICTs and other security technologies are generally complicating the definition of the role of ethics**, as well as the identification of its theoretical approaches and operational instruments needed to address ICTs-related issues."[145] One explanation is that intentional actions are at the heart of traditional ethics of science and technology which thinks from the duo of the lonely scientific Frankenstein who intentionally creates his creature. However, scientific and technological developments "have the potential to bring **unintentional or highly unpredictable consequences that are usually the result of collective decisions**".[146] According to René von Schomberg, we do not have ethical theory at our disposal which would be an *Ethics of Knowledge Policy and Knowledge Assessment*[147] that is an ethics which addresses "both the aspect of **unintentional side consequences** (rather than intentional actions) and the **aspect of collective decisions** (rather than individual decisions)."[148]

A second reason is that it is not sure that a specific field of research such as *surveillance ethics* exist. If **Gary T. Marx** was one of the first scholars who identified ethical issues and coined ethical tools in order to help in identifying them regards to surveillance technologies[149], most of

[145] Ibid., 61.

[146] Ibid.

[147] René von Schomberg, "From the ethics of technology towards an Ethics of knowledge Policy abd Knwoledge Assessment," in *A working document for the European Commission services* (EU: European Commission's Directorate General for Research, 2007).

[148] Silvia Venier and Emilio Mordini, "Deliverable 4. FInal Report - A Privacy and Ethical Impact Assessment Framework for Emerging Sciences and Technologies," in *PRESCIENTproject. Privacy and emerging fields of scienbce and technoolgy: Towards a common framework for privacy and ethical assessmenttechnologies: Five case studies* (EC: Seventh Framework Programme (FP7), 2012), 62.

[149] G.T. Marx, "Ethics for the new surveillance", *The Information Society*, 14 (1998): 171-85.

the inspirations for offering ethical perspective on surveillance technologies come from ICTs ethics, computer ethics, ethics of technology, technology ethics, philosophy of technology, professional ethics or applied ethics.[150] Few researches have been devoted to ethical issues relating specifically to surveillance technologies. A lot of research still has to be done.

2.4.1.2 Ethics in the Official Documents at the European Union (EU) Level

At the European Union (EU) level, ethics appears at different stages.

2.4.1.2.1 The Ethical Key frame for Design and Implementation of all EU Policies

The ethical key frame for design and implementation of all EU policies set in the articles of the Lisbon treaty – and its reformed version signed on 13 December 2007[151] - and of the Charter of Fundamental Rights. This is nowadays representing the basis upon which the ethical issues of emerging technologies are identified. Fundamental human rights, ethical, human and societal concerns intermingle in what is becoming the European innovation model and their references are scattered in various several official documents.[152] The values stated in those two key

[150] For the distinction between those different fields of research, see: Silvia Venier and Emilio Mordini, "Deliverable 4. FInal Report - A Privacy and Ethical Impact Assessment Framework for Emerging Sciences and Technologies," in *PRESCIENTproject. Privacy and emerging fields of scienbce and technoolgy: Towards a common framework for privacy and ethical assessmenttechnologies: Five case studies* (EC: Seventh Framework Programme (FP7), 2012), 63.

[151] Treaty of Lisbon amending the Treaty on European, Union and the Treaty established the European Community, signed at Lisbon, 13 December 2007. Available at: http://eur-lex.europa.eu/JOHtml.do?uri=OJ:C:2007:306:SOM:EN:HTML

[152] This key frame for design and implementation of all EU policies has engendered a complex landscape of ethical governance tools of emerging technologies at the European Union (EU) level. For more details about the place of ethics in the European official documents and its inclusion in technology governance, see: Silvia Venier and Emilio Mordini, "Deliverable 4. FInal Report - A Privacy and Ethicak Impact Assessment Framework for Emerging Sciences and Technologies," in *PRESCIENTproject. Privacy and emerging fields of scienbce and technoolgy: Towards a common framework for privacy and ethical assessmenttechnologies: Five case studies* (EC: Seventh Framework Programme (FP7), 2012).

See also: Philippe Goujon and Catherine Flick, "Givernance approaches. A critical appraisal of theory and practice. Deliverable 4.1 ," in *ETICA: Ethical Issues of Emerging ICT Applications* (EC: Seventh Framework Programme, 2011).

See also: Serge Gutwirth et al., "Deliverable D1: Legal, social, economic and ethical conceptualisations of privacy and data protection," in *PRESCIENT. Privacy and emerging fields of science and technology: Towards a common framework for privacy and ethical assessment* (EC: Seventh Framework Programme, March 2011).

See also: Michael Frieddewald and Rocco Bellanova, "Deliverable 1.1: Smart Surveillance - State of the Art," in *SAPIENT. Supporting fundamental Al rights, Privacy and Ethics in surveillance Technologies* (EC: Seven Frameworks Programme, January 2012).

Ethics has been proved to be a dynamic notion, open to various operations of translation. Indeed, two main used can be easily identified in the EU-sponsored security research relating to the assembling of technology and security, for example through the formulation of the calls for application of the FP7 security Theme. (1) “References to ethics have been used, on the one hand, to reduce concerns about the effects of the growing reliance on technology in security policies to narrowly defined issues of trusts and acceptability”, while defining those issues in the general terms of societal and ethical issues. (2) “On the other hand, references to ethics have also been used to contest the standing of technology as a “salvation tool”, as a support both to academic studies and to more activist engagements with security, surveillance and technology”. See: Michael Frieddewald and Rocco Bellanova, "Deliverable 1.1: Smart Surveillance - State of the Art," in *SAPIENT. Supporting fundamental Al rights, Privacy and Ethics in surveillance Technologies* (EC: Seven Frameworks Programme, January 2012), 209.

documents are, for example, human dignity, freedom, democracy, human rights protection, pluralism, non-discrimination, tolerance, justice, solidarity and gender equality.

2.4.1.2.2 The European Group on Ethics in Science and New Technologies (EGE)

The European Group on Ethics in Science and New Technologies (EGE) is the organ which "provides the Commission with high quality and independent advice on ethical aspects of science and new technologies in connection with the preparation and implementation of Community legislation or policies"[153]. EGE publishes more specific texts dedicated to specialized fields of ethics[154]. EGE is currently working on an Opinion on the Ethics of Security and Surveillance Technologies which is to be finalised by the beginning of 2014. It would be the first EGE's opinion regards to those issues.[155]

2.4.1.2.3 Commission's Framework Programme Seventh (FP7) of Research

Regards to researches funded under the Commission's Framework Programmes Seventh (FP7) of research and technological development, a set of ethical questions are asked to whom make proposals in order to help candidates in identifying ethical dilemmas and issues that may rise in their research[156]. The questions-based approach is particularly interesting. Questions are classified under headings relating to ethical issues – e.g. Informed Consent, Privacy, Dual Use – and to specific "object" of research – e.g. Research on Human embryos/foetus, research on Animals or research involving Developing Countries. The specific *Data protection and privacy ethical guidelines*[157] is of interest and may be a start to identify ethical issues that may be taken into account in the SALT Framework. Nevertheless, other ethical issues listed for example under the heading *Informed Consent* must also be considered in more details.

[153] European Group on Ethics in Science and New Technologies to the European Commission, "The Protection of fundamental ethical principles in international research and innovation programmes," in *Report on the third meeting of the European Commission's international Dialogies on Bioethics*, ed. bepa: Bureau of European Policy Advisers (Brussels: European Commission , 2011). Available at: http://ec.europa.eu/bepa/european-group-ethics/docs/ibd/idb_20sept.2011.pdf

[154] Biotechnology was the first field of research and development for which ethics was applied at the European Union level. The EGE was established in 1991 for providing advices for this specific field. Since 2009 and the role of the EGE has been extended to other fields of research and development as: research on human embryos, patenting of inventions related to human stem cells, medical databases in clinic and multi-centre trials, etc. The EGE is currently working on an Opinion on the Ethics of Security and Surveillance Technologies which is to be finalised by the beginning of 2014.

[155] A first public Round table is organised on 18 September 2013 in Brussels, involving experts from inside and outside academia, the Chairs of the National Ethics Councils (NECs) or equivalent bodies within the EU and beyond, representatives of the European and international institutions, civil society organizations and other stakeholders and members of the public.

[156] CORDIS: Community research and Developement Information Service, "Getting Through Ethics Review," in *Sventh Framework Programme (FP7)* (EU: European Commission). Available at: http://cordis.europa.eu/fp7/ethics_en.html#ethics-cl

[157] Expert Working Group on data protection and privacy, "Data Protection and privacy ethical guidelines," in *Ethical Review in FP7* (EU: European Commission, 2009). Avalaible at: ftp://ftp.cordis.europa.eu/pub/fp7/docs/privacy.doc

2.4.1.3 Ethical Approaches

As already mentioned, different ethical theories exist in order to identify and to respond to ethical issues arising from scientific and technological innovation, while the first of them has been developed as bioethics in the field of medicine and medical research.[158] These different ethical theories can be set along a continuum bounded by two limits that are presented later in this section:

(1) *An essentialist conception of ethics* which assesses innovations with a normative frame based on universal and prescriptive principles.
(2) *A pragmatist conception of ethics* which defines ethics as a "savoir-faire", a capacity to make moral choice when faces with situations raising unprecedented ethical dilemmas or challenges.

2.4.1.3.1 Essentialism: Definition and Limits

For the common approach, ethics is dealing with notions of goodness, justice and dignity. This ethical vision can be qualified as *essentialist or principled conception of ethics* since the ethical vocation and expertise is to assess innovations with a normative frame based on universal and prescriptive principles. This is the way, Beauchamp and Childress[159], understand ethics when questioning the *benevolence of the technology.* When considering emerging technologies which confront us to unknown situation and unprecedented questions, this essentialism can lead to a normative violence well explained by Butler, in her book "Giving An Account of Oneself"[160] in which she refers to Adorno's text, "Minimum Moralia" (1969). Adorno, says Butler, guards against the universalizing pretension of a collective ethos, which can exert a certain form of violence. For Adorno, moral questions only arise when the community as a whole no longer shares a collective ethos. It is at this crux that the collective ethos can take a violent turn by laying claim to universality in order to recover its lost collective character.

This position is very in line with Dewey[161]who considers 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.

2.4.1.3.2 Ethics as a "Savoir Faire": a Pragmatic Approach

[158] For more detailed analysis of biomedical ethics, see: T. L. Beauchamp and J.F. Childress, *Principles of biomedical ethics (6th ed.)* (New York: Oxford University Press, 2008).

[159] Ibid. In chapter 6, the authors state that:« Whereas ***beneficence*** refers to an action done to benefit others, ***benevolenc***e refers to the morally valuable character trait—or virtue—of being disposed to act for the benefit of others ". See also:. http://plato.stanford.edu/entries/principle-beneficence/

[160] Butler, J. (2005), « Giving An Account of Oneself », Fordham University Press; 4 edition. We read the following french traduction, and we refer to it in this paper : Butler, J (2007) « Le récit de soi », PUF, Pratiques théoriques, 2007 (2005).

[161] Dewey, J., 1998, The Essential Dewey, L. Hickman and T.M. Alexander (ed.), Bloomington: Indiana University Press.

Opposite to this essentialist approach of ethics, Ladrière[162] suggests a pragmatist approach of ethics. According to him, ethics is a "savoir-faire", a capacity to make moral choice when faced with situations raising unprecedented ethical dilemmas or challenges. In that frame, Ladrière emphasizes that ethics is not the 'exclusive matter' 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 believe of the universality of the human reason"[163]

Hence, 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 is one 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 and according to Ladrière (op cit), 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.

For Dewey as for Ladrière, the ethical approach can only be collective and democratic, based on the confrontation of different positions.

In this collective deliberation, the responsibilities of the so-called expert are to explore the ethical issues involved by the technologies in progress, to elaborate methodologies to support a sound democratic deliberation and to inform this deliberation with his/her knowledge of the ethical tradition or cultural ethical heritage framing the deliberation.

So those authors do not refuse ethical principles but they do refuse to confer to them a normative or a prescriptive status. As well suggested by Dewey[164], we never affront an ethical problem from a "tabula rasa", without using some ethical references or principles transmitted by the tradition. 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 decision and action. For Dewey, these principles are explorative or analytical tools 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 of inquiry to question and forecast unknown ethical

[162] Ladrière, J., L'éthique dans l'univers de la rationalité, Artel/fides, Namur, 1997.

[163] Ibid.

[164] Dewey, J., *Démocratie et éducation*, Armand Collin, Paris, 1975.

puzzles. They have no intrinsic normative force but constitute a sort of moral background that may help facing an unknown moral situation.

2.4.2 Privacy Frameworks Regards to Ethical Issues

In this subsection, we propose two existent privacy frameworks relating to ethical issues which are of interest for the design of the SALT Framework and which should be analysed in more details during the second step of this project and more specifically regards the two specific surveillance technologies that are at the core of the PARIS project: CCTV and biometric surveillance technologies.

The following privacy frameworks regards to ethical issues were chosen among many others possible ones because of the different focus they put on ethical perspective regards to privacy and because they already treat, sometimes partially, CCTV and/or biometric surveillance technologies. Nevertheless, a deeper analysis is necessary in order to achieve a complete translation of those frameworks for the specific cases of CCTV and biometric surveillance.

2.4.2.1 Beatrice von Silva-Tarouca Larsen: Ethics and CCTV Surveillance

Beatrice von Silva-Tarouca Larsen developed **an ethical principles approach** in her book *Setting the watch, Privacy and the Ethics of CCTV Surveillance.*[165] After carrying a deep and thorough analysis of the Ethics of video surveillance, with a focus on the privacy interests in public space, anonymity interests of people being monitored, the possible legitimising role of crime prevention and the policy principles and the regulation of public CCTV surveillance, the author concludes that, first of all, there are moral reasons for broadening the concept of privacy to the public space. She focuses on two principles on what constitutes a "good life" – Dignity and Autonomy of the person – and that are the founding bases of the International Declaration of the Human Rights.

Von Silva–Tarouca Larsen argues in that sense that to "maintain his **dignity** and **autonomy**, a person must be able to control access to himself and protect himself against unwanted scrutiny and judgment, irrespective of whether or not he is secluded in his private home or is abroad in public".[166]

She also identifies **anonymity**, like all privacy-related claims, as of particular value in fending off the controlling powers of the State. Surveillance by CCTV is indeed seen by the author as "an instrument of social control with a wider scope than routine police enforcement" in that it "exercises pressure to conform to the expectations of the authorities 'standards of good behaviour and could create a chilling and oppressing effect". In that sense, in a report on video

[165] Beatrice von Silva-Tarouca Larsen, *Setting the watch, Privacy and the Ethics of CCTV Surveillance* (Oxford: Hart Publishing, 2011).

[166] For the recognition, from a legal perspective, of privacy interests in the public space as applied to video surveillance, see ECHR, Peck vs. UK, App. 44647/98, 28 January 2003. In this case, the European Court of Human Rights confirmed that individuals were entitled to have their privacy protected in public places, although their expectations of privacy were lower.

surveillance commissioned by the Council of Europe, Butarelli, Secretary General of the Data Protection Supervision Authority of Italy, had already identified that the widespread use of video surveillance was triggering a series of risks for human rights, endangering the freedom of behaviour (in so far as seeing without being seen could trigger submissive behaviours amongst citizens being watched) or the right to move anonymously and the right to privacy.[167]

Finally, when examining the question of "how much risk of intrusion into citizens' rights should policy makers be prepared to accept in the interest of trying to enhance protection against street crime", von Silva-Tarouca Larsen recognises that citizens are usually willing to accept a high level of intrusion and trade their anonymity for "unbstantiated promises of security". The responsibility of balanced policy making in the field of Security is thus devoted first and foremost to policy makers who should make a careful use of such a powerful tool. von Silva-Taruca Larsen argues that "CCTV is often ill thought-out and an unnecessary overreaction", pushing towards society into a "total surveillance society" where CCTV plays the role of informer. She therefore advocates for the implementation of complex regulatory schemes and administrative procedures to contain the negative potential of public CCTV surveillance schemes as there remains always a risk of intrusive practices. Proportionality of the interference, i.e. a careful balancing of the interests in Security and in protecting the social values at stake (e.g. the protection of fundamental rights), should guide public action.

2.4.2.2 David Wright: an Ethical Framework to Assess the Impact of ICTs

In order to reach his aim of developing a framework for the ethical impact assessment of information technology[168], David Wright had to study both ethical methods and issues related to ICTs. Reviews on related literature and pro-active proposition are parts of his paper which is structured in three distinct parts. The first one is devoted to specific values which may be of interest for the ethical impact assessment. A second one "identifies several ethical tools which can be used by decision-makers to engage stakeholders in considering the principles, values and issues contained in the previous section"[169], in considering ethical principles, values and issues. A third part is dedicated to the procedural aspects or practices of an ethical impact assessment.

For identifying relevant criteria for the SALT Framework which is the main task of our text, the first part of Wright's paper is an interesting guidance and may seem to be the sole relevant part regards to PARIS project. Indeed, the second and the third parts appear to be relevant to inform and/or to foster appropriate policies.

---

[167] Buttarelli, Giovanni. *Protection of personal data with regard to surveillance and Guiding principles for the protection of individuals with regard to the collection and processing of data by means of video surveillance*. Report for the European Commission. 2000. Available at: http://www.coe.int/t/dghl/standardsetting/dataprotection/Reports/Report_Buttarelli_2000.pdf

[168] David Wright, "A framework for the ethical impact assessment of information technology", *Ethics and Information Technology*, 3 (13) (2011): 199-226. A revised version was published in 2012: David Wright and Emilio Mordini, "Privacy and ethical impact assessment," in *Privacy impact assessment* (New York: Springer, 2012), 397-418.

[169] Ibid. 215.

Nevertheless, Wright is right in showing, with the help of different scholars he quotes, that technology assessment as a process, or a practice or a policy instrument, is not detachable from ethical question and issues. The same can be said about the various ethical tools listed, those "practical methods designed to improve ethical deliberation by capturing all ethically relevant aspects of an issue"[170].

As he indicated, the identification of ethics regards to values, on a one side, and to policy design, on the other side, is somehow artificial. They "are two different needs. Although the former supports the latter." For example, in Wright's proposed framework of ethical issues and principles, "under the principle of respect for autonomy, dignity is a social value (indeed, a fundamental right) while informed consent is a matter of policy. However, in particular situations, say with regards to the consequences of the application of a new technology, stakeholders could debate whether dignity is being respected or whether consent has truly been informed. The ethical tools can be used to engender debate over the extent to which social values are respected by a new technology (or whatever) and what might be the ethical implications arising from the application of a new technology".[171]

2.4.2.2.1 Stakeholders: Definition and Involvement

The need to involve stakeholders in the process, in the sense that stakeholders are defined as **all the people who are or may be interested in or are or may be affected by the outcome**[172], is another good example of ethical value that is directly linked to the way the TA as process or policy instrument is designed. Beyond the regular emphasis of European Union on the need to involve general public in regulatory processes with respect to modern technologies, this need for engaging stakeholders - as defined above- is well explained by the claim that technologies are neither neutral nor value-free. "Because IT artefacts are designed, constructed, and used by people, they are shaped by the interests, values, and assumptions of a wide variety of communities of developers, investors, users, etc"[173] say Orlikowski and Iacono. Those authors published an important paper in 2001 - "Reasearch commentary: Desperately seeking the "IT" in IT research-a call to theorizing the IT artifact" - in which they reviewed 188 articles published over 10 years in the journal *Information Systems Research.* Among the several conceptualisations of IT artefacts they found there, they make several points. One is worth being mentioned here. They mentioned the difficulty or sometimes the impossibility to understand or identify all the critical implications of an IT artefacts – both intended and unintended - for individuals, groups, organisations and society. Following this line of thought, Wright claims that "while it may be impossible to foresee all the ethical or other consequences of an emerging technology, nevertheless, an ethical impact assessment, **involving different**

[170] Ibid. 216-217. Those ethical tools or value appraisal techniques are well defined in: V. Beekman and F. W. A. Brom, "Ethical tools to support systematic public deliberations about the ethical aspects of agricultural biotechnologies", *Journal of Agricultural and Environmental Ethics*, 20(1) (2007): 3-12. And also in: Volkert Beekman et al., "Ethical Bio-Technology Assessment Tools for Agriculture and Food Production. Final Report Ethical Bio-TA Tools," in *Ethical Bio-TA Tools* (EC: Fifth Framework Programme, February 2006).

[171] Ibid. 201.

[172] The pragmatist philosopher John Dewey offers a similar definition of the public for an issue, that is neither "a general public", nor the sole interested and already involved people who are in institutional position to make their voices heard. See: John Dewey, *The public and its problems* (Ohio: Swallow Press, Ohio University Press, 1991).

[173] W.J. Orlikowski and C. S. Iacono, "Reasearch commentary: Desperately seeking the "IT" in IT research-a call to theorizing the IT artifact", *Information Systems Research*, 12(2) (2001): 121-34.

stakeholders from different disciplines and backgrounds, may be a good way of avoiding the traps discerned by Orlikowski and Iacono – i.e. of not seeing the context specificity of a technology and of not examining its critical implications for individuals, groups, organisations and society".[174] It is because "what I might regard as negative in the architecture of, let's say, a national IT system for electronic health records may well differ from what the designers think. This is clearly why **it is useful (necessary) to engage all relevant stakeholders** to discuss the consequences, to minimise information asymmetries and for all stakeholders, especially the proponents of the architecture, system, project, technology or whatever to engage with their peers with an open mind and a willingness to address problems and to recognise that it will most likely be in their own interests to do so at an early stage, rather than, when the system or architecture in installed and when there may be significant antipathy on the part of other stakeholders".[175]

It will be **a challenge for the SALT framework** to be able to translate such a necessity to involve different stakeholders who are not solely the experts who prepare the SALT framework. It is evident that **the involvement of stakeholders** – more than experts and less than a general public – is out of the scope of a SALT framework. The same can be said about the integration of the ethical tools above mentioned, **ethical tools** which may facilitate the involvement of stakeholders. However, I suggest investigating about the possible integration of several questions about the involvement of stakeholder into the SALT framework: Were stakeholders consulted or are going to be consulted? Who are those stakeholders? Is there one or several ethical tool which are used in order to help the involvement of those stakeholders and which ones?

2.4.2.2.2 A Questions-Based Approach

Wright rejects a prescriptive ethical guidance for the main reason that ethical values and principles are influenced by the context in which they are considered. He cited Moor[176] and Nissenbaum[177] as authors who highlight the need to consider ethics in context. Rather than this prescriptive ethical guidance, Wright adopts **a pragmatist approach** based on **questions aiming of identifying ethical issues[178]**. Those questions aim at **generating personal reflexion and debate among stakeholders**.

Another challenge for the SALT framework will be to address privacy issues (including ethical issues) in such a way that those questions will be likely to generate self questioning for the user

[174] David Wright, "A framework for the ethical impact assessment of information technology", *Ethics and Information Technology*, 3 (13) (2011): 203.

[175] Ibid., 204.

[176] J. H. Moor, "Why we need better ethics for emerging technologies?", *Ethics and Information Technology*, 7(3) (2005): 111-9.

[177] Helen Nissenbaum, "Privacy as contextual integrity", *Washington Law Review*, 79(1) (2004).

[178] A similar approach based on questions is also developed at CORDIS, as already mentioned above, but also by scholars such as Gary Marx, Van Gorp, Kuzma et al.

See: G.T. Marx, "Ethics for the new surveillance", *The Information Society*, 14 (1998): 171-85.

See also: A. Van Orp, "Ethics in and during technological research; An addition to IT ethics and scienbce ethics," in *Evaluating new technologies*, ed. P. Sollie and M. Düwell (Dordrecht: Springer, 2009), 35-50.

See also: J. Kuzma and al., "An integrated approach to oversight assessement for emerging technologies", *Risk Analysis*, 28(5) (2008): 1197-219.

of the SALT framework and eventually debate among stakeholders (with the meaning defined above).

Wright uses the ethical values that form the key frame for design and implementation of all EU policies and that was mentioned above in this section. “The values set out in these texts could serve as an ethical guidance. In fact, it has been adopted here as the baseline for identifying the key values or ethical principles or issues.” [179]

He structures his ethical frameworks with four ethical values/principles posited in Beauchamp and Childress[180], used as headings for several ethical issues. A brief explanatory text and a set of questions follow each of those ethical issues “aimed at helping the technology developer or policy-maker to facilitate a consideration of the ethical issues which may arise in their undertaking.”[181]

A remark is worth to be mentioned here, r**egards to the SALT framework**. The specific people or person or group of people who use the SALT framework should be 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 different stakeholders.

2.4.2.2.3 Ethical Values/Principles and Related Ethical Issues

Here are the several ethical values/principles and related ethical issues retained by Wright:

(1) Respect of autonomy (right to liberty)
   i. Dignity
   ii. Informed consent
   iii. Nonmaleficience (avoiding harm)
   iv. Safety
   v. Social solidarity, inclusion and exclusion
   vi. Isolation and substitution of human contact
   vii. Discrimination and social sorting

(2) Beneficence
   i. Universal service
   ii. Accessibility
   iii. Value sensitive design
   iv. Sustainability

[179] David Wright, "A framework for the ethical impact assessment of information technology", *Ethics and Information Technology*, 3 (13) (2011): 202.

[180] T. L. Beauchamp and J.F. Childress, *Principles of biomedical ethics (5th ed.)* (New York: Oxford University Press, 2001).

[181] Ibid. 204.

(3) Justice
    i. Equality and fairness (social justice)

(4) Privacy and data protection
    i. Collection limitation (data minimisation) and retention
    ii. Data quality
    iii. Purpose specification
    iv. Use limitation
    v. Confidentiality, security and protection of data
    vi. Transparency (openness)
    vii. Individual participation and access to data
    viii. Anonymity
    ix. Privacy of personal communications: monitoring and location tracking
    x. Privacy of the person
    xi. Privacy of personal behaviour

Further analysis of those ethical values/principles and related ethical issues is needed and must imply a particularly focus on the questions formulated by Wright regards to each of them. They may be particularly interesting for the SALT Framework.

2.5 Socio-political and ethicAl Recommendations for SALT Framework

In the section 2.2., devoted to **psychological perspective on privacy**, several recommendations have been made. Psychology is an applied and academic field that studies the human mind and behaviour. Research in psychology seeks to understand and explain how we think, act and feel. Applied psychology focuses on the use of different psychosocial principles to solve real world problems. So it is important to take into account the psychology perspective when developing the SALT framework. It must consider its definition, its dimensions, its functions and the effect the lack of privacy can cause on the population. People expect to have a balance between the privacy they desire and the one they obtain. We have to keep in mind that one of the objectives of PARIS is to help in developing privacy-enhanced surveillance systems. The study of privacy-security relationship from the point of view of social psychology must:

- Analyze the balance between desired privacy and achieved privacy in different types of spaces.
- Evaluate the optimal degree of surveillance in different spaces (public, semi-private and private).
- Analyze the acceptance of security systems implementation.
- 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.
- Evaluate the conflict among privacy, security and surveillance systems in the population.
- Analyze the social and psychological consequences of the invasion (lack) of privacy.

The section 2.3 (Privacy from a Socio-Political Perspective) contains two main inputs. (1) The claim of privacy as a social value is the keystone of the socio-political perspective on privacy. That is defending privacy as a social value, while challenging the sole addressing a challenge both to the conception of privacy as an individual right and/or value and to the one of its consequential turn of mind, that is the balancing relationships between privacy – conceived as an individual interest and/or value and/or right – and other social values such as (national) security. (2) The general claim in favour of privacy as a social value must be sustained by a conceptualization of privacy. Regards to the kind of conceptualization proposed, the effects are very different. In fact, the way privacy is conceptualised allows identifying very different kind of harms or concerns. This is worth emphasizing for the construction of the SALT framework which may be very different regards to the kind of taxonomy or conceptualization of privacy retained for its construction. Indeed, as a short term research aim, the reading of different existent taxonomies of privacy reveals that, while planning the construction of the taxonomy which will be relevant for the SALT Framework, it is necessary to be transparent in the methodological design of the taxonomy and reasons for choosing certain criteria rather than others.

Therefore a full subsection is dedicated to the identification – their outline and their interests for the SALT framework - different taxonomies of privacy which are of interest for the construction of the SALT Framework. In the next deliverable (D 2.2), a detailed analysis of their content still must be done regards to different details such as, for example: (1) The types of categories retains in the taxonomies. For example, a taxonomy which takes into account as a relevant criteria the intellectual property rights regime over information is very different than one which takes into account the social context of intersubjectivity; (2)Ttheir purpose. Indeed, the purpose of the taxonomy is not trivial. Helping Law enforcement or helping the design of a system-to-be which integrates Privacy-By-Design principles are two very different purposes. Regards to the kind of purpose, some common criteria to the analyzed taxonomy may be relevant (or not) for the SALT Framework; (3) the sources used. For example, legal sources or theoretical rationales built on the study and analyze of new and emerging technologies provide very different perspective on privacy; (4) The consequences and the types of consequence of the breaking of the criteria used in those different taxonomies. For example, the consequence may be law pursuit or a psychological effect on individuals. (5) Criticisms that have been addresses to those different taxonomies.

The several existent taxonomies which are worth being analyzed in the next deliverable are the following ones. (1) Finn, Wright and Friedewald: seven types of privacy (2) Steeves: privacy in intersubjective and social interactions (2) Solove: A taxonomy of privacy problems (3) Nissenbaum: contexts of privacy (4) Extended version of Privacy Impact Assessment.

The **section 2.4 (Privacy from an Ethical Perspective)**, proceeds to a review of the state-of-the art of the ethical perspective on privacy. Regards to the aim of this text of indentifying relevant criteria for the design of an ethical-based approach within the SALT framework, the focus is placed on (1) several ethical approaches that may be of interest for extracting ethical issues relating to surveillance technologies and (2) on several existent ethical frameworks. Different key sources are identified along this section and listed at this end with the recommendation to analyze them in details during the next step of this research. The next deliverable (D 2.2) will build on the findings of this section to provide a definitive list of requirements, adapted to the context of surveillance.

One specific remark is worth mentioning. **Surveillance technologies are a challenge for ethics.** If generally speaking, what is an “ethical issue” is in itself an issue, the question remains largely

open regards to surveillance technologies. This is true for different reasons. A first reason is related to surveillance technologies itself. The argument is also true for ICT's technology at large. Indeed, "**the development of new ICTs and other security technologies are generally complicating the definition of the role of ethics**, as well as the identification of its theoretical approaches and operational instruments needed to address ICTs-related issues."[182] One explanation is that intentional actions are at the heart of traditional ethics of science and technology which thinks from the duo of the lonely scientific Frankenstein who intentionally creates his creature. However, scientific and technological developments "have the potential to bring **unintentional or highly unpredictable consequences that are usually the result of collective decisions**".[183] According to René von Schomberg, we do not have ethical theory at our disposal which would be an *Ethics of Knowledge Policy and Knowledge Assessment*[184] that is an ethics which addresses "both the aspect of **unintentional side consequences** (rather than intentional actions) and the **aspect of collective decisions** (rather than individual decisions)."[185] A second reason is that it is not sure that a specific field of research such as *surveillance ethics* exist. If **Gary T. Marx** was one of the first scholars who identified ethical issues and coined ethical tools in order to help in identifying them regards to surveillance technologies[186], most of the inspirations for offering ethical perspective on surveillance technologies come from ICTs ethics, computer ethics, ethics of technology, technology ethics, philosophy of technology, professional ethics or applied ethics.[187] Few researches have been devoted to ethical issues relating specifically to surveillance technologies. **A lot of research still has to be done.**

Several sources were identified for further investigating towards ethical issues and criteria that may be relevant for their integration into the SALT framework. (1) The Lisbon treaty and its reformed version signed in 2007. (2) The Charter of Fundamental Rights. (3) The European Group on Ethics in Science and New Technologies (EGE) and specially its current work on an Opinion on the Ethics of Security and Surveillance Technologies which is to be finalised by the beginning of 2014, Opinion that will be the first one regards to those issues. A first public Round table is organised on 18 September 2013 in Brussels, involving experts from inside and outside academia, the Chairs of the National Ethics Councils (NECs) or equivalent bodies within the EU and beyond, representatives of the European and international institutions, civil society organizations and other stakeholders and members of the public. (4) Commission's Framework Programme(FP7) Seventh of research. Regards to researches funded under the Commission's Framework Programmes Seventh (FP7) of research and technological development, a set of ethical questions are asked to whom make proposals in order to help candidates in identifying

[182] Ibid., 61.

[183] Ibid.

[184] René von Schomberg, "From the ethics of technology towards an Ethics of knowledge Policy abd Knwoledge Assessment," in *A working document for the European Commission services* (EU: European Commission's Directorate General for Research, 2007).

[185] Silvia Venier and Emilio Mordini, "Deliverable 4. FInal Report - A Privacy and Ethical Impact Assessment Framework for Emerging Sciences and Technologies," in *PRESCIENTproject. Privacy and emerging fields of scienbce and technoolgy: Towards a common framework for privacy and ethical assessmenttechnologies: Five case studies* (EC: Seventh Framework Programme (FP7), 2012), 62.

[186] G.T. Marx, "Ethics for the new surveillance", *The Information Society*, 14 (1998): 171-85.

[187] For the distinction between those different fields of research, see: Silvia Venier and Emilio Mordini, "Deliverable 4. FInal Report - A Privacy and Ethical Impact Assessment Framework for Emerging Sciences and Technologies," in *PRESCIENTproject. Privacy and emerging fields of scienbce and technoolgy: Towards a common framework for privacy and ethical assessmenttechnologies: Five case studies* (EC: Seventh Framework Programme (FP7), 2012), 63.

ethical dilemmas and issues that may rise in their research[188]. The questions-based approach is particularly interesting. The specific *Data protection and privacy ethical guidelines*[189] is of interest and may be a start to identify ethical issues that may be taken into account in the SALT Framework. Nevertheless, other ethical issues listed for example under the heading *Informed Consent* must also be considered in more details.

Among different ethical approaches, we favoured an ethical approach that consider **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) Seventh 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 ethical perspective 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 stable responses.

Two existent **privacy frameworks regards to ethical issues** were presented. Other ones may still be identified during the next step of this research. Those two ones are of interest for the design of the SALT Framework and should be analysed in more details during the second step of this project and more specifically regards the two specific surveillance technologies that are at the core of the PARIS project: CCTV and biometric surveillance technologies. (1) **Beatrice von Silva-Tarouca Larsen: Ethics and CCTV surveillance.** Her book is especially interesting because it deals specifically CCTV surveillance technologies. (2) **David Wright: an ethical framework to assess the impact of ICTs**. This author makes very important proposals which are of interest for identifying relevant criteria for the SALT framework. He identifies different ethical values/principles/issue, explains them and offers a question-based approach with concrete questions that may be addressed regards to all of those ethical issues. Here are those ethical values/principles and related ethical issues retained by Wright. Further analysis of those ethical values/principles and related ethical issues is needed and must imply a particularly focus on the questions formulated by Wright regards to each of them.

(1) Respect of autonomy (right to liberty)

xii. Dignity

xiii. Informed consent

xiv. Nonmaleficience (avoiding harm)

xv. Safety

xvi. Social solidarity, inclusion and exclusion

xvii. Isolation and substitution of human contact

xviii. Discrimination and social sorting

(4) Beneficence

i. Universal service

ii. Accessibility

iii. Value sensitive design

[188] CORDIS: Community research and Developement Information Service, "Getting Through Ethics Review," in *Sventh Framework Programme (FP7)* (EU: European Commission). Available at: http://cordis.europa.eu/fp7/ethics_en.html#ethics-cl

[189] Expert Working Group on data protection and privacy, "Data Protection and privacy ethical guidelines," in *Ethical Review in FP7* (EU: European Commission, 2009). Avalaible at: ftp://ftp.cordis.europa.eu/pub/fp7/docs/privacy.doc

iv. Sustainability

(5) Justice

i. Equality and fairness (social justice)

(6) Privacy and data protection

i. Collection limitation (data minimisation) and retention
ii. Data quality
iii. Purpose specification
iv. Use limitation
v. Confidentiality, security and protection of data
vi. Transparency (openness)
vii. Individual participation and access to data
viii. Anonymity
ix. Privacy of personal communications: monitoring and location tracking
x. Privacy of the person
xi. Privacy of personal behaviour

Beside the list of ethical values/principles and related issues, several points received a particularly strong attention because they are real **challenges for the design of the SALT framework**

(1) The need to involve stakeholders in the process, in the sense that stakeholders are defined as **all the people who are or may be interested in or are or may be affected by the outcome.** It will be **a challenge for the SALT framework** to be able to translate such a necessity to involve different stakeholders who are not solely the experts who prepare the SALT framework. It is evident that **the involvement of stakeholders** – more than experts and less than a general public – is out of the scope of a SALT framework. The same can be said about the integration of the ethical tools above mentioned, **ethical tools** which may facilitate the involvement of stakeholders. However, I suggest investigating about the possible integration of several questions about the involvement of stakeholder into the SALT framework: Were stakeholders consulted or are going to be consulted? Who are those stakeholders? Is there one or several ethical tool which are used in order to help the involvement of those stakeholders and which ones?

(2) Another challenge for the SALT framework will 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).

(3) A remark is worth to be mentioned here, regards to the SALT framework. The specific people or person or group of people who use the SALT framework should be **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 different stakeholders.

3 Privacy from a Legal Perspective - European Legal Framework for Privacy and Data Protection

Claire Gayrel (CRIDS - University of Namur)

The present chapter aims at providing a global review of the European legal requirements in the matters of privacy and data protection, in particular in order to understand the balance between privacy and other counterveiling interests and the legal 'concepts' that the SALT framework will have to integrate. [190] The objectives of the present section is : i) to understand the *balance between privacy and public space*, which we understand as the extent to which privacy interests are at stake when surveillance systems are deployed, notably in public spaces and; ii) to identify the relevant criteria which structure the perimeter of a SALT framework. From a legal perspective, such criteria are composed of the applicable international/European/national relevant sources of law with respect to the protection of privacy and personal data and sectoral legislations in relation to specific technologies (e.g. videosurveillance), their scope of protection/application, definitions, principles and obligations.

In this aim, the present chapter is divided in six parts. First, we will come back to the essential issues of the debate surrounding the *privacy v. public security balance* in the European Union in order to have an overview of the legal "context" within which the PARIS project intends to produce innovative solution (1). Second, we will present the legal landscape of the protection of privacy and personal data in the Member States, which will be the occasion to identify the main relevant normative sources that may be taken into account by the SALT framework (2). Third, we will present with more details the caselaw of the European Court of Human Rights (ECHR) with regard to the right to private life and data protection, with specific attention on some important developments in relation to the extent of protection of private life to informational issues and public surveillance (3). Fourth, we will present the core concepts and principles enshrined in the Directive 95/46, which is the main relevant EU wide instrument on the protection of personal data applicable in all Member States (4). Because this instrument does not address the issues of protection of personal data in relation to specific surveillance technologies, we will finally look at European guidance with regard to videosurveillance activities (5) and biometric technologies (6) and how these matters are dealt with in two Member States, Belgium and France.

3.1 Balancing Privacy v. Surveillance: General 'Context'

The present section intends to inform the PARIS project (and the consortium partners) about the "context" within which it intends to produce innovative solution for balancing privacy/data protection rights against competing interests. It constitutes an "introductory" section to the legal perspective and challenges of surveillance operations to privacy and data protection rights. It starts by coming back to the notion of privacy, in order to briefly recall the evolution of the scope of this right from the right to be let alone towards the emergence of a right to data protection. Follows the presentation of some contrasted views and issues raised regarding the relation and interaction between the right to privacy and the right to data protection, which are

[190] Description of work, Task 1, point 1

both highly relevant for PARIS project. We will then discuss the issue of balancing privacy with public competing interests and the current trends in EU lawmaking in the balance between privacy and security. We will finally see the various tools/methods under development to carry out and enforce a proper and fair balance.

3.1.1 Scope of Privacy: from the Right to be let Alone to the Right to Data Protection[191]

The conceptualization of the right to privacy is attributed to Warren and Brandeis's famous article published in 1890 in the Harvard Law Review in reaction to the development of modern devices to reproducing sounds and images, in particular photographs and exploitation or publication by press of the said images.[192] They conceived the right to privacy as a general right of the individual to be let alone. Although implicit, traditions of privacy can also be traced back in continental law.[193] Withman notably traces back the rise of French privacy law partly in the introduction of the freedom of press, which was considered as a threat to one's personal honour[194], and partly in relation to the culture of Paris art world, which made arise the right to one's image[195]. In Germany, the conception of privacy is wholly based on the concept of personality, which rests on the idea of free self-realization, inspired by Christian Humanism. Referring to Robert Post, Whitman considers that the fundamental contrast between the US and the continental conceptions of privacy consists in the distinction between privacy as an aspect of dignity and privacy as an aspect of liberty. European privacy protections are a right to respect personal dignity, as the rights to one's image, name and reputation. By contrast, privacy in America is rather oriented toward the value of liberty, especially the right to freedom from intrusions by the State and the right to one's own home.[196] However, Whitman also specifies that this contrast is far from being absolute, and that there are actually only "relative differences" between both systems.

Indeed, the acknowledgement of the right to privacy in Europe in Article 8 of the European Convention on Human Rights (ECHR) of 1950[197] precisely aimed at preventing intrusions by the State in the sanctity of home and correspondence. Providing that "*everyone has the right to*

[191] This brief and short section is destined to inform about the « context » of the PARIS project in relation to privacy and data protection and does not intend to exhaustively review the various conceptions of privacy. For a global overview of these various theories of privacy and their shortcomings, see for instance Daniel Solove, Understanding Privacy (Cambridge: Harvard University Press, 2008), Chap. II pp. 12-39. The author reviews some of the most outstanding attempts to conceptualize privacy by scholars, such as the right to be let alone (Warren and Brandeis), secrecy, control over personal information, personhood (as J. Rubenfeld and its approach of privacy as an anti-totalitarian right), intimacy

[192] Samuel D. Warren and Louis D. Brandeis, "The Right to Privacy", *Harvard Law Review* Vol. IV. No. 5 (1890)

[193] James Q. Withman, "The Two Western Cultures of Privacy: Dignity Versus Liberty", *The Yale Law Journal* 113 (2004): 1151-1221

[194] For example, the French Constitution of 1791 included the freedom of press, but at the same time it added protections against "calumnies and insults relative to private life"

[195] During the decades after 1819, the primary means of protecting one's honour was through the duel; From the 1850s, the right to one's image emerged (1867 Dumas Case and 1877 Jean-Auguste-Dominique Ingres Case).

[196] *Ibidem*, p. 1162: "*On the one hand, we have an Old World in which it seems fundamentally important not to lose public face; on the other, a New World in which I seems fundamentally important to preserve the home as a citadel of individual sovereignty*"

[197] Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, signed in Rome, 1950

respect for his private and family life, his home and his correspondence" and that "*there shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society* […]", the right to privacy primarily focused on interferences by States in one's private sphere, conceiving the right to privacy as conferring a right to "opacity".[198]

As the Court enjoys recalling, the Convention is a "*living instrument*"[199] that seeks to provide effective and concrete rights. This has led the Court to expand progressively the notion of private life and the obligations held by States under Article 8. Privacy evolved from an opacity tool against the State towards a much wider instrument of decisional autonomy.[200] Its scope came to cover virtually all the domains in which individuals are confronted with the need to make fundamental choices in their life, such as sexual life and sexual preferences, personal and social life, relationships with other human beings, choice of residence et cetera.[201] Along the expansion of the scope of protection afforded under Article 8, the Court also interpreted extensively the obligations of the States under the horizontal effect of the Convention. This allowed the Court to address interferences into individuals' privacy by non-State actors.

The adoption by the Council of Europe of the Convention for the protection of individuals with regards to automatic processing of personal data in 1981[202], formalized fundamental fair information practices, such as the principle of fair processing, purpose limitation principle, principle of legitimacy and recognition of subjective rights of data subjects to access and rectify data relating to them et cet… As will be explained in the next section of the present chapter, the Court of Strasbourg progressively integrated elements of data protection within Article 8 caselaw. The adoption in the EU of legislative instruments aiming at the harmonization of data protection regulations between Member States (and subsequent liberalization of flows of personal data)[203] further contributed to the rise of a right to data protection, today formally recognized in Article 8[204] of the EU Charter of Fundamental Rights.[205]

[198] Paul De Hert and Serge Gutwirth, "Privacy, data protection and law enforcement. Opacity of the individual and transparency of power", in *Privacy and the criminal law*, ed. E. Claes et al. (Antwerpen/Oxford: Intersensia, 2006), 61-104

[199] The Court first aknowledged it in *Tyrer v. United Kingdom*, 25 April 1978

[200] Antoinette Rouvroy et Yves Poullet, "The Right to Informational Self-Determination and the Value of Self-Development", in *Reinventing Data Protection?*, ed. Serge Gutwirth et al. (Springer, 2009), 64-67

[201] As will be explained further in chapter III of the present report the Court stated that the notion of private life is a broad one which is not susceptible to exhaustive definition.

[202] Council of Europe Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data signed in Strasbourg, 1981

[203] First and foremost Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the automatic processing of personal data and on the free movement of such data, *OJEC* L281, 23 November 1995. In relation to protection of privacy in the electronic communications sector: Directive 2002/58/EC of the European Parliament and of the Council of 17 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, *OJEU* L201, 31 July 2002. In relation to the police and judicial cooperation between Member States: Council Framework Decision 2008/977/JAI of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, *OJEU* L350, 30 December 2008 ; in relation the data protection in EU institutions and agencies : Regulation 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community Institutions and bodies and on the free movement of such data, *OJEC* L8, 12 January 2001

[204] Article 8 of the Charter of Fundamental Rights of the EU:

3.1.2 Relation Between the Right to Privacy and the Right to Data Protection

While the legislations in the field of data protection clearly originate in the right to privacy, the relation between both rights, in particular in view of the recent autonomisation of the right to data protection from the right to privacy in the EU Charter, raises some issues.

From the point of view of the ECHR, it must be highlighted that if elements of data protection have been integrated under the notion of private life in ECHR caselaw, the Court did not bring a general recognition of data protection rights under Article 8 of the Convention.[206] The notion of private life is broader insofar as it aims at protecting the underlying values of dignity and autonomy of the individuals (right to self-determination).[207] In particular, private life concerns may be raised under Article 8 of the ECHR regarding a processing technology in spite of the absence of processing of personal data as such.[208] However, the scope of personal data protection may also be broader than the one of private life in that it enshrines a series of principles that are presently not fully integrated within ECHR caselaw under Article 8 or as far as data protection regulations may apply to certain processing that do not raise private life concerns according to the Court.[209] This implies that Privacy and data protection do not fully overlap, raising questions as to their respective roles and interactions.

P. De Hert and S. Gutwirth identified these differences in scope on the basis of a distinction between privacy as a 'tool of opacity' (stopping power, setting normative limits to power), and data protection mainly as 'tools of transparency' (regulating and chanelling necessary/reasonable/legitimate power).[210] They address and support the underlying normative character/potential of privacy as a tool to prohibit certain uses of powers, while data protection as "transparency tools" would intervene only after the normative choices to resort to such powers is taken in order to frame them. From that perspective, the authors welcome positively the constitutionalisation of the right to data protection in the EU Charter, insofar as

1. Everyone has the right to the protection of personal data concerning him or her.

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

3. Compliance with these rules shall be subject to control by an independent authority.

[205] For the record, the EU Charter of Fundamental Rights adopted in 2000 has now binding effect since 2010 with the entrance into force of the Lisbon Treaty on European Union (Art. 6) that the Charter has acquired the same value than the EU Treaties.

[206] Paul De Hert, "Balancing security and liberty within the European human rights framework. A critical reading of the Court's case law in the light of surveillance and criminal law enforcement strategies after 9/11", *Utrecht Law Review* Vol. 1 issue 1 (2005)

[207] Antoinette Rouvroy and Yves Poullet, "The Right to Informational Self-Determination and the Value of Self-Development",*op. cit.*

[208] Personal data are defined in Convention 108 and other EU instruments as "*any information relating to an identified or identifiable individual*"

[209] See in section II of the present chapter an example in relation to videosurveillance. For a detailed analysis see Paul De Hert, "Balancing security and liberty within the European human rights framework…", *op. cit.*

[210] Paul De Hert and Serge Gutwirth, "Privacy, data protection and law enforcement. Opacity of the individual and transparency of power", *op. cit.*

data protection has a precise target which is distinct from privacy concerns and aims at organizing the fair processing of personal data by both public and private actors.

In contrast, A. Rouvroy and Y. Poullet have raised concerns regarding the constitutionalisation of the right to data protection from the right to privacy, in that it risks obscuring the essential relation between them and further weaken the anchorage of data protection in the fundamental values of dignity and autonomy.[211] In their perspective, both data protection and privacy must not be seen as a final, intrinsic value, an end in itself, but rather as an intermediate, instrumental tool in order to preserve and promote other fundamental values and rights. Privacy is conceived as a pre-condition for the exercise and enjoyment of most other fundamental rights and freedoms. Further, the authors argue that privacy and data protection, as far as they contribute to foster autonomic capabilities of individuals are, in a given society at a given time, necessary for sustaining a vivid democracy.[212] In this sense, privacy is not only an individual right but also a social value.[213]

Besides the constitutionalisation of the right to data protection in the Charter, the relation and future articulation of this right with the right to privacy is also questioned by the Draft Regulation[214] and Draft Directive[215] proposals of the European Commission for the respective replacement of the Directive 95/46 and Framework Decision 2008/977. In both proposals, references to the right to privacy have been removed from both the explanatory memorandums and content of the instruments, and widely known notions of "privacy by design" and "privacy impact assessment" have been transformed into "data protection by design" and "data protection impact assessment".[216] The deletion of privacy behind personal data protection in the proposals seems to support an evolution in the favour of an autonomisation of the right to data protection from the right to privacy, in addition to its constitutionalisation.[217] However, as strengthened by G. González Fuster, "*there is nothing in EU pointing unequivocally in that direction*". Therefore, the degree to which the right to the

[211] Antoinette Rouvroy and Yves Poullet, "The Right to Informational Self-Determination and the Value of Self-Development", *op. cit.*

[212] *Ibidem*, p. 50

[213] See PRACTIS Report, D.5.1 Overview on ethical and legal issues

[214] European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, COM(2012)11 final, Brussels, 25.1.2012

[215] European Commission, Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, COM(2012)10 final, Brussels, 25.1.2012

[216] On the deletion of « privacy » in the legislative proposals of the European Commission, see Luiz Costa and Yves Poullet, "Privacy and the Regulation of 2012", *Computer Law & Security Review* 28 (2012): 254-262 and Gloria Gonzáles Fuster, "Security and the future of personal data protection in the European Union", *Security and Human Rights* 28 (2012): 331-342

[217] Both can be distinguished. As explained by Gloria Gonzáles Fuster, "*the pertinence of alluding the right to the protection of personal data in post-Lisbon EU personal data protection instruments is in any case hardly debatable, taking into account its presence both in the Charter and the Treaties. What is nevertheless questionable is the suitability of referring to such right not in addition to the right to respect for private life, but in place of it.", op. cit.*, p. 335

protection of personal data can be regarded as autonomous from the right to privacy is questionable.[218]

The intrinsic link between privacy and data protection seems to remain in spite of the constitutionalisation of the right to data protection in the Charter. Indeed, if the European Court of Justice recently recognized the fundamental right to data protection enshrined in article 8 of the EU Charter[219], it has also stated that "*the limitations which may lawfully be imposed on the right to the protection of personal data correspond to those tolerated in relation to Article 8 of the Convention* [ECHR]".[220] Further, the Court recalled that "*that fundamental right is closely connected with the right to respect of private life expressed in Article 7 of the Charter*."[221] In line with the Court's judgement and in line with Y. Poullet and A. Rouvroy, we believe data protection is not an end *per se*, but rather an instrument to the service of the protection of private life and other values, in particular the autonomy and dignity of individuals. Above the academic debate on the interaction/relation and future of privacy and data protection rights, the SALT framework should address and integrate both rights, as Member States are bound by their commitments both towards the ECHR and the European Union.

3.1.3 Balancing Privacy v. Countervailing Interests: the Proportionality Principle

The right to privacy may conflict with other *values*, *human rights*, or *public and private interests*. It may indeed conflict with other fundamental rights, such as freedom of expression, or freedom of the press. Privacy may also conflict with public interests, among which public/national security interests that are more specifically foreseen in the framework of the present research project.

Indeed, privacy is not an absolute right and remains subject to legitimate limitations according to article 8§2 of the ECHR. This implies that when privacy conflicts with other interests, this requires arbitration between those competing interests. The resolution of conflicts in the matter of fundamental rights, in particular those enshrined in Articles 8 to 11 of the ECHR, generally requires a *balancing of interests*, which derives from the proportionality policy applied by the Court. The proportionality principle originates in German administrative law in the XIX century and has migrated to EU, ECHR and elsewhere[222] to become "*one of the defining feature of global constitutionalism*".[223] It has been analysed as one of the most significant factor of extension of the judicial power during the XXth century, implying substantial modifications of

[218] *Ibidem*, p. 336. As argued by the author, there is no clear guidance from the European Court of Justice regarding the identification of the existence of a right to personal data protection, its possible interpretation as an autonomous right and the provisions relevant for the determination of lawful limitations to it.

[219] E.C.J., 9 November 2011, *Volker und Markus Schecke GbR and Harmut Eifert v. Land Hessen*, joint cases C-92/09 and C-93/09

[220] *Ibidem*, §52

[221] *Ibidem*, §47 and E.C.J., 24 November 2011, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECEMD) v. Administración, del Estado*, joint cases C-468/10 et C-469-10, §41

[222] Paul Martens, "L'irrésistible ascension du principe de proportionnalité", in *Présence du droit public et des droits de l'Homme. Mélanges offerts à J.Velu* (Bruxelles : Bruylant, 1992) : t. 1, p. 49.

[223] Alec Stone Sweet and Jed Matthews, "Proportionality, Balancing and Global Constitutionalism", *Columbia Journal of Transnational Law* 47 (2008): 74

the function of adjudication of litigations.[224] But proportionality is not the only way of adjudication. The balancing method used by the ECHR can be distinguished from a categorical approach, dominant in the US Supreme Court caselaw.[225] American Courts do not explicitly engage in balancing but rather in categorisations, in that they determine the scope of a right in order to leave out or include within it elements of this right and avoid conflict with other interests. The proportionality principle, as a balancing method, is said to offer more flexibility in the adjudication of conflict between human rights and national security interests, provided that the Court are willing to exercise its power of judicial review independently.[226] Nevertheless, the application by the ECHR of the proportionality principle reveals a case by case approach that also raise concerns regarding legal certainty[227], in particular in relation to the application of the proportionality test in the framework of Article 8§2 of the Convention. As yet, from a legal perspective and for the purposes of the SALT framework, the balancing objective of PARIS project is understood in reference to the proportionality principle. In section 3 of the present report, we will come back with more details on the content of the proportionality principle in ECHR caselaw, since it is of primordial relevance for surveillance system implemented in EU Member States.

3.1.4 Balancing Privacy v Surveillance: Some Current Trends in EU Lawmaking

Prior to the power of the judicial power to review privacy limitations, it is first and foremost the role of the legislator to address the issue of the balance between privacy and security interests. Following the 9/11 terrorist attacks, Member states of the European Union have adopted particular measures to face the terrorist threats, but more generally to reinforce the judicial and police cooperation in criminal matters in the so-called "area of Freedom, Security and Justice" of the EU[228]. The various initiatives adopted under this objective composes the increasingly complex landscape of collection, storage and cross-border exchange of personal data between Member States in this area. This landscape cannot be exhaustively restituted here.[229] Instead, based on previous research in this field, we believe it is worth mentioning some major trends in the development of the Area of Freedom, Security and Justice challenging the balance between privacy and security: a broad notion of security, the enlargement of access to European databases, the increasing recourse to commercial data for law enforcement purposes and the deletion of privacy/freedoms considerations behind data protection safeguards.

[224] Olivier De Schutter, *Fonction de juger et droits fondamentaux. Transformation du contrôle juridictionnel dans les ordres juridiques américain et européens*, (Bruxelles: Bruylant, 1999)

[225] *Ibidem* and Stefan Sottiaux, *Terrorism and The Limitations of Rights, the ECHR and the US Constitution*, (Oxford: Hart Publishing, 2008)

[226] According to Stefan Sottiaux, a flexible approach induces decision-makers, both in the political and judiciary branches, to adopt "*strategies of accommodation*", while categorical approaches give rise to "*strategies of avoidance*". While balancing approach encourage political and judicial branches to respond to the security threat from within the human rights framework, *categorical approaches result in all-or-nothing solutions*.

[227] Sebastien Van Drooghenbroeck, *La proportionnalité dans le droit de la convention européenne des droits de l'homme, prendre l'idée simple au sérieux*, (Bruxelles : Bruylant, 2001) : chap. III

[228] The objective of the European Union to establish an area of justice Liberty and Security has been introduced in the Amsterdam Treaty of 1997. It is now mentioned in Article 3§2 of the TEU

[229] For an exhaustive review, see Franzisca Boehm, *Information Sharing and Data Protection in the Area of Freedom, Security and Justice* (Springer, 2012)

3.1.4.1 A Broad Notion of Security

Numerous texts providing for the processing of personal data for security-related purposes and relevant for the question of balancing have been adopted or are currently discussed. They translate a broad notion of security addressing a broad spectrum of issues[230], including border controls, asylum, immigration, the prevention and repression of crime and the police and judicial cooperation between Member States authorities. Transfers of information between Member States authorities in charge of borders control have considerably been developed, notably in the framework of the CIS (Custom Information System)[231], the VIS (Visa Information System)[232], the SIS I and II (Schengen Information System I and II)[233] and Eurodac[234]. Reinforcement of the exchange of information between police forces and criminal jurisdictions has also been developed in particular in the framework of Europol[235], Eurojust[236], and wholly articulated under the principle of availability.[237] Moreover, transatlantic cooperation in the fight against terrorism providing for the exchange of personal data such as the Swift[238]

[230] On the multifaceted character of the notion of "security and EU law", whether in primary or secondary law and both with regards to its external/internal/national occurrences, see Gloria Gonzalès Fuster et al., "Legal approaches to security, privacy and personal data protection", PRISMS Deliverable 5.1., 3 February 2013

[231] The CIS system has been instituted by the Convention established on the basis of former article K3 of the Treaty on the European Union, on the use of information technology for customs purposes of 26 July 1995, *OJEC* C 317, 27/11/1995

[232] The Visa Information System (VIS) at the EU level has been instituted in two stages: Council decision 2004/512/EC of 8 June 2004 establishing the Visa Information System, *OJEU* L 213, 15/06/2004 and Regulation 767/2008 of the European Parliament and of the Council of 9 July 2008 concerning the VIS and the exchange of data between Member States on short-stay visas, *OJEU* L 218, 13/08/2008

[233] The Schengen Information System has been replaced by the second generation SIS, said SIS II. The purpose of SIS II is to ensure a high level of security in the so-called JLS area. It is implemented through two main instruments: i) The Regulation 1987/2006 of the European Parliament and of the Council of 20 December 2006 on the establishment, operation and use of the second generation SIS (SIS II), *OJEU* L 381, 28/12/2006. This instrument, based on the former first pillar of the EU, relates to alert procedures concerning individuals. In this framework, SIS II contains all those categories of data supplied by each Member States as required for the alerts issued for the purposes of refusing entry or stay; ii) The Council Decision 2007/533/JHA of 12 June 2007 on SIS II, *OJEU* L 205, 07/08/2007. This decision constitutes the former third pillar instrument, relating to alert procedures in the framework of police and judicial cooperation in criminal matters, in particular: alerts concerning serious crimes or threats to public security, persons wanted for surrender or extradition, missing persons, persons wanted for judicial proceedings, but also alerts for objects.

[234] Council Regulation 2725/2000 of 11 December 2000 concerning the establishment of "Eurodac" for the comparison of fingerprints for the effective application of the Dublin Convention, *OJEU* L 316, 15/12/2000

[235] Council Act of 26 July 1995 drawing up the Convention on the establishment of a European Police Office, *OJCE* L 316 of 27 November 1995

[236] Council Decision of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime, *OJEU* L 63 of 6 March 2002

[237] Defined in The Hague Program of the Council of 2005, the principle of availability was first introduced in the Prüm Treaty on the initiative of 6 Member States which main purpose was to improve the exchange of information by giving reciprocal access to national databases containing DNA, fingerprints and vehicle registration data. The main provisions of the treaty have substantially been transposed into Council Decision 2008/615/JHA of 23 June 2008, on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime, *OJEU* L 210, 06/08/2008. Another application of this principle can be found in the Council Framework Decision 2006/960/JHA of 18 December 2006 on simplifying the exchange of information and intelligence between law enforcement authorities of the Member States of the European Union, *OJEU* L 386, 29/12/2006.

[238] Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging Data from the European Union to the United States for purposes of the Terrorist Finance Tracking Program, *OJEU* L8, 13/01/2010

(financial information) and PNR[239] (Passenger Name Records) Agreements, but also bilateral agreements between the US and Member States[240] are part of the privacy v. security landscape. Member States or European Commission's initiatives goes in the direction of an increasing interoperability of existing databases originally established for different purposes and increasing regulation of vast governmental access to private data.

3.1.4.2 Enlargement of Access to European Databases: Towards More Interoperability

The European Council has called for an increasing interoperability of databases created under the Area of Freedom, Security and Justice, leading to some controversial proposals and decisions providing for the connection of systems created originally for different purposes.[241] The concept of interoperability has first been defined by the European Commission as the "*ability of IT systems and of the business processes they support to exchange data and to enable the sharing of information and knowledge*"[242]. According to a very restrictive vision of the Commission, "*interoperability is a technical rather than a legal or political concept*". The European Data Protection Supervisor (EDPS) expressed strong concerns with respect to this emerging political concept: "*Interoperability is mentioned not only in relation to the common use of large scale IT systems, but also with regard to possibilities of accessing or exchanging data, or even of merging databases […] this Communication intends to propose new objectives for large scale IT systems which go beyond their original purpose and will therefore automatically require a new and complete analysis of their impact on the protection of personal data.*[243]" The Commission's definition is narrow, since it reduces the concept of interoperability to the issue of interconnecting IT-systems, leaving apart the political, legal, but also economic, social, cultural or semantic dimensions of this concept[244]. Interoperability between European databases is currently under progress. A Council decision has been adopted, providing the access by Europol and national competent authorities to the European Visa Information System (VIS)[245]. Although the VIS has originally been developed in view of the application of the European visa policy and not as a law enforcement tool, such access is provided for the purposes "*of the prevention, detection and investigation of terrorist offences and of other*

[239] The last in date: Agreement between the United States of America and the European Union on the use and transfer of passenger name records to the United States Department of Homeland Security, *OJEU* L215, 11/08/2012

[240] In particular the signature by 21 Member States with the United States of Agreements "On Enhancing Cooperation in Preventing and Combating Serious Crime" establishing the principle of availability of fingerprinting data and DNA data on a reciprocal basis between the signatory Parties.

[241] On the erosion of the purpose limitation principle, see Frank Dumortier, Claire Gayrel, Joëlle Jouret, Damien Moreau and Yves Poullet, « La protection des données dans l'Espace européen de Liberté, de Sécurité et de Justice », *Journal de Droit Européen* 166 (2010) : 33-46

[242] Communication of the Commission to the Council and the European Parliament on improved effectiveness, enhanced interoperability and synergies among European databases in the area of justice and home affairs, 24 November 2005, COM(2005)0597 final, non published in the OJ

[243] Comments of the EDPS on the communication of the Commission on interoperability of European databases, Brussels, 10 March 2006

[244] Paul De Hert and Serge Gutwirth, "Interoperability of police databases within the EU: an accountable political choice?", *TILT Law & Technology Working Paper series* (2006) available at http://ssrn.com/abstract=971855

[245] Council decision 2008/633/JHA of 23 June 2008 concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences, *OJEU* L 218, 13/08/2008

serious criminal offences". The European Parliament however refused to provide an automatic access to Europol and Eurojust to the Custom Information system (CIS).[246] The proposal for a decision allowing access by national competent authorities to Eurodac, the European central database containing the fingerprints of asylum seekers and illegal immigrants, for law enforcement purposes has also been abandoned for the moment. Full interoperability is highly questionable, since it contributes to simply deny the fundamental purpose limitation principle of data protection. Nevertheless, enlargement of access to various European databases by various authorities for increasingly various purposes is presently the trend.[247]

3.1.4.3 The Increasing Recourse to Commercial Data for Law Enforcement Purposes

Another major threat challenging the privacy v. security balance, relates to the increasing recourse to personal data held by the private sector, originally collected for commercial purposes. In 2004, the EU already adopted an instrument providing the obligation for air carriers to transmit API data (Advanced passenger information) to Member States public authorities on their request[248]. Destined to improve border controls and to combat illegal immigration[249], the use of API data was based on the objective to fight against terrorism[250]. The EU, willing to go a step further in this matter, introduced a first proposal in 2007[251] and a second proposal for a Directive on the transmission and exchange of PNR data for all international flights[252]. The Data Retention Directive of 2006[253] constitutes another example of the increasing recourse to commercial data for law enforcement purposes. It provides the obligation on electronic communications providers and networks to retain traffic and location data for a term between 6 to 24 months to be determined in each Member State. This information is made available to national competent authorities for the purpose of investigation and prosecution of serious crimes. All these proposals and instruments generate considerable debate among legal scholars and NGOs for the strong concerns they raised in relation to the right to privacy.

[246] Article 11 and 12 of the initiative of the French Republic with a view to adopting a Council decision concerning the Convention on the use of information technology for customs purposes (CIS), proposal of the 20th January 2009, Procedure CNS/2009/0803

[247] Franzisca Boehm, *op.cit.,* Chapter C "Cooperation and Data Exchange of the AFSJ Actors and Their compliance with European Data Protection Standard", pp. 321-366

[248] Directive 2004/82/EC of the European Parliament and of the Council of 29 April 2004 on the obligation of carriers to communicate passenger data, *OJEU* L 261, 06/08/2004

[249] Article 1 of the Directive 2004/82/EC

[250] See recital 2 of the Directive 2004/82/EC making reference to the European Council declaration on combating terrorism of 25 and 26 of March 2004

[251] Proposal for a Council Framework decision on the use of PNR for law enforcement purposes of 6 November 2007, COM(2007)664 final, Procedure CNS/2007/0237 (withdrawn)

[252] Proposal for Directive of the European Parliament and of the Council on the use of Passenger Name Records for the prevention, detection, investigation and prosecution of terrorist offences, COM(2011)32 final, 2.2.2011, Procedure 2011/0023/COD

[253] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks, *OJEU* L 105 of 13 April 2006

3.1.4.4 The Evacuation of the Privacy Debate Behind Data Protection Safeguards

Another major trends in EU instruments/proposals relevant regarding the privacy v. security balance is the progressive deletion of fundamental rights debate behind the discussion surrounding data protection safeguards. Such deletion can also be compared with the deletion of privacy in EU data protection legislative proposals discussed earlier. EU legislative proposals are often accompanied by poor and limited discussion and debate of the fundamental rights and liberties are stake by the envisaged security-related measure. This is particularly striking in the Impact assessment carried out by the European Commission and accompanying legislative proposals.[254] Till now, the impact assessment carried out by the European Commission for legislative actions such as the establishment of a PNR system, or the Directive on the retention of traffic data, shows a restrictive analysis of the fundamental rights challenges. The proportionality analysis is extremely poor. In the case of the Data retention Directive, no serious data have been produced concerning the various options capable of showing that there were no less intrusive means, and the IA analysis in this respect can be reduced to a formal statement that the proposal is proportionate. In general, these IAs only provides a general statement recognizing the privacy interference of the measure and immediately turn to more extensive discussion regarding the data protection safeguards. The balance between privacy and security generally shifts to a balance between data protection and security.[255] But in view of the differences in scope of both rights, any interference by a processing of personal data into privacy should also be addressed in relation to the proportionality test of Article 8§2 of the ECHR.

3.1.5 Balancing Privacy and Data Protection v. Surveillance: in Search of Methods and Tools

The search for a fair balance between privacy and other competing interests, in particular security-related interests raise question as to how achieving this correct balance. Various initiatives, at various levels translate a search for tools and methods for balancing privacy and other competing interests.

At European Union legislative level, it is worth mentioning the development of specific lawmaking tools destined to help the decision-making process, although not specifically focused on the privacy v. security balance. For example, the concern for addressing specific attention to fundamental rights issues in any legislative action has recently been established through a specific strategy for the effective implementation of the Charter[256] and Specific operational guidelines on taking account of fundamental rights in impact assessments.[257] The legal validity of legislative proposals should be examined not only formally, but substantially, by

[254] Claire Gayrel and Yves Poullet, "Methodology Balancing Privacy v. Security, the Increasing Role of Impact Assessment in the EU. Benefits and Risks", in *Circulation Internationale de l'Information et Sécurité*, ed. Karim Benyekhlef et Esther Mitjans (Montréal: Thémis, 2013): 177

[255] This is also the view expressed by Gloria Gonzàles Fuster during its presentation at PRISMS Workshop, Brussels, 13 May 2013.

[256] Communication from the Commission "*Strategy for the effective implementation of the Charter of Fundamental Rights by the European Union*" of 19 October 2010, COM(2010)573/4

[257] Commission Staff Working Paper on "*Operational Guidance on taking account of Fundamental Rights in Commission Impact Assessments*" of 6 May 20011, SEC(2011)567 final

answering to a "fundamental rights checklist": "*1. What fundamental rights are affected? ; 2. Are the rights in question absolute rights (which may not be subject to limitations […]; 3. What is the impact of the various policy options under consideration on fundamental rights […]?; 4. Do the options have both a beneficial and negative impact, depending on the fundamental rights concerned […]?; 5. Would any limitation of fundamental rights be formulated in a clear and predictable manner?; 6. Would any limitation : a) be necessary to achieve an objective of general interest or to protect the rights and freedoms of others? Be proportionate to the desired aim? Preserve the essence of the fundamental rights concerned?".*[258] A lot of improvement is expected in this matter from the European legislator. These tools are destined to help the decision-making process.

On the other side of the Atlantic, It is worth mentioning the initiative of the Office of the privacy Commissioner of Canada of a reference document proposing a guide for a "trust inspiring balancing of privacy and security".[259] From "Making the case" to "setting the stage", "running the program" and "calibrating the system", this document intends to provide a guiding tool to public security and national safety stakeholders when they are envisaging the implementation of surveillance measures.[260]

At the level of operators implementing surveillance measures interfering with the right to privacy of individuals, the elaboration of privacy impact assessment, as a tool to identify, assess and mitigate privacy risks, constitute an important development.[261] Important discussion remains regarding the nature and scope of a privacy impact assessment evaluating personal data processing technologies.[262] The Draft Regulation on data protection proposes to establish the obligation to carryout "data protection impact assessment" for processing presenting specific risks[263]. Those processing said to present specific risks are those implying: "*(a) a systematic and extensive evaluation of personal aspects relating to a natural person or for analysing or predicting in particular the natural person's economic situation, location, health, personal preferences, reliability or behaviour, which is based on automated processing and on which measures are based that produce legal effects concerning the individual or significantly affect the individual; (b) information on sex life, health, race and ethnic origin or for the provision of health care, epidemiological researches, or surveys of mental or infectious diseases, where the data are processed for taking measures or decisions regarding specific individuals on a large scale; (c) monitoring publicly accessible areas, especially when using optic-electronic devices (video surveillance) on a large scale; (d) personal data in large scale filing systems on children, genetic data or biometric data*."

[258] *Ibidem*, p.5

[259] Office of the Privacy Commissioner of Canada, "A matter of Trust: Integrating Privacy and Public Safety in the 21st Century. A reference Document From the Office of the Privacy Commissioner of Canada", November 2010, online at http://www.priv.gc.ca/information/pub/gd_sec_201011_e.asp

[260] Chantal Bernier, « Intégrer le droit à la vie privée aux mesures de sécurité publique du 21ème siècle :une expérience canadienne », in *Circulation Internationale de l'Information et Sécurité*, *op. cit.*, pp. 141-152

[261] For a review of existing Privacy Impact Assessments, see the PIAF Research Project http://www.piafproject.eu/Index.html, in particular David Wright et al., A Privacy Impact Assessment Framework for data protection and privacy rights, Deliverable D1 (2011)

[262] Ed. David Wright and Paul De Hert, *Privacy Impact Assessment* (Springer, 2012)

[263] Article 33 of the Draft Regulation

The integration of privacy requirements at early stage of the development of new processing technologies, called "privacy by design"[264], may also become an obligation of the controller under the future European data protection regulation. It is provided that the controller "*shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject."*[265] Additionally, the Draft Regulation introduces the principle of privacy by default according to which "*the controller shall implement mechanisms for ensuring that, by default, only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected or retained beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage. In particular, those mechanisms shall ensure that by default personal data are not made accessible to an indefinite number of individuals*." Privacy by default aims at the effective enforcement of the principle of minimisation.[266]These principles are discussed further in relation to "Accountability".

3.1.6 Relevance for the PARIS Project

This brief overview of the issue of the balance between privacy and security at EU legislative level is particularly instructive for the context of the PARIS project. Although the PARIS project aims at addressing the privacy v. surveillance at the level of operators of surveillance system, it is important to recall that the question of proportionality is central for this task and that the aim to develop a methodology, a way to achieve a correct balance is actually a concern shared at various levels, legislative and operational, and a challenge for the European Union and its Member States. In view of this legal context, it seems to us that the SALT framework, as far as legal aspects are concerned, should focus on two major challenges: the integration of both privacy and data protection requirements in order to adopt a human rights perspective and not only a technical/data protection approach, and a way to operationalize the proportionality requirement at all stages. Section 3 of the present chapter will explain the content of this proportionality requirement.

3.2 Sources of Protection of Privacy and Personal Data

The protection of privacy and personal data is enshrined in Europe in several instruments, both at Council of Europe (1), European Union (2) and national levels (3), referring to both legal binding and non-binding instruments. It is necessary to recall that the PARIS project is carried out while a revision of the legal instruments of personal data protection are presently under study, both at Council of Europe and European Union levels (4).

3.2.1 Council of Europe

All EU Member States are Member States of the Council of Europe, set up in 1949 in the aftermath of the second world war, and which original objective and function is to promote

[264] This concept is generally attributed to Ann Cavoukian, Ontario's Privacy and Information Commissioner

[265] Article 23§1 of the Draft Regulation

[266] Article 5 c) of the Draft Regulation

fundamental rights, democracy and the Rule of law in Europe. In contrast with the EU, which explicitly referred to fundamental rights only in 1997 at the time of adoption of the Amsterdam Treaty, the Council of Europe has been the leading European organization in this field. As far as the protection of privacy and personal data are concerned, one must first recall the fundamental role of the European Convention for the protection of Human Rights and Fundamental Freedoms of 1950[267]. This Convention is of great influence in Europe, since all the signatory parties are under the obligation to enforce the Convention and the case law emerging from the disputes settled by the instituted European Court of Human Rights of Strasbourg (further referred to as ECHR), in charge of the interpretation of the Convention. Article 8 of the ECHR is specifically dedicated to the protection of private life, family life, home and correspondence and is of particular interest for the purposes of understanding the scope of 'private life' and the limitations to this right.

Besides, it is worth mentioning that all EU Member States are also signatory Parties to the Council of Europe Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data signed in Strasbourg in 1981. It lays down the fundamental principles of data protection that we will generally find in Member States EU legislations. The COE Convention 108 applies to any automated processing (excluding manual processing) of personal data by public or private entities, and among the public entities, does not distinguish the processing of personal data for police or judicial purposes. That is why this instrument is generally considered as the most comprehensive data protection instrument in Europe. We will see that the ECHR has often referred to Convention 108 in its reasoning, although it has not yet fully incorporated a systematic data protection perspective when dealing with surveillance technologies. Convention 108 has further been supplemented by Additional Protocol 181 regarding supervisory authorities and transborder data flows laying down specific rules on these issues that were lacking in the original convention.

Although non-binding, the recommendations adopted by the Committee of Ministers of the Council of Europe are very relevant sources in relation to privacy and data protection matters. Among more than 20 Recommendations are related to data protection, and for the purposes of the present report, it is worth mentioning the R87(15) regulating the use of personal data in the Police sector, and R(2010)13 on the protection of individuals with regard to automatic processing of personal data in the context of profiling.

3.2.2 European Union

3.2.2.1 Data Protection: an Autonomous Fundamental Right Closely Connected to the Right to Private Life

In the EU, the protection of private life and data protection is enshrined in the Charter of Fundamental Rights. Its Article 7 provides the right to private and family life, home and communications, while Article 8 innovates through the explicit recognition of the fundamental right to data protection.[268] Both rights are therefore protected under an equal value. In this

[267] European Convention for the protection of Human Rights and Fundamental Freedoms, signed in Rome in 1950

[268] Article 8 of the Charter of Fundamental Rights of the EU :

1. Everyone has the right to the protection of personal data concerning him or her.

sense, if the European Court of Justice has been led to recognize the fundamental right to data protection enshrined in article 8 of the EU Charter[269], it has also recalled that "*that fundamental right is closely connected with the right to respect of private life expressed in Article 7 of the Charter*."[270] As argued earlier, we believe that the autonomy of the right to the protection of personal data does not imply denying privacy as its fundament.

3.2.2.2 Data Protection in EU Law: a Fragmented Approach Inherited from the Pillars Structures of the EU

The regulation of the processing of personal data at EU level comprises several instruments. In contrast with the Convention 108 of the Council of Europe which has adopted a rather comprehensive approach, the EU legal landscape for the protection of personal data is characterized by a fragmented approach widely inherited from the former pillar structure of the EU.

The first and fundamental instrument regulating the processing of personal data in the EU is the Directive 95/46 of 25 October 1995.[271] The Directive aimed at the approximation of Member States legislations in the field of data protection in view of the subsequent liberalization of flows of personal data within the internal market. The Directive was therefore adopted on the basis of the former Treaty of the European Community (TEC, former first pillar).[272] Because of the limitations of competences of the European Community in the matters of police and judicial cooperation, the Directive 95/46 explicitly excludes from its scope of application those matters.[273] The EU further adopted a specific instrument destined to apply to the processing of personal data in the field of police and judicial cooperation in criminal matters on the basis of the former Treaty of the EU (TEU – former third pillar). The scope of Framework decision 2008/977/JHA[274] is however limited to the protection of personal data which "*have been transmitted or made available between Member States*"[275] and does not regulate the processing of personal data by police and judicial authorities at national level. In any case, neither the Directive 95/46 nor the framework decision 977/2008 applies to the processing of personal data necessary for '*national security purposes'*, which remains within the sovereign competence and responsibility of Member States. Besides, the protection of privacy in relation to electronic communications has been the object of a specific legislation, the so-called e-

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

3. Compliance with these rules shall be subject to control by an independent authority.

[269] E.C.J., 9 November 2011, *Volker und Markus Schecke GbR and Harmut Eifert v. Land Hessen*, joint cases C-92/09 and C-93/09

[270] *Ibidem*, §47 and E.C.J., 24 November 2011, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECEMD) v. Administración, del Estado*, joint cases C-468/10 et C-469-10, §41

[271] Directive 95/46, *op. cit.,* further referred to as 'Directive 95/46'

[272] In particular on the basis of former Article 95 of the Treaty of the European Community (TEC), current Article 114 of the Treaty on the Functioning of the European Union (TFEU)

[273] The scope of Directive 95/46 is discussed with mor details further, in part III of the present chapter

[274] Framework Decision 2008/977/JHA, *op. cit.*

[275] Article 1§2 of Framework Decision 2008/977/JHA

privacy Directive 2002/58.[276] Finally, the processing of personal data by EU institutions and EU agencies is regulated under Regulation 45/2001.[277]

Except in relation to electronic communications, European Union law in the field of data protection does not specifically address one or another processing technology. Guidance regarding the interpretation of the concepts and principles enshrined in this instrument is an essential challenge. The National Data Protection authorities, gathered at EU level within the Article 29 Working Party plays a key role in this respect, providing opinions and recommendations on general and specific aspects of the law, constituting very valuable sources of interpretation of the Directive 95/46 and Directive 2202/58.[278] This chapter extensively relies on these sources of interpretation of the data protection concepts and principles.

3.2.3 National Law

As explained above, since the EU does not have an exclusive competence for the regulation of protection of personal data (even under the Lisbon Treaty)[279], national legislations remain the primary source of legislation in the field of data protection. Member States are bound by both the ECHR and EU law and are therefore responsible for their proper and correct implementation. Also, Member States are not subject to the separation of competence between former first pillar ad third pillar matters, which implies that most Member States' legislations generally include police, judicial and even intelligence activities within the framework of their general data protection law (with adaptations). The national caselaw and the opinions and recommendations of the national Data Protection Authorities should also be taken into account. Moreover, to the exception of the e-privacy Directive, there is no specific/sectoral legislation at EU level governing the use of specific surveillance technologies. However, as we will see in the case of videosurveillance, there may be sectoral national legislations that requires to be taken into account. This is why the last two sections of the present chapter will provide a brief overview of the French and Belgian framework for videosurveillance and biometrics (PARIS use cases).

3.2.4 Data Protection Under Revision

Data protection is under revision, both at Council of Europe and European Union levels. Thirty years after its adoption, the Council of Europe launched in 2011 a public consultation in order to assess the necessity and desirability to revise the Convention 108 in the light of new technological challenges.[280] The European Commission is also at the initiative of recent proposals destined to revise current instrument, in view of promoting a "*comprehensive*

[276] Directive 2002/58/EC*, op. cit.*

[277] Regulation 45/2001, *op. cit.*

[278] This consultative body has been created by Article 29 of the Directive 95/46

[279] Under the Lisbon Treaty, the regulation of the protection of personal data is a shared competence between the EU and Member States

[280] See all the documents in relation to the 'Modernisation of Convention 108' at : http://www.coe.int/t/dghl/standardsetting/dataprotection/modernisation_en.asp

approach on personal data protection in the European Union."[281] A proposal of Regulation and a proposal of Directive have been made in view to replace the Directive 95/46 and the Framework decision 2008/977/JHA. We discussed earlier the deletion of privacy behind personal data in the current proposals and the proposals for the introduction of the principles of '*data protection by design'*, '*data protection by default'* and '*data protection impact assessment'* will be discussed later in relation to accountability. The present draft proposals are still awaiting the first reading of the European Parliament. About 4000 amendments should be examined in relation to the Draft Regulation, the legislative process of which is under great pressure of multiple lobbyings activities. While the Draft Regulation was planned to be adopted during the year 2014, it seems that an adoption should not occur before 2015. In view of the uncertainty regarding the outcome of the legislative process, in particular with respect to the Draft Regulation, the present chapter will first and foremost rely on the existing applicable requirements (namely the Directive 95/46).

3.3 The Right to Privacy and Data Protection in ECHR Caselaw

Article 8

"*1. Everyone has the right to respect for his private and family life, his home and his correspondence.*

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

It is immediately obvious that Article 8 is divided into two parts. The first part, Article 8§1, sets out the precise rights which are to be guaranteed to an individual by the State – the right to respect for private life, family life, home and correspondence. The second part, Article 8 §2, makes it clear that those rights are not absolute in that it may be acceptable for public authorities to interfere with the Article 8 rights in certain circumstances.[282] Article 8§2 also indicates the circumstances in which public authorities can validly interfere with the rights set out in Article 8§1; only interferences which are in accordance with the law and necessary in a democratic society in pursuit of one or more of the legitimate aims listed in Article 8§2 will be considered to be an acceptable limitation by the State of an individual's Article 8 rights. Furthermore, the Court has held that, while the essential object of Article 8 is to protect the individual against arbitrary action by public authorities, there may in addition be positive obligations where the State may have to act affirmatively to respect the wide range of personal interests set out in this provision[283]. It means that interferences by private actors may nevertheless be imputable to the States as long as they can be considered to have failed to take measures to secure respect for private life of individuals.

[281] Communication from the European Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions COM(2010)609 final, "A comprehensive approach on personal data protection in the European Union", 4/11/2010

[282] Articles 9, 10 and 11 are similarly subject to legitimate limitations

[283] ECHR, *X. & Y. v. The Netherlands*, 26 March 1985

ECHR caselaw in relation to article 8 of the Convention is extensive and it is not the purpose of the present report to provide an exhaustive view in this respect.[284] We will therefore focus our attention on some important developments of the ECHR caselaw that are of particular interest for the definition of a SAlegalT framework in relation to surveillance technologies. We will start by recalling the scope of protection afforded by Article 8 under the notion of private life (leaving aside the scope of protection afforded by Art. 8 under the notions of family life, home and correspondence) with a specific attention to the integration of data protection aspects under Art. 8 caselaw and the elements taken into account for the interference assessment. We will then examine the conditions for legitimate interferences into private life under Art. 8§2, namely the legality, legitimacy and necessity requirements.

3.3.1 The Right to Respect for Private Life: Scope of Protection

Originally, the right to privacy was conceptualized in a negative way. It referred to the "*right to be let alone*", implying that the State and the public authorities should prevent themselves from any interference in the sphere of the private life of the individuals. But as the Court of Strasbourg enjoys recalling, the Convention is an "*alive instrument*"[285]. On this ground the Court expressly stated that "*the notion of 'private life' is a broad one, which is not susceptible to exhaustive definition*"[286]. The Court has filled the notion of private life gradually.

An overview of the notion of private life (although not exhaustive) was given by the Court in the *Pretty* case, where it held as follows: *" It covers the physical and psychological integrity of a person […] it can sometimes embrace aspects of an individual's physical and social identity […] elements such as, for example, gender identification, name and sexual orientation and sexual life fall within the sphere protected by article 8 […] Article 8 also protects a right to personal development, and the right to establish and develop relationships with other human beings and the outside world [see* Niemietz*] Though no previous case law has established any right to self-determination as being contained in article 8 of the Convention as such, the Court considers that the notion of personal autonomy is an important principle underlying the interpretation of its guarantees.* [287]*"* The Court has then officially recognized the right to self-determination in the *Evans* case of 2006[288].

3.3.1.1 The Protection of Personal Data in Article 8 ECHR Caselaw

On several occasions, the Court has brought several data protection aspects within the scope of Article 8 of the Convention. The Court notably ruled that the storing by a public authority of

[284] On this issue, see for instance Frédéric Sudre (under the dir.), *Le droit au respect de la vie privée au sens de la Convention européenne des droits de l'homme* (Bruxelles: Bruylant, 2005)

[285] The Court in ECHR, *Tyrer v. The United-Kindgom*, 25 April 1978, has first employed the expression in §31. It is now a well-established case law of the Court. See for instance ECHR, *Marckx v. Belgium*, 13 June 1979, §58 and ECHR, *Soering v.The United-Kingdom*, 7 July 1989, et cetera…

[286] ECHR, *Costello-Roberts v. The United Kingdom*, 25 March 1993, §36 on the basis of ECHR, *Niemietz v. Germany*, 16 December 1992, § 29: "*The Court does not consider it possible or necessary to attempt an exhaustive definition of the notion of "private life*."

[287] ECHR, *Pretty v. The United-Kingdom*, 29 April 2002

[288] ECHR, *Evans v. The United Kingdom*, 7 March 2006

information relating to an individual's private life amounts to an interference within the meaning of Article 8.[289] The subsequent use of the stored information has no bearing on that finding.[290] Not only private information, but also public information can also benefit from the protection of Article 8 "*where it is systematically collected and stored in files held by public authorities*."[291] The refusal to give a data subject access to the personal data held by public authorities falls within Article 8 allowing the data subject to bring a claim for access under this article.[292]

Nevertheless, it cannot be considered that the ECHR has brought a general recognition of data protection rights under Article 8 of the ECHR.[293] Indeed the Court asserts that "*in determining whether the personal information retained by the authorities involves any of the private-life aspects mentioned above, the Court will have due regard to the specific context in which the information at issue has been recorded and retained, the nature of the records, the way in which these records are used and processed and the results that may be obtained*."[294] It is precisely in cases involving 'public surveillance systems' that the Court has been led to carry out such evaluation. These cases are indeed highly relevant for the purposes of the present report in several aspects since the outcome of the evaluation of the ECHR contribute to question and/or illustrate the traditional public/private borders.

3.3.1.2 Protection of Article 8 Beyond the "Private Sphere"

The first important ruling in this respect is the *Niemietz* case where the Court ruled that "*it would be too restrictive to limit the notion [of private life] to an 'inner circle' in which the individual may live his own personal life as he chooses and to exclude therefrom entirely the outside world not encompassed within that circle. Respect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings*." This has led the Court to expand the protection of Article 8 to professional activities: "*[t]here appears, furthermore, to be no reason of principle why this understanding of the notion of 'private life' should be taken to exclude activities of a professional or business nature since it is, after all, in the course of their working lives that the majority of people have a significant, if not the greatest, opportunity of developing relationships with the outside world*." On this basis, the Court further recognized that there is a "*a zone of interaction of a person with others, even in a public context, which may fall within the scope of "private life*"."[295] As explained above, the Court takes into account the specific context in which data are gathered and used in order to determine whether monitoring of individuals outside a person's home or private premises (in other words in public spaces) may nevertheless be considered to interfere with individual's private life. ECHR caselaw shows that the Court has taken into account several elements, giving weight to one or more of these elements according to the specific circumstances of the case. These elements are not cumulative conditions, but enlighten factors helping the Court in its

[289] ECHR, *Leander v. Sweden,* 26 March 1987, §48

[290] ECHR, *Amann v. Switzerland*, 16 February 2000

[291] ECHR, *Rotaru v. Romania,* 4 May 2000

[292] ECHR, *Gaskin v. United Kingdom,* 7 July 1989

[293] Paul De Hert, "Balancing security and liberty within the European human rights framework…", *op. cit.*

[294] ECHR, *S. and Marper v. United Kingdom*, 4 December 2008, § 69

[295] ECHR, *P.G. and J.H. v. United Kingdom*, 25 September 2001, §56

evaluation as to whether certain surveillance measures, although occurring in public spaces or public context, may constitute interference into one's private life.

3.3.1.3 Elements Taken Into Account for the Interference Assessment

Whether the individual has or not a reasonable expectation of privacy

The U.S. Supreme Court has originally introduced this criterion in 1964 in a case involving the right to privacy of individuals under the Fourth Amendment.[296] Although not explicitly foreseen in the European Convention of Human Rights, the Court introduced the criterion of "reasonable expectation of privacy"[297], but further asserted that it is generally not a conclusive factor: "*Since there are occasions when people knowingly or intentionally involve themselves in activities which are or may be recorded or reported in a public manner, a person's reasonable expectations as to privacy may be a significant, although not necessarily conclusive, factor. A person who walks down the street will, inevitably, be visible to any member of the public who is also present*."[298] If the underlying reasoning seems to imply that there may be spaces where individuals' expectation of privacy may be less important, the Court generally does not give weight from this criterion solely in its evaluation.

Whether there is systematic recording and storage of the data

This is a very important element in the Court's evaluation, notably with respect to 'public information' or behaviour of individuals in public spaces. In *Rotaru*, the Court recognized that files gathered by security services on a particular individual fall within the scope of Article 8, even if the information has not been gathered by any intrusive or covert method. With regard to surveillance by cameras, the Court however considered that the monitoring of the actions of an individual in a public place by the use of photographic equipment which does not record the visual data does not, as such, give rise to an interference with the individual's private life.[299] In the Court's view "*given that nothing is recorded, it is difficult to see how the visual data obtained could be made available to the general public or used for purposes other than to keep a watch on places […] the data available to a person looking at monitors is identical to that which he or she could have obtained by being on the spot in person. Therefore, all that can be observed is essentially public behaviour. The applicants have also failed to demonstrate plausibly that private actions occurring in public could have been monitored in any way*."[300] The Court's approach in this ruling is problematic from a data protection perspective[301], since the definition of "processing" does not distinguish whether data is recorded or not.[302] Whether

[296] U.S. Supreme Court, *Katz v. United States*, 389 US. 347 (1967)

[297] ECHR, *Halford v. United Kingdom*, 25 June 1997

[298] *P.G. and J.H.*, *op.cit.*, §57

[299] ECHR, *Pierre Herbecq and the Association Ligue des droits de l'homme v. Belgium*, 14 January 1998

[300] *Ibidem*

[301] Paul de Hert, "Balancing security and liberty within the European human rights framework...", *op. cit.*

[302] In particular the definition of 'processing' under EU law in Directive 95/46 as "any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction." However, the definition of 'automatic processing" in Convention 108 as "including the following operations if carried out in whole or in part by automated means: storage of data, carrying out of logical and/or arithmetical

there is systematic recording of the data or not remains significant in the Court's assessment. Moreover, the Court has confirmed this approach in the *Perry* case: "*the normal use of security cameras per se whether in the public street or on premises, such as shopping centres or police stations where they serve a legitimate and foreseeable purpose, do not raise issues under Article 8 § 1 of the Convention*."[303]

Whether the data is recorded in view to identify individuals

This is an important, and sometimes decisive, criterion. In *P.G. and J.H. v. The United Kingdom,* the Court had to determine whether the voice samples of suspects recorded with a covert device at the Police station constituted or not an interference into the applicant's privacy. The Government of United Kingdom argued that "*the use of the listening devices in the cells and when the applicants were being charged did not disclose any interference, as these recordings were not made to obtain any private or substantive information. The aural quality of the applicants' voices was not part of private life but was rather a public, external feature. In particular, the recordings made while they were being charged – a formal process of criminal justice, in the presence of at least one police officer – did not concern their private life. The applicants could have had no expectation of privacy in that context*."[304] Making reference to convention 108, The Court rejected this argument, taking into account that since "*a permanent record has nonetheless been made of the person's voice and it is subject to a process of analysis directly relevant to identifying that person in the context of other personal data […] the recording of the applicants' voices when being charged and when in their police cell discloses an interference with their right to respect for private life*."[305] The Court came to the conclusion that the recording of a voice sample constituted an interference into the applicant's right to private life, precisely because it was used in view of identifying these persons. Similarly, in the case of *Perry*, concerning surveillance by cameras of a suspect in police station premises, the Court also gave weight to the purpose of identification of the person to characterize the interference: "*the footage in question in the present case had not been obtained voluntarily or in circumstances where it could be reasonably anticipated that it would be recorded and used for identification purposes*."[306] With respect to the general retention of fingerprinting data, the Court has also stressed their importance as unique element of identification of individuals (see *Infra*). In contrast, in the *Friedl* case regarding the use of photographs by public authorities during public demonstrations and records of these photographs in a police file, the Court considered that there was no interference since the photographs were not taken in view of identifying individuals, but only retained as a record of the demonstration.[307]

Whether the data is disclosed beyond a foreseeable degree

Regarding surveillance by cameras, we have explained above that the Court takes consideration whether the visual data is recorded or not and can therefore be made available to the general public. In another case relating to surveillance cameras in the streets, the Court gave weight to

operations on those data, their alteration, erasure, retrieval or dissemination" does not expressly refer to the sole 'collection' as an automatic processing.

[303] ECHR, *Perry v. United Kingdom*, 17 July 2003, §40, ECHR, *Aydogdu v. Turkey*, 11 January 2011

[304] *P.G. and J.H*., *op.cit*., §54

[305] *Ibidem*, §59-60

[306] ECHR, *Perry v. the United Kingdom*, §42

[307] ECHR, *Friedl v. Austria*, 26 January 1995

the fact that the disclosure to the medias of the footage concerning the applicant's suicide attempt in the street characterized an interference into the applicant's privacy: "*the relevant moment was viewed to an extent which far exceeded any exposure to a passer-by or to security observation […] and to a degree surpassing that which the applicant could possibly have foreseen when he walked in Brentwood on 20 August 1995*."[308]

Whether the information may give rise to 'private life concern' considering possible unknown future uses

This is in relation to biometric data, in particular fingerprinting and DNA data that the Court gave weight to the capabilities and possible future uses of these data to consider that the sole retention of such data disclosed an interference into one's private life.[309]

Referring to its previous ruling *in P.G. and J.H. v. United Kingdom* regarding voice samples, the Court has adopted a broad approach, referring widely to the notions of 'personal data' and 'processing' with respect to the retention of fingerprinting. If this is true that fingerprinting "*constituted neutral, objective and irrefutable material and, unlike photographs, were unintelligible to the untutored eye and without a comparator fingerprint*"[310], the Court nevertheless considers that since fingerprints "*objectively contain unique information about the individual concerned allowing his or her identification with precision in a wide range of circumstances*", there are thus capable of affecting his or her private life and "*retention of this information may in itself give rise, notwithstanding their objective and irrefutable character, to important private life concerns*".[311]

In the same case, the Court had to consider the collection and retention of cellular samples and DNA profiles. With respect to these data the Court has given weight to the possible uses that may give rise, in the future, to privacy concerns: "*bearing in mind the rapid pace of developments in the field of genetics and information technology, the Court cannot discount the possibility that in the future the private life interests bound up with genetic information may be adversely affected in novel ways or in a manner which cannot be anticipated with precision today*."[312] In its analysis, the Court distinguishes cellular samples from DNA profiles. While the retention per se of cellular samples must be regarded as interfering with the right to private life given the nature and the amount of personal information that they contain[313], the retention of DNA profiles (although they contain a more limited amount of personal information) is equally regarded as an interference in view of their capacity to be used beyond neutral identification (e.g. identification of genetic relationships between individuals, which is a very sensitive issue).[314]

[308] ECHR, *Peck v. United Kingdom*, 28 January 2003, §62

[309] ECHR, *S. and Marper v. the United Kingdom*, 4 December 2008

[310] According to the argument of the Government of the United Kingdom, §84

[311] *Ibidem*, §85

[312] *Ibidem*, §71

[313] *Ibidem*, §73

[314] *Ibidem*, §75

Ad hoc approach: the case of GPS surveillance

There are also cases where the Court has developed, in addition to some criteria explained supra, an *ad ho*c approach to specific circumstances. A recent example of such *ad hoc* evaluation of the interference into one's private life can be found in a case involving surveillance of the applicant by GPS (Global Positioning System).[315] The Court has considered that "*GPS surveillance is by its very nature to be distinguished from other methods of visual or acoustical surveillance which are, as a rule, more susceptible of interfering with a person's right to respect for private life, because they disclose more information on a person's conduct, opinions or feelings*."[316] The Court has therefore considered that surveillance by GPS and processing and use of the data obtained thereby may constitute an interference with an individual's private life, according to the specific circumstance, such as: the duration of the surveillance, its objective, the systematic recording or not of the data obtained through GPS surveillance and the use of such data "*in order to draw up a pattern of the applicant's movements, to make further investigations and to collect additional evidence at the places the applicant had travelled to, which was later used at the criminal trial against the applicant*."[317]

In this perspective, the Court does not seem willing to consider that surveillance by GPS, irrespective of the circumstances, amounts to an interference into private life of individuals. It does not give the same weight to GPS surveillance and acoustic surveillance for example, for which the Court has adopted a rather principled approach according to which wiretapping amounts to an interference. Surveillance by GPS will require examination of the specific circumstances to determine whether in a given case, there is interference or not with an individual's privacy.

While article 8 affords protection to one's private life, the Court has become familiar with the notion of "personal data" (understood as any information relating to an identified or identifiable individual) and increasingly willing to make reference to Convention 108 in determining that automatic processing of personal data may disclose interference into one's private life. Nevertheless, in certain significant cases (notably regarding surveillance by cameras), the Court caselaw has not fully incorporated a data protection perspective in its reasoning, remaining attached to the demonstration that certain type of "information" or certain type of "processing" must involve private life concerns to benefit from the protection of Article 8. This contributes to illustrate that privacy does not fully equal data protection. Privacy may be broader than data protection, since privacy concerns may be raised even when there is no processing of personal data. Also, data protection may be applicable although a certain processing may not involve private life issues.

We will now turn to explain the conditions under which "interferences" into one's privacy may be allowed under Article 8§2 of the Convention.

[315] ECHR, *Uzun v. Germany*, 2 September 2010

[316] *Ibidem*, §52

[317] *Ibidem*, §50-51

3.3.2 Legitimate and Proportionate Interferences Into the Right to Private Life by Public Authorities

Once the Court has assessed whether the circumstances of the case involve an interference into the private life of the applicant, the Court comes to assess whether this interference may be justified. The interference must first be "in accordance with the law" (the legal requirement) and "necessary in a democratic society" to achieve one or more of the goals listed in Article 8§2.

3.3.2.1 The Legal Requirement

Interferences into one's private family life, home and correspondence must be in "*accordance with the law".* If the Court finds that the legal requirement is not satisfied in a given case, the measure interfering into the individual's private life will be considered as violating Article 8 and the case will end there. The legal requirement enshrines two conditions: the interference must have a legal basis and must be foreseeable, in particular "*the quality of the law in question must be such that it is accessible to the persons concerned, and formulated with sufficient precision to enable them, if need be with appropriate advice, to foresee, to a degree that is reasonable in the circumstances, the consequences which a given action may entail*."[318]

Certain surveillances practices appear to be particularly vulnerable in this regard, in particular telephone tapping. It is notably in this specific area that the Court has been led to condemn State Parties in a series of cases.[319] Scholars have also noticed that the Court is more willing to exercise a strict standard of review in relation to the legality requirement than to the much more political test of "necessity".[320] Regarding cases evoked in the present chapter, the Court found that interferences by the defendant State were not "in accordance with the law" in the case of *Perry* (covert videosurveillance in a police station) and, *P.G. and J.H. v. UK* (covert recording of voice samples in police station premises. In the case of *Uzun* regarding surveillance by GPS, the Court however considered that the interference was in accordance with the law. It therefore turned to the legitimacy and necessity requirements to determine whether the said interference was admissible or not.

3.3.2.2 The Interference Must Pursue a Legitimate Aim

It falls on the respondent State to identify the objective or objectives of the interference, such as enumerated in Article 8§2: "*national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others*." Actually, the Court's caselaw does not question the argument of State Parties in this regard. It has rarely if ever rejected the legitimate aim or aims identified, even when this may be disputed by the applicant on the ground that the reason given by the State is not the actual reason motivating the interference.

To come back to some of the legitimate aims advanced by States in some of the cases discussed in the present report, the Court agreed that "*the retention of fingerprint and DNA information*

[318] ECHR, *Andersson v. Sweden*, 25 February 1992, §73

[319] See for instance ECHR, *Malone v. United Kingdom*, 2 August 1984, *Kruslin v. France* and *Huvig v. France*, 24 April 1990

[320] Paul De Hert, "Balancing security and liberty within the European human rights framework…", *op.cit.*

pursues the legitimate purpose of the detection, and therefore, prevention of crime"[321] or that the disclosure of the CCTV material to the media contributed to pursue "*the legitimate aim of public safety, the prevention of disorder and crime and the protection of the rights of others*."[322]

3.3.2.3 The Interference Must Be Necessary in a Democratic Society: a Proportionality Policy

First, with respect to the term "necessary", the Court ruled that "*while it is not synonymous with 'indispensable', neither has it the flexibility of such expressions as 'admissible', 'ordinary', 'useful', 'reasonable' or 'desirable'*."[323] The Court further ruled that "*the notion of 'necessity' implies that an interference corresponds to a pressing social need, and in particular that it is proportionate to the legitimate aim pursued*" and "*if the reasons adduced by national authorities to justify it are relevant and sufficient*."[324] Instead of a simple necessity test, the Court applies a proportionality policy, which at its simplest, involve balancing the rights of the individual with the interests of the State.

Content of the proportionality test

The proportionality test or balancing test has raised considerable discussion among scholars. As explained earlier, it originates in German administrative law in the XIX century and has migrated to EU, ECHR and elsewhere to become "*one of the defining feature of global constitutionalism*".[325] 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.[326]

Application of the proportionality test by the ECHR: an ad hoc approach

It is worth mentioning that the approach of the ECHR is generally considered as an *ad hoc* balancing, in that it favours an adjudication of the litigation *in concreto* rather than *in abstrato.*[327]

Most importantly, the Court's caselaw affords a margin of appreciation to Member States to make the initial assessment of proportionality of an interference, the breadth of which varies according to the circumstances, the subject matter and its background. The margin of appreciation left to Member States will vary according to the nature and seriousness of the interests to be protected from interference, the nature of the interference and the pressing

[321] *S. and Marper v. the United Kingdom*, §100

[322] *Peck v. the United Kingdom*, §67

[323] ECHR, *Handyside v. the United Kingdom*, 7 December 1976, §48

[324] ECHR, *Olsson v. Sweden*, 24 March 1988, §67-68

[325] Alec Stone Sweet and Jed Matthews, *op. cit.*

[326] The said definition of the content of the proportionality principle derives from Robert Alexy, *A theory of Constitutional Rights*, trans. Julian Rivers (Oxford: Oxford University Press, 2002) (original publication in German in 1983)

[327] Alec Stone Sweet and Jed Matthews, *op. cit.*

social need served by the interference.[328] Member States may enjoy a broader margin of appreciation in areas showing a variety of customs and practices across Member States or when national security interests are at stake. With respect to secret surveillance, the Court has considered for example that if "*the existence of some legislation granting powers of secret surveillance over the mail, post and telecommunications is, under exceptional conditions, necessary in a democratic society*", "*this does not mean that the Contracting States enjoy an unlimited discretion to subject persons within their jurisdiction to secret surveillance. The Court, being aware of the danger such a law poses of undermining or even destroying democracy on the ground of defending it, affirms that the Contracting States may not, in the name of the struggle against espionage and terrorism, adopt whatever measures they deem appropriate*."[329] Special attention will be paid to the existence of adequate and effective guarantees against abuse and arbitrariness, also in relation to the legal requirement.

The ECHR has not explicitly transposed into its caselaw the threefold requirements (points i), ii) and iii) explained above). The caselaw of the ECHR demonstrates that there is no consistent and systematic application of these three stages of the proportionality test. [330] It may exercise its control over the suitability of the interference and apply the least-restrictive means test or may avoid to exercise such controls. The broader the margin of appreciation of the State is, the less scrupulous the judicial review of the Court over the suitability and the least-restrictive means principles will be. In particular, in relation to Article 8, P. de Hert asserts that "*a lot of mist remains to cloud our understanding of the Court's approach to legitimate limitations of privacy*".[331] The three stages of the proportionality test would be more systematically applied in the context of art. 10 of the Convention, while the varying tests applied (from loose to strict scrutiny) under Article 8 make the Court's caselaw often unpredictable.[332]

We cannot provide a complete review of the ECHR caselaw in relation to the application of the proportionality test under Article 8§2, which would require an entirely dedicated research. Neither this section intends to provide a global overview of ECHR caselaw in relation to new technologies.[333] Instead we will focus here on the reasoning of the Court in some specific cases involving videosurveillance activities and biometrics systems and their outcomes. The two cases presented hereunder have been chosen as far as they constitute illustrations of the complexity, as an *ad hoc* approach, of the proportionality analysis in ECHR caselaw in relation to Article 8.

[328] ECHR, *Z. v. Finland*, 25 February 1997. For an exhaustive analysis of the factors determining the breadth of the margin of appreciation of States see Yutaka Arai-Takahashi, The margin of appreciation doctrine and the principle of proportionality in the jurisprudence of the ECHR (Antwerpen: Intersentia, 2002)

[329] ECHR, *Klass v. Germany*, 6 September 1978, §48-49

[330] Sebastien Van Drooghenbroeck, *op. cit.*, in particular chap. III

[331] Paul De Hert, "A Human Rights Perspective on Privacy and Data Protection Impact Assessments", in *Privacy Impact Assessment,* ed. David Wright and Paul de Hert, (London, Brussels: Springer, 2012), 42.

[332] *Ibidem*

[333] For a global overview of the ECHR caselaw in relation to new technologies in the last decade, see Claire Gayrel and Jean Herveg, "Chronique de Jurisprudence de la Cour européenne des Droits de l'Homme 2002-2008 *, Revue du Droit des Technologies de l'Information* 37 (2009) and Jean Herveg, Chronique de Jurisprudence de la Cour européenne des Droits de l'Homme 2009-2011, , *Revue du Droit des Technologies de l'Information* 48-49 (2012)

Non proportionality of indefinite retention of biometric data of non-convicted persons

In the case of *Marper v. UK*, the particular circumstances of the case submitted to the Court concerned the retention of fingerprint and DNA data of persons who have been suspected, but not convicted, of certain criminal offences. The control of the Court was therefore strictly limited to the issue of whether the retention of biometric data of non-convicted persons was justified or not under Article 8 §2 and did not address whether the retention of such data in general could be regarded as justified or not.

The Court considered that the United Kingdom did not enjoy a broad margin of appreciation with regard to the retention of biometric data such as fingerprints and DNA information taking into account two main factors. First, the Court gave weight to "*the intrinsically private character of this information*", which "*calls for the Court to exercise careful scrutiny of any State measure authorizing its retention and use by the authorities without the consent of person concerned*."[334] Second, the Court proceeded to an overview of the rules established for the retention of fingerprint and DNA information in Council of Europe Member States and noticed that "*England, Wales and Northern Ireland appear to be the only jurisdictions to allow the indefinite retention of fingerprint and DNA material of any person of any age suspected of any recordable offence*". Given the strong consensus existing among the contracting States who have chosen to set limits on the retention and use of such data with a view to achieve a proper balance, the Court judges that it narrows the margin of appreciation of the United Kingdom in the said case.

Although the Court adopts a rather critical view with respect to the suitability of the measure[335], it nevertheless refrains to conclude that the interference at stake would not be suitable: "*While neither the statistics nor the examples provided by the Government in themselves establish the successful identification and prosecution of offenders could not have been achieved without the permanent and indiscriminate retention of the fingerprint and DNA records of all persons in the applicant's position, the Court accepts that the extension of the database has nonetheless contributed to the detection and prevention of crime*."[336] The Court will not proceed to the least-restrictive means test and will turn directly to the final balancing *stricto sensu*.

[334] *Marper v. United Kingdom*, §104

[335] *Ibidem*, §115-116: "*115. Although the power to retain fingerprints, cellular samples and DNA profiles of unconvicted persons has only existed in England and Wales since 2001, the Government argue that their retention has been shown to be indispensable in the fight against crime. Certainly, the statistical and other evidence, which was before the House of Lords and is included in the material supplied by the Government (see paragraph 92 above) appears impressive, indicating that DNA profiles that would have been previously destroyed were linked with crime-scene stains in a high number of cases. 116. The applicants, however, assert that the statistics are misleading, a view supported in the Nuffield Report. It is true, as pointed out by the applicants, that the figures do not reveal the extent to which this "link" with crime scenes resulted in convictions of the persons concerned or the number of convictions that were contingent on the retention of the samples of unconvicted persons. Nor do they demonstrate that the high number of successful matches with crime-scene stains was only made possible through indefinite retention of DNA records of all such persons. At the same time, in the majority of the specific cases quoted by the Government (see paragraph 93 above), the DNA records taken from the suspects produced successful matches only with earlier crime-scene stains retained on the data base. Yet such matches could have been made even in the absence of the present scheme, which permits the indefinite retention of DNA records of all suspected but unconvicted persons*."

[336] *Ibidem*, §117

In this respect the Court considers that the "*blanket and indiscriminate*[337] *nature of the powers of retention of the fingerprints, cellular samples and DNA profiles of persons suspected, but not convicted of offences, fails to strike a fair balance between the competing public and private interests*".[338] The Court also notices the risk of stigmatisation, stemming from the fact that non convicted persons are treated in the same way as convicted person, raising concern with regard to the right to presumption of innocence.[339]

To conclude, Member States do not enjoy a very broad margin of appreciation in the implementation of biometric systems. Even though there are differences among Member States in this respect, the Court is not willing to allow a very wide margin of appreciation, in particular regarding the purposes of collection, retention periods and conditions for disclosure, requiring that they be strictly provided by law (in connection with the legal requirements) and accompanied with adequate safeguards.[340]

Non proportionality of disclosure to medias of camera footage

In the case of *Peck*, the applicant had been filmed in the public space while he was attempting suicide. The police, thanks to the videosurveillance system, intervened promptly. In order to advertise about the benefits of videosurveillance in the prevention of crime, the camera footage (showing the applicant with a knife just before his suicide attempt) was disclosed to local and national medias.

The suitability of videosurveillance and advertising of CCTV system and its benefits for the detection and prevention of crime, as argued by the Government of the United Kingdom, is not disputed by the Court. However, the Court will emphasize its control in the specific circumstances of the case on the least-restrictive means test: "*The Court notes that the Council had other options available to it to allow it to achieve the same objectives. In the first place, it could have identified the applicant through enquiries with the police and thereby obtained his consent prior to disclosure. Alternatively, the Council could have masked the relevant images itself. A further alternative would have been to take the utmost care in ensuring that the media, to which the disclosure was made, masked those images. The Court notes that the Council did not explore the first and second options and considers that the steps taken by the Council in respect of the third were inadequate*."[341] Moreover, the fact that the footage had been publicly disclosed to promote the effectiveness of CCTV system in the detection of crime, whereas the applicant had in fact been not charged of any offence, should have been carefully

[337] The Court notes §119: "*The material may be retained irrespective of the nature or gravity of the offence with which the individual was originally suspected or of the age of the suspected offender; fingerprints and samples may be taken – and retained – from a person of any age, arrested in connection with a recordable offence, which includes minor or non-imprisonable offences. The retention is not time-limited; the material is retained indefinitely whatever the nature or seriousness of the offence of which the person was suspected. Moreover, there exist only limited possibilities for an acquitted individual to have the data removed from the nationwide database or the materials destroyed (see paragraph 35 above); in particular, there is no provision for independent review of the justification for the retention according to defined criteria, including such factors as the seriousness of the offence, previous arrests, the strength of the suspicion against the person and any other special circumstances*."

[338] *Ibidem*, §125

[339] *Ibidem*, §122

[340] See also the analysis of Nancy Yue Liu, *Bio-Privacy, Privacy Regulations and the Challenge of Biometrics* (New York: Routledge, 2012) p. 113

[341] *Peck*, §80

considered.[342] On these grounds the Court concludes that the disclosure of the said footage constituted a disproportionate and unjustified interference.[343]

3.3.3 Conclusions

The purpose of this section was to provide a general overview of the ECHR caselaw in relation to Article 8 of the Convention, in particular as far as it is relevant for the identification of the public/private borders. First, an individual's right to private life exists beyond the private sphere, since the right to privacy actually encompasses a right to self-determination of the individual. Second, legitimate and justified interferences into an individual's private life is submitted to the proportionality test. If Member States enjoy a certain margin of appreciation (varying according to the case), such margin is in no case unlimited. Although not systematically and consistently applied by the ECHR, the proportionality principle (as described in its three-steps analysis: suitability test; Least-restrictive means test; and balancing *stricto sensu*) is highly relevant for the SALT framework, and should be integrated, at all relevant stages of the implementation of a surveillance system. Finally, It is important to understand that privacy does not equal personal data protection. Privacy may be broader than data protection, since privacy concerns may be raised even when there is no processing of personal data. Also, data protection may be applicable although a certain processing may not involve private life issues. This is why data protection rules are presented distinctly from private life considerations in the present chapter.

3.3.4 Relevance and Perspectives for the SALT Framework

As far as the SALT framework should integrate privacy requirements, the elements of the ECHR caselaw in relation to Article 8 are of fundamental importance. At this (early) stage of the research project, we can make two general suggestions regarding the integration of these privacy requirements into the SALT framework.

First, as far as the identification of privacy interests are at stake, we would suggest that the SALT framework establish as a principle that any envisaged surveillance technology involve potential concerns according to Article 8§1. This could be established as a precautionary principle. Indeed, in view of the voluntarily open and broad definition of the notion of private life, it would be very hazardous for the SALT framework to aim at determining whether an intended surveillance technology constitutes or not an interference into one's private life. It appears much wiser and privacy-productive to start from the principle that any surveillance measure involves an interference into private life of individuals, wherever or whenever it occurs.

Second, the SALT framework should instead focus its attention on the way to integrate the elements of the ECHR caselaw in relation to legal and legitimate interferences. We propose to build on the permissible limitation test proposed by P. De Hert, who has identified seven core elements: the technology should be used in accordance with and as provided by the law; the technology or processing should serve a legitimate aim; the technology should not violate the

[342] *Ibidem*, §84
[343] *Ibidem*, §87

core aspects of the privacy rights; the technology should be necessary in a democratic society; the technology should nor have or give unfettered discretion; the technology should be appropriate, least intrusive and proportionate; the technology should be consistent with other human rights.[344]

3.4 General Data Protection Law: Directive 95/46, Core Concepts and Content Principles

This is the basic EU legal instrument regulating the processing of personal data and the free movement of such data within the EU. It enshrines core concepts and principles that are also widely common to other major sources of regulation of data protection, such as the Convention 108[345] or the OECD Guidelines[346]. It applies to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system.[347] Because of the choice of the instrument, a directive, the regulation of data protection leaves Member States a substantial margin of appreciation for the implementation of the Directive into their national law. It is therefore important to keep in mind that the purpose of the Directive was primarily the approximation of national laws in the field of protection of personal data so as to liberalize the flows of personal data between Member States. The Directive did not aim at achieving a full harmonization of Member States laws. For the purposes of the SALT framework, it is therefore essential to understand the importance of EU law legal requirements, but also of Member States legal requirements, which will frame in practice the implementation of any surveillance measure. If the Directive has contributed to a closer approximation of national laws, many divergences of interpretation on several aspects of the law remain.[348] Moreover, besides divergences between Member States, Studies Reports regarding the implementation of the Directive 95/46 has also demonstrated a range of difficulties that arise in relation to the application of Directive 95/46 within the new global and technological environment.[349] This part will not provide an exhaustive analysis of the Directive. It will leave aside the enforcement mechanisms provided in the Directive 95/46 to ensure compliance with the law (establishment of national independent supervisory authorities, provision of sanctions et cet…), the data subject's rights in relation to the processing of personal data pertaining to

[344] Paul De Hert, "A Human Rights Perspective on Privacy and Data Protection Impact Assessment"s, *op. cit.*, p. 33-76

[345] Council of Europe Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data signed in Strasbourg, 1981

[346] OECD Guidelines of 1980 governing the protection of privacy and transborder data flows of personal data

[347] Article 3§1 of Directive 95/46

[348] Douwe Korff, Comparative Study on different approaches to new Privacy Challenges, in particular in the light of technological developments, Working Paper No. 2: Data Protection in the EU: the difficulties in meeting the challenges posed by global social and technical developments, 20 January 2010. This study is based on previous comparative legal analysis carried out by the author (Douwe Korff, Comparative Summary of National laws, University of Essex/European Commission, 2002) and on five Country Reports regarding Denmark, France, Germany, the UK and the Czech Republic all submitted in 2010 and available at: http://ec.europa.eu/justice/data-protection/document/studies/index_en.htm

[349] Douwe Korff, Comparative Study on different approaches to new Privacy Challenges, in particular in the light of technological developments, Working Paper No. 1: The challenges to European data protection laws and principles, 20 January 2010

them (access, rectification, opposition) and many specific issues (territorial scope of application, processing of personal data for historical, statistical or scientific purposes, processing of personal data for literary, journalistic or artistic purposes). This first part of the present chapter rather intends to focus on the core concepts and content principles enshrined in the Directive, without specific attention to one or another technology or context of processing. They constitute a first list of requirements that the SALT framework will have to deal with.

3.4.1 Material Scope of Application

In line with the Convention 108, it does not cover the processing of personal data carried out by a natural person in the course of a purely personal or household activity.[350] Moreover, the Directive does not apply to the processing of personal data "*in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law*."[351] Police and judicial processing of personal data are typically excluded from the scope of application of Directive 95/46, which has led the European Union to adopt a specific instrument in this field, the Framework decision 977/2008. Besides, Directive 95/46 provides for specific regimes regarding processing for journalistic, literary or artistic purposes[352] and processing for historical, statistical or scientific purposes.[353]

Member States have all implemented specific rules regarding processing of personal data while exercising freedom of expression rights and in the field of research and generally provide for the exclusion of personal and household activities in compliance with the Directive. However, the majority of Member States have not necessarily implemented the wide exclusion of security-related processing activities, although the obligations and principles applicable to these processing have been adapted. National laws of data protection are generally inclusive, applying, in principle (with special limitations, exceptions, exemptions) to the matters of police or state security. However, there are fundamentally different approaches between Member States legislations as to which extent security-related surveillance processing fall under the requirements of data protection national laws. States may be more or less flexible with regard to police and security-related processing activities.

For example, the Belgian Privacy Act provides for exemptions to the processing of personal data carried out by intelligence services on one hand, and by police services on the other hand.[354] Intelligences agencies are quasi-excluded from the scope of application of the Act, while the police sector benefit from a much rather restrictive set of exemptions. Police services are only exempted from the obligation of information of the data subject, and from the general regime of data subjects' rights of access, rectification and opposition. In contrast, the UK Data

[350] Article 3§2

[351] *Ibidem*

[352] Article 9 of the Directive 95/46

[353] Articles 6§1 b) and e) and 11§2

[354] Article 3§4 of the Belgian Privacy Act

Protection Act provides for rather broadly-phrased exemptions concerning data used to safeguard national security, and concerning processing for the purpose of the prevention or detection of crime, the apprehension or prosecution of offenders, or the assessment or collection of any tax or duty.[355]

If national laws generally provide exemptions to the police sector and judicial processing, not all security-related related processing are excluded from the scope of application of data protection legislations. This implies that many public authorities, and in particular police forces, may nevertheless be submitted to data protection law.

3.4.2 Main Notions

The material scope of application of the principles enshrined in the Directive 95/46 also follows from the definition and understanding of the essential notions of 'personal data' and 'processing'. The notions of 'controller' and 'processor' also require a short examination in order to understand the allocation of responsibility under the Directive.

3.4.2.1 Notion of Personal Data

Personal data are defined both in Convention 108 and in the Directive 95/46 as "*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*."[356] The definition of this notion is of considerable importance since it determines whether the national legislations of data protection apply or not to certain types of processing.

The uncertainty as to whether certain type of data should be considered as personal data and the divergences of interpretation of the notion between Member States has led the Article 29 Working Party to issue an Opinion.[357] The Opinion analyses the various elements in the definition ("any information", "relating to", "identifiable" and "natural person") providing a very wide interpretation of the notion. This opinion is briefly summarized hereunder.

In relation to the element of "any information", the Article 29 Working Party has expressed that it covers not only objective information (factual records, such as name, date of birth, bank account number et cet…), but also subjective information (opinions, assessments regarding one individual). It includes information on individuals, regardless of the position of those persons (consumer, patient, employee et cet…) in whatever type of activities he undertakes (private, public, recreational, work activities). Finally, it includes information available in whatever form, be it alphabetical, numerical, graphical et cetera.

[355] Sections 28 and 29 of the UK Data Protection Act

[356] Article 2 a) of Directive 95/46

[357] Article 29 Data Protection Working Party, *Opinion 04/2007 on the concept of Personal data*, 20 June 2007, WP136

According to the Article 29 Working Party, "*in order to consider that the data "relate" to an individual, a content element OR a purpose element OR a result element should be present*".[358] A content element is present when the information is "about" one person, such as for instance the results of a medical analysis. The purpose element is present when the data are used or likely to be used, taking into account all the circumstances surrounding the present case, with the purpose to evaluate, treat in a certain way or influence the status or behaviour of the individual. The result element will be present when the use of the data is likely to have an impact on a certain person's rights and interests, taking into account all the circumstances surrounding the precise case.

Regarding the element of "identifiable" individual, the Opinion of the Article 29 Working Party is quite detailed. To summarize, the approach of the Working Party insists on the fact that identification is not only whether one knows the name of the person, but rather whether that person can be distinguished from others of the group, or whether one can link information about this unknown person to information held elsewhere. Crucially, an individual may be identifiable directly or indirectly. As mentioned in recital 26 of the Directive, in order "*to determine whether a person is identifiable account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person*". The criterion of "*all means likely reasonably to be used*" should take into account all the factors at stake: the cost of conducting identification, the intended purpose, the way the processing is structured, the advantage expected by the controller, the interests at stake for the individuals, as well as the risk of organizational dysfunctions and technical failures.

In spite of these clarifications/explanations from the Article 29 Working Party, several issues remain in particular regarding anonymisation and profiling activities. Basically, if it is effectively impossible to identify someone, this person cannot be considered as 'identifiable' and the regime of the protection of personal data should consequently not apply to the data. Such data could be considered as 'anonymised data'. However, it is now pointed out that because highly sophisticated 'data matching software' will be much more readily available, anonymity becomes much harder to achieve. Member States prove to have different approaches in this respect, which much rest on the question of whether the national law or Data protection authority considers the question of 'identifiability' as relative or not. Certain countries only considers pseudonimised data or encoded data as 'personal data' with respect to the person who detain the 'key', and considers that the same data are not 'personal data' in relation to other persons. Other Member States, such as Belgium, will continue to consider that encoded data are 'personal data' with respect to anyone (whether that person has the 'key' or not) and will only consider fully anonymised data (data that cannot be linked anymore to anyone and by anyone) as falling outside the scope of the law.

3.4.2.2 Notion of 'Processing'

For the record, the notion of processing covers "*any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or*

[358] WP136, p. 10

combination, blocking, erasure or destruction."[359] First of all, this definition is said to be technologically neutral, translating the unambiguous will of the Legislator to regulate the processing of personal data through any technological means. Second, the collection of personal data, whether manually or by automatic means is considered as a processing. Third, the list of operations mentioned in the definition is generally not considered as an exhaustive list, implying that the notion of "processing" is susceptible of evolution in the light of new technologies.

3.4.2.3 Notions of 'Controller" and 'Processor'

The Directive defines the 'controller' as '*the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data'*.[360] The identification of the controller is essential as it allows allocating responsibility for the compliance with data protection rules, but also for the determination of which national law is applicable. The Article 29 Working Party made clear that being a controller is primarily the consequence of factual circumstances.[361] Therefore, it is the concrete circumstances as to who actually 'determined' the purposes and means of the processing who will be identified as the 'controller' and therefore responsible for the processing activity. In practice, it is the level of influence on the 'why' (purposes) and 'how' (means) of the processing that will guide the qualification of the controller. Regarding the means of the processing, the Article 29 Working Party considers that there are essential elements of a processing that are inherently reserved to the determination of the controller: which data shall be processed? Which third parties shall have access to the data? When data shall be deleted?[362]

The 'processor' is the "natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller".[363] The identification of the processor plays to identify which national law for security of processing will apply. Indeed, the core responsibility of the processor is ensuring the security of the processing and the personal data.[364]

3.4.3 Principle of Fair and Lawful Processing

This principle is mentioned both in Convention 108 and in Directive 95/46 stating that personal data must be processed "fairly and lawfully". The general requirement of lawfulness imply that any processing must comply with the law, not only with data protection legislation, but also with other relevant legal requirements. The requirement of fairness is a broad standard calling for a general duty of transparency and legitimacy in the processing of personal data. This is

[359] Article 2 b) of Directive 95/46

[360] Article 2 d) of Directive 95/46. The definition specifies that "where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law"

[361] Article 29 Data Protection Working Party, *Opinion 01/2010 on the concepts of 'controller' and 'processor'*, 16 February 2010, WP169, pp. 8-9

[362] *Ibidem*, p. 14

[363] Article 2 e) of Directive 95/46

[364] Article 17 of Directive 95/46

made explicit in the Draft Regulation which provides that personal data must be processed "*lawfully, fairly and in a transparent manner in relation to the data subject*." Processing can, in theory, meet the specific requirements of the Directive (or of national laws), yet still be "unfair" and therefore, not allowed. The requirement of fairness allows a certain margin of appreciation and must be considered for each type of processing.

3.4.4 Purpose Limitation Principle

The Directive 95/46 provides that personal data must be "*collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes*." It is one of the central feature of data protection instruments and the Article 29 Working Party has recently issued an extensive Opinion on the purpose limitation.[365] This Opinion is of interest for the purposes of the SALT framework, since it provides general guidance of interpretation of what is meant by a "specific, explicit and legitimate purpose" and the prohibition for further "incompatible use".

The Article 29 Working Party recalls that the purpose limitation principle contributes to transparency, legal certainty and predictability, preventing the use of personal data in a way that the individuals might find unexpected, inappropriate or otherwise objectionable.

3.4.4.1 The Purpose Must Be Specific

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.[366] 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 Working Party 29 rejects purposes that would be too vague or general, such as "marketing purposes", "IT security purposes" or "research", but also warns about overly legalistic approach which may be counter-productive (e.g. very detailed description of purposes providing extensive disclaimers and therefore unhelpful information to data subjects).

3.4.4.2 The Purpose Must Be Explicit

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.[367] This requirement contributes to transparency and predictability.

[365] Article 29 Data Protection Working Party, *Opinion 03/2013 on purpose limitation*, 2 April 2013, WP203

[366] WP203, p. 13

[367] WP203, p. 17

3.4.4.3 The Purpose Must Be Legitimate

The Working Party 29 makes clear that the requirement of a legitimate purpose is not necessarily satisfied when the processing is based on one of the legitimating grounds for processing listed in article 7 of the Directive 95/46 (see further). The requirement of legitimate processing is broader, implying that the processing must be "in accordance with the law" in the broadest sense.

3.4.4.4 Principle of Prohibition of Further Processing for Incompatible Use

The Article 29 Working Party provides a guidance for assessing the compatibility of any further use. Some key factors (the list is not exhaustive but indicative) to be considered during the compatibility assessment are the following:

- The relationship between the purposes for which the data have been collected and the purposes of further processing: the greater the distance between the purposes of collection and the purposes of further processing, the more problematic is the further use in view of the compatibility assessment.
- The context in which the data have been collected and the reasonable expectations of the data subjects as to their further use: an important aspect is the nature of the relationship between the controller and the data subject, and in view of the nature of this relationship whether the processing falls under generally expected practices in this given context.
- The nature of the data and the impact of the further processing on the data subjects
- The safeguards applied by the controller to ensure fair processing and to prevent any undue impact on the data subjects

3.4.4.5 Exceptions

Where the compatibility assessment would lead to the conclusion that the processing is incompatible, the only grounds on which it can nevertheless be carried out are those provided in article 13 of the Directive 95/46, providing that "*Member States may adopt legislative measures to restrict the scope of obligations and rights provided for in article 6(1) [purpose limitation principle] when such a restriction constitutes a necessary measure to safeguard (a) national security; (b) defence; (c) public security; (d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions; (e) an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters; (f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e); (g) the protection of the data subject or of the rights and freedoms of others*."

It must be highlighted that exceptions to the purpose limitation principle must be provided by legislative measures, implying that it is to the Legislator to provide for such exception. Moreover, when adopting such derogations to the purpose limitation principle, the Legislator is subject to several conditions. First, the measure must be aimed at safeguarding important public interests as listed in article 13 of the Directive 95/46, including public security, national security, important economic or financial interest or prevention and repression of crime. Second, the legislative measure is obviously submitted to the conditions established in Article 8 of the ECHR and related caselaw. For the record, the measure will need to satisfy the

requirements of clarity and foreseeability on the one hand, and must be necessary in a democratic society (proportionality test). Public authorities and the private sector are therefore not allowed to carry out further processing for an incompatible use in the absence of a legislation explicitly authorizing such processing.

Actually, this demonstrates that discussion about the purpose limitation principle is also a key feature of the general issue of balancing privacy v other competing interests, in particular security related purposes. The extent to which the European Legislator, and sometimes national legislators, use their power to allow derogations to the purpose limitation principle has raised considerable concerns with respect to the right to privacy. Scholars have discussed in detail the fact that the purpose limitation principle is actually so much eroded by the European Legislator itself, that it allows us to wonder whether this principle still have any meaning.[368] In particular, the adoption of the so-called Data Retention Directive and the proposals for a European Passenger Name Records (PNR) System in the aftermath of the EU-US agreement on the transfer of PNR data raise many questions. Both systems basically provide for the further use of data by competent public authorities for law enforcement purposes (which are by the way not always well defined) of data originally collected by the private sector (Internet Providers, Airlines) in the framework of commercial activities. These two examples clearly illustrate the incompatibility of uses between the original purpose and the further purpose of the processing.[369] Beyond discussion on the purpose limitation principle, many doubts are expressed regarding the compatibility of some legislative measures with Article 8 of the ECHR.

3.4.5 Principle of Legitimacy

Any processing must rely on one of the lawful grounds for processing provided in the Directive[370] and as implemented in national law. The Directive provides for six legitimating grounds for processing, which are also recalled in the Draft Regulation with only very slight differences.[371] Personal data may be processed only if:

(a) the data subject has unambiguously given his consent.

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract

(c) processing is necessary for compliance with a legal obligation to which the controller is subject

(d) processing is necessary in order to protect the vital interests of the data subject

(e) processing is 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

(f) processing is 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

[368] Frank Dumortier, Claire Gayrel, Joëlle Jouret, Damien Moreau and Yves Poullet, « La protection des données dans l'Espace européen de Liberté, Sécurité et Justice », *Journal de Droit Européen* 166 (2010): 33-46

[369] WP203, p. 16-17, where the Working Party clearly take the examples of the Data retention Directive and the PNR system to illustrate the "incompatibility" of purposes

[370] Article 7 of the Directive 95/46

[371] Article 6§1 of the Draft Regulation

overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Article 1 (1).

We will discuss further and with more details the lawful grounds for processing in the specific contexts of videosurveillance and biometrics. Let's mention here that the European Court of Justice has judged that this list of lawful grounds was exhaustive.[372] The controller is required to justify the processing on one of these grounds and cannot therefore invoke another ground.

3.4.5.1 Consent

The possibility to process personal data on the basis of the consent of data subjects is not uniformly dealt with by Member States. The Article 29 Working Party has progressively adopted some guidance regarding the issue of consent in specific contexts[373], and finally adopted a general opinion.[374] First of all, the Working Party recalls that data subject's consent is only one ground, among others, for the processing of personal data and that it is not always the primary or the most desirable means of legitimating a processing of personal data.[375] 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*."[376] 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.

3.4.5.2 Authorization by Law

Where a processing will find to be based on a 'legal obligation' or where necessary for the performance of a public task, one must not forget the requirements established by the ECHR under Article 8. Such a law authorizing/providing a processing of personal data should satisfy the legal and legitimacy requirements and be considered as 'necessary in a democratic society'.

3.4.5.3 Legitimate Interests of the Controller

In this case, the legitimate interests of the controller must also be balanced with the interests for fundamental rights and freedoms of the data subject. Such balance leaves some margin of appreciation to Member States. In practice, it makes this legitimate ground for processing the most open-ended and vaguest criteria. We will see in the cases of videosurveillance and biometrics dealt with further what is the guidance of the Article 29 Working Party in this respect.

[372] ECJ, *ASNEF*

[373] The Working Party has sometimes dealt with the limits of consent in specific situations, in particular in relation to electronic health records (WP131), employment (WP148), transborder data flows (WP114).

[374] Article 29 Data Protection Working Party, *Opinion 15/2011 on the definition of consent*, 13 July 2011, WP187

[375] *Ibidem*, p. 10

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

3.4.6 Transparency Principle

The principle of transparency commands that the data subject be informed about the processing of his/her personal data. The Directive distinguishes between two situations: the cases of direct collection from the data subject and the cases of indirect collection. Moreover, there are exceptions to the transparency principle.

In case of direct collection, the controller must provide to the data subject all the necessary information, having regard to the specific circumstances of the processing, to ensure a 'fair' processing, and at least the following information: "*(a) the identity of the controller and of his representative, if any; (b) the purposes of the processing for which the data are intended; (c) any further information such as - the recipients or categories of recipients of the data, - whether replies to the questions are obligatory or voluntary, as well as the possible consequences of failure to reply, - the existence of the right of access to and the right to rectify the data concerning him*".[377]

In case of indirect collection, the controller must "*at the time of undertaking the recording of personal data or if a disclosure to a third party is envisaged, no later than the time when the data are first disclosed provide the data subject with at least the following information, except where he already has it: (a) the identity of the controller and of his representative, if any; (b) the purposes of the processing; (c) any further information such as - the categories of data concerned, - the recipients or categories of recipients, - the existence of the right of access to and the right to rectify the data concerning him; in so far as such further information is necessary, having regard to the specific circumstances in which the data are processed, to guarantee fair processing in respect of the data subject*."[378]

This principle is closely related with the principle of a fair processing. There are however exceptions to the obligation of transparency. The Directive provides that Member States may limit the obligation of information where necessary to safeguard: "(*a) national security; (b) defence; (c) public security; (d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions; (e) an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters; (f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e); (g) the protection of the data subject or of the rights and freedoms of others*."[379] Much of these exceptions are understandable, notably in the context of criminal investigations and intelligence activities. Such exception must nevertheless be provided by law. This implies that the controller alone cannot invoke one of the exception without the authorization of the law.

As explained earlier, if the scope of application of national laws implementing the Directive 95/46 is in general inclusive, all national laws generally provide exceptions to the obligation of transparency for criminal justice (investigation) purposes.

There is also an exception to the obligation of information for the cases of indirect collection, "*where, in particular for processing for statistical purposes or for the purposes of*

[377] Article 10 of Directive 95/46

[378] Article 11§1 of Directive 95/46

[379] Article 13 of Directive 95/46

historical or scientific research, the provision of such information proves impossible or would involve a disproportionate effort or if recording or disclosure is expressly laid down by law."[380]

3.4.7 Data Quality Principle

The personal data processed must be "*adequate, relevant [and not excessive] in relation to the purposes for which they are collected and/or further processed*", and "*accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified*". This is a fundamental principle of the protection of personal data. Since the processing of personal data often entails effects for individuals (credit decision, billing, granting of a social service et cet…), it is of capital importance that the controller be under the obligation to process accurate and up to date data.

3.4.8 Proportionality Principle: Towards an Explicit Principle of Data Minimisation

The Directive 95/46 and Convention 108 provide that 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 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. The Draft Regulation clarifies this approach providing that personal data shall be "*limited to the minimum necessary in relation to the purposes for which they are processed*".[381]

3.4.9 Principle of Limited Retention

The personal data shall be "*kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed*."[382] As explained earlier in relation to the notion of 'controller', the determination of the retention duration is an essential element of the processing and this is a core responsibility of the controller. In this determination, the controller shall take du account of the purposes (specific, explicit and legitimate) for which he processes personal data and delete, destroy the personal data once the purpose is achieved. Nevertheless, the Directive further provides that "*Member States shall lay down appropriate safeguards for personal data stored for longer periods for historical, statistical or scientific use*". Retention beyond the "necessary period" for statistical purposes for example is possible under the conditions established by national law (e.g. anonymisation of the data).

3.4.10 Security principle

[380] Article 11§2 of Directive 95/46

[381] Article 5 c) of the Draft Regulation

[382] Article 6§1 e) of Directive 95/46

This is the principle according to which "*the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other forms of processing*."[383] It refers to the 'protection of personal data' in the literal sense. The obligation to implement appropriate technical and organization measures to secure the data is often shared between the controller and its processor. When resorting to a processor, the controller must "*choose a processor providing sufficient guarantees in respect of technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with those measures*."[384] The controller and the processor shall be bound by a contract.[385] The security rules that will apply to the processing will be those provided by the national law of the place where the processor is established.[386]

3.4.11 The Processing of Sensitive Data

The Directive provides specific attention, and lays down certain additional rules, concerning the processing of special categories of data, referred to as 'sensitive data'. In particular three 'categories of data' are foreseen. First, the Directive provides, as a principle, the prohibition of processing of "*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*."[387] Second, the Directive addresses the processing of data relating to offences, criminal convictions or security measures.[388] Third, the Directive foresees the use of a national identification number or similar general identifiers.[389] The Directive also provides for a series of exemptions that proceed from the same logic than legitimate grounds for processing.[390] The Directive further provides a broad, open-ended exemption, allowing Member States to adopt further exemptions "*for reasons of substantial public interests*".[391] The exemptions allowing the processing of sensitive data will not be detailed here. It is enough, at this stage of the project, to highlight that the processing of certain categories of personal data are submitted to specific, stricter rules and that the SALT framework will obviously have to integrate the specific requirements in this respect.

3.4.12 Restrictions on International Transfers

If the Directive aims at the approximation of national legislations in view of the liberalization of flows of personal data within the Union, there are however restrictions regarding the transfer

[383] Article 17§1 of Directive 95/46
[384] Article 17§2 of Directive 95/46
[385] Article 17§3 of Directive 95/46
[386] Article 17§4 of Directive 95/46
[387] Article 8§1 of Directive 95/46
[388] Article 8§5 of Directive 95/46
[389] Article 8§7 of Directive 95/46
[390] Article 8§2 of Directive 95/46
[391] Article 8§4 of Directive 95/46

of personal data outside the European Union (and European Economic Area[392]. This is a rather complex matter. This section explains the basic principles and requirements of the Directive in this respect.

First, the Directive establishes that transfers of personal data may only occur towards of countries ensuring an 'adequate level of protection'.[393] The European Commission is competent (but this competence is shared with Member States) to assess the level of protection of personal data provided in third countries and to adopt what is commonly called 'adequacy decisions'.[394] Such decisions have been adopted only with regard to a quite limited list of countries: Andorra, Argentina, Australia, Switzerland, Faeroe Island, Guernsey, Israel, Isle of Man, Jersey, New Zealand and Uruguay.[395] Some decisions have also been limited to certain sectors, such as in the case of Canada and the US Safe Harbour Scheme.[396]

Transfers of personal data towards 'non adequate' destinations must either comply with one of the derogations established under article 26§1 of the Directive 95/46[397] or must be accompanied by 'adequate safeguards' provided by the controller and subject to the authorization of the Member State.[398] It is also possible for the controller to resort to 'standard contractual clauses' adopted by the European Commission[399] and for which national authorization for the transfer is not necessary, at least in theory.[400]

[392] The Directive 95/46 applies to the European Economic Area, which includes all EU countries and in addition, non-EU countries Iceland, Liechtenstein and Norway.

[393] Article 25§1 of Directive 95/46

[394] Article 25§6 of Directive 95/46

[395] A direct access to all 'adequacy decisions' of the European Commission is provided here: http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm

[396] *Ibidem*

[397] *(a) the data subject has given his consent unambiguously to the proposed transfer; or (b) the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of precontractual measures taken in response to the data subject's request; or (c) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party; or (d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims; or (e) the transfer is necessary in order to protect the vital interests of the data subject; or (f) the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.* See also the guidance of the Article 29 Working Party, Working Document on common interpretation of article 26 (1) of Directive 95/46/EC, 25 November 2005, WP114

[398] Article 26§2 of Directive 95/46

[399] Two set of clauses are available for the controller-to-controller transfers of personal data: Commission Decision 2001/497/EC of 15 June 2001 on standard contractual clauses for the transfer of personal data to third countries under Directive 95/46/EC, *OJEC* L181, 04/07/2001 and Commission Decision 2004/915/EC of 27 December 2004 amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses, *OJEU* L385, 29/12/2004. A specific set of clauses is available for controller-to-processor transfers: Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries, *OJEU* L39, 12/02/2010

[400] Indeed, problems have been reported regarding the 'prior approval' by some national Data Protection Authority of the use standard contractual clauses, Commission Staff Working Document SEC(2006)95 on the implementation of the Commission decisions on standard contractual clauses for the transfer of personal data to third countries (2001/497/EC and 2002/16/EC) of 20 January 2006

3.4.13 Automated Individual Decision

The Directive provides that automated individual decisions, that is to say decisions which produce legal effects concerning the data subject or decision which significantly affect him based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct et cet…, must be accompanied by appropriate safeguards such as the right for the data subject to express his point of view.[401] Basically, the Directive aims here at expert systems, in which aspects of a person's personality or other intangible matters are evaluated. Such system should always provide for some 'human intervention' and should never rely exclusively on the automated system. There are some divergences between Member States regarding the 'adequate safeguards' framing the use of such automated systems.[402]

3.4.14 Perspectives for the SALT Framework

A brief overview of the general principles and obligations enshrined in the Directive 95/46 allows to identify various challenges raised by the objective of the SALT framework. First of all, the Directive 95/46 is written in general terms, and intends to apply to any processing technology. This implies that these general (technologically neutral) terms may sometimes be difficult to apply to a specific processing technology and context of processing. However, this is not so unusual, since law generally requires a work of interpretation. Second, because the Directive 95/46's first objective is the 'approximation' of national laws, there are many significant divergences of interpretation between Member States regarding the implementation of such principles and obligations in concrete circumstances. This implies that the legal framework for any surveillance technology must be found primarily at national level, in national regulations. Third, as far as security-related processing activities are concerned, in particular those carried out by public authorities vested with public security/public order competences, national law may provide legitimate exemptions to some of data protection obligations and principles, and Member States approach in this respect requires closer examination on a case by case basis.

3.5 PARIS Use Case: a First Look Into Videosurveillance

Videosurveillance is widely used in European Member States, while its regulation is far from being harmonized. The legal framework for Member States of the European Union consists of international and national legal instruments. It is one of the area where the divergences of approaches among Member States are the most striking. Although Directive 95/46 explicitly intends to apply to the processing of image and sound data, along with convention 108, some Member States have adopted specific legislation in relation to certain uses of videosurveillance. We will briefly recall how videosurveillance is dealt with at Council of Europe level (1), European Union level (2), and look into Belgian and French legislations in this respect (3) to see how the data protection principles presently finds to apply to cameras. In particular, the analysis of the French and Belgian legislations will allow to see how the Legislator distinguishes the installation of cameras according to different spaces/premises.

[401] Article 15 of Directive 95/46

[402] Douwe Korff, Working Paper No. 2, *op.cit*., pp. 82-86

3.5.1 Council of Europe and Videosurveillance

Article 8 of the ECHR therefore applies to the processing of image and/or sound data if they provide information on a identified or identifiable. The European Court of Human Rights has already judged that surveillance by cameras raise privacy concerns when there is systematic recording of the data captured. Moreover, Individuals who are lawfully within s State's territory also have the right to free movement, as protected in Article 2 of Additional Protocol No. 4 to the ECHR. This means that individuals have a general right o enjoy freedom of movement and conduct without being subject to detailed monitoring. As has been already explained, interferences into one's privacy may be legitimate if such interference finds to be necessary in a democratic society. Besides, videosurveillance activities generally fall within the scope of application of Convention 108, as far as sound and image data provide information on identified or identifiable individuals. In compliance with convention 108, the Council of Europe's European Committee on Legal Co-operation (CDCJ) has adopted guiding principles for the protection of individuals with regard to videosurveillance. More recently, the Parliamentary Assembly of the Council of Europe has adopted a specific resolution regarding videosurveillance of public areas. Noting that several Member States provided minimum guarantees in this respect, the CDCJ nevertheless stressed the need for more specific regulation: "*Considering that the existing equipment for video surveillance and software allows the use of a very strong zoom (with enlargement of up to 30-50 times) and high resolution, the Assembly strongly encourages Council of Europe member states to adopt legislation laying down limits for the installation of such equipment with respect to each specific place concerned*."[403]

3.5.2 European Union and Videosurveillance

There is no specific legal instrument regulating videosurveillance at EU level. The main applicable instrument is therefore the Directive 95/46, as briefly presented earlier. It is applicable to the processing of sound and image data, as explicitly foreseen in recital 14 of the Directive, which unambiguously intended to take into account the rapid growth of videosurveillance. Article 33 of the Directive requires that the European Commission report, at regular intervals, on the application of the Directive to the processing of sound and image data.[404] Because of important divergences between Member States regarding the implementation of data protection principles and obligations in relation to videosruveillance, the Working Party issued a first Opinion in 2002[405] and a subsequent opinion in 2004[406] with the aim to contribute to uniform application of national measures.

[403] Council of Europe Parliamentary Assembly, Resolution 1604 (2008) on videosurveillance of public areas of 25 January 2008

[404] In 2003, the British Institute of International & Comparative Law published a *Report on the Implementation of Directive 95/46/EC to the Processing of Sound and Image Data*. We are not aware whether the European Commission has carried out or not other (more recent) comparative study.

[405] Article 29 Data Protection Working Party, *Working Document on the Processing of Personal Data by means of Video Surveillance*, 25 November 2002, WP67

[406] Article 29 Data Protection Working Party, *Opinion 4/2004 on the Processing of Personal Data by means of Video Surveillance*, 11 February 2004, WP89

3.5.2.1 Scope of Application of Directive 95/46 to Videosurveillance Activities

As explained earlier, the Directive 95/46 does not apply to the processing of sound and image data for purposes concerning public security, defence, State security, and the activities of the State in the areas of criminal law. However, as underlined by the Working Party 29, many Member States applies their national law to these activities and provide for specific exemptions. In carrying out such surveillance activities and in all cases and circumstances, Member States remain submitted to Article 8 of the ECHR.[407]

3.5.2.2 The Notions of Personal Data and Processing Applied to Videosurveillance

Capture of images and sounds constitute a processing.[408] In contrast with the Council of Europe Consultative Body, the Working Party 29 has also made clear that surveillance by camera may involve a processing of personal data irrespective of whether there is continuous or discontinuous image acquisition.[409] The Working Party 29 recalls that the Directive 95/46 applies to any information, including sound and image data, concerning an identified or identifiable individual. As explained earlier, "*to determine whether a person is identifiable account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person*". One of the essential factor to determine whether the means likely reasonably to be used to identify the person will be the purpose of the processing. With respect to videosurveillance processing, which is generally implemented in order to allow the use of the images to possibly identify certain individuals, the Working Party 29 has stated that all the data captured by the cameras should therefore be considered as personal data, although identification will be necessary only rarely.[410] It has also considered that image and sound data are personal data even when a car number plate or a PIN code is filmed, instead of an individual's face.[411]

3.5.2.3 Lawfulness of the Processing

The principle that a processing should be "lawful" is of particular interest in the framework of videosurveillance. We have explained that any processing shall be in accordance with the law, and not only data protection legislation. This is particularly relevant in the case of videosurveillance, which may involve a range of laws and regulations according to the circumstances of installation of cameras (e.g. right to image, civil law et cetera…). Certain public bodies or local authorities may be subject to limited competences in the field of security and public order. The data controller, whether a public or private body, must check all the applicable national provisions before installing cameras.

3.5.2.4 Purpose Limitation Principle

[407] WP89, p. 13

[408] Recital 14 of Directive 95/46

[409] WP89, p. 15

[410] WP136, p. 18

[411] WP67, p.13 and WP89, p. 15

The data controller shall identify clearly the purpose or purposes sought and should refer those purposes in a document with other important privacy policy features.[412]

3.5.2.5 Legitimate Grounds for Processing

The Working Party 29 provides examples in relation to each legitimate ground for processing. Except some cases where the videosurveillance may possibly (although it is very questionable) rely on consent[413] and cases where the videosurveillance may be necessary to protect the vital interest of the data subject[414], there are mainly three legitimate grounds that may justify videosurveillance.

Legal obligation

In some cases, the installation of cameras is the result of a legal obligation on part of the controller. For example, in Belgium, it is notably the case regarding the installation of cameras in stadiums during certain football matches. The circumstances in which cameras shall be installed (masculine matches of football of 2nd and 1st national division and international matches), the number of cameras, the places to monitor, and the filming arrangements are regulated in detail.[415] Again in Belgium, it is compulsory for certain categories of casinos and gambling establishments to install a videosurveillance system.[416]

Performance of a task carried out in the public interest or in the exercise of official authority vested in the controller

This is notably the case when the controller is required to perform a task in the public interest, such as to detect road traffic offences or violent conduct on public transportation means. In general, the Article 29 Working Party considers that processing operations by means of videosurveillance should always be grounded on express legal provisions if they are carried out by public bodies.[417]

The legitimate interest of the controller

The legitimate interest pursued by the data controller should not override data subject's interests or fundamental rights and freedoms. In carrying out this analysis, careful consideration should be given to the scope of the tasks, powers and legitimate interests of the controller. "*Superficiality and the groundless extension of the scope of the tasks and powers*

[412] WP89, p. 17

[413] For example, concerning premises where a person's private life is led, such as in the case of installation of cameras in co-ownership

[414] The Working Party refers to the distance monitoring of patients in resuscitation units

[415] Royal Decree of 22 February 2006 relating to the installlation of cameras in stadiums - Arrêté Royal du 22 février 2006 relatif à l'installation et au fonctionnement de cameras de surveillance dans les stades de football, *MB*, 03/02/1999

[416] Royal Decree of 22 December 2000 relating to surveillance of casinos and gambling establishments - Arrêté Royal du 22 décembre 2010 relatif aux modalités de surveillance et de contrôle des jeux de hasard dans les établissements de jeux de hasard de classe IV et où les lieux de paris sont engagés, *MB*, 29/10/2010

[417] WP89, p. 18

should be absolutely banned."[418] Additionally, the Working Party 29 recommends that the parties concerned be heard in advance.

3.5.2.6 Principle of Subsidiarity of Videosurveillance

Videosurveillance systems should only be deployed on a subsidiary basis, implying that they shall be implemented only if other protection and security measures (stronger lighting of streets at night, alarms, armoured doors et cet…) prove clearly insufficient and/or inapplicable. This principle is actually consistent with ECHR caselaw under Article 8 according to which an interference into one's privacy may only be justified if there is no less intrusive means available to achieve the aim pursued.

This also requires assessing the indirect effects produced by massive recourse to videosurveillance, in particular considering the increasingly use of cameras near public buildings and offices.

3.5.2.7 Principle of Proportionality

Videosurveillance systems should only be installed for purposes that actually justify recourse to such systems. Basically, "*whilst a proportionate video surveillance and alerting system may be considered lawful if repeated assaults are committed on board buses in peripheral areas or near bus stops, this is not the case with a system aimed either at preventing insults against bus drivers and the dirtying of vehicles, or else at identifying citizens liable for minor offences such as the fact of leaving waste disposal bags outside litter bins and/or in areas where no litter is to be left about."*[419] This is the a basic example illustrating Article 8 ECHR caselaw according to which in order to be "necessary", the interference must be justified by a "pressing social need".

3.5.2.8 Proportionality of the Filming Arrangements

The principle under which data must be adequate, relevant and not excessive requires a careful assessment of the filming arrangements, by having regard, notably, to the following issues:

a) the visual angle as related to the purposes sought. Basically, the Article 29 Working Party explains that if the surveillance is performed in a public place, the visual angle should not allow visualising areas inside private places.
b) The type of equipment, fixed or mobile.
c) Actual installation of arrangements, fixed vie and/or movable cameras.
d) Possibility of zooming.
e) Image freezing functions
f) Connection with a center to send sound and/or visual alerts
g) The steps taken as a result of videosurveillance.[420]

3.5.2.9 Retention Periods

[418] *Ibidem*
[419] WP 89, p. 19
[420] WP89, p. 20

First, it will be necessary to consider whether retention of images is necessary or not. And where retention will be found necessary, the retention period should be in line with the purpose pursued.

3.5.2.10 Principle of Data Minimisation

The Article 29 Working Party underlines that many purposes can actually be achieved with a minimum of personal data. The data controller should therefore reduce, to the greatest possible degree, the processing of personal data. For example, where a camera aims at calculating the number of tills to be kept open in a supermarket, depending on the number of incoming customers, the system should process the minimum personal data necessary.

3.5.2.11 Transparency Principle

In order to ensure a fair processing, data subjects should be informed that videosurveillance is in operation in the area they are crossing. The information should be visible, positioned at a reasonable distance from the places monitored and may be provided in a summary fashion (such as symbols) provided that it is sufficient to ensure a fair processing in the circumstances of the case.

3.5.2.12 Additional Safeguards

The Article 29 Working Party stresses the need that specific processing operations be examined on a case by case basis, following notably from article 20 of the Directive 95/46 according to which certain processing presenting specific risks to the rights and freedoms of the data subjects should be subject to prior checking by supervisory authorities. Among the processing operations presenting specific risks, the Working Party mentions the "*permanent interconnection of videosurveillance systems managed by different data controllers*", "*the possible association of image and biometric data such as fingerprints", "the use of voice identification systems*", the use of facial recognition systems, the possibility to trace routes and trails and/or reconstruct or foresee a person's behaviour, the taking of automated decisions.[421]

We will now present hereunder an overview of the legal framework applicable to the deployment of videosurveillance in France and Belgium. This "overview" does not intend to provide an exhaustive analysis of each legal framework. Instead, it aims at identifying how these legal frameworks address the issue of the type of space/premise/place where cameras can be installed. We will see that both legal frameworks distinguish different categories of spaces, providing specific rules for the monitoring of each category of places. This is highly relevant for the definition of a SALT framework to see how these categories of spaces are established.

3.5.3 Overview of the French Legal Framework in Relation to Videosurveillance Activities

[421] WP89, p. 24

The regulation of videosurveillance in France mainly follows from two laws. The Act on Information Technologies and Civil Liberties ('Loi Informatique et Libertés')[422] is mainly applicable to cameras monitoring *non publicly accessible spaces.* The monitoring *of publicly accessible spaces/premises* by means of cameras is regulated by the 'Loi d'orientation et de programmation pour la sécurité intérieure'[423] (further referred to as the "LOPSI Act") as amended, notably by the Loi d'orientation et de programmation pour la performance de la sécurité intérieure (known as the "LOPPSI Act"). The criterion to determine if a space or premise is publicly accessible or not is whether there exist access restrictions to such space/premise. Publicly accessible spaces include all spaces, whether public or private for which there is no access restrictions. The payment of a fee to access the place is not considered as an access restriction. Libraries, public services premises, restaurants, shops, cinemas enter within the scope of publicly accessible premises. In contrast, non publicly accessible spaces/premises will be those spaces where there are access restrictions, such as schools, public or private offices.[424] It must be noticed that certain controllers may be simultaneously subject to both laws according to the place/space/premise that is monitored. For example, if the entrance of a school must be considered as a publicly accessible space submitted to the LOPSI Act, cameras monitoring the playground area will be considered as falling under the scope of the Information Technology and Civil Liberties Act.

3.5.3.1 "Videoprotection" of Publicly Accessible Spaces/Premises

Videosurveillance activities of publicly accessible areas are regulated under article 10 of the LOPSI Act of 1995 as amended. The modification of the law in 2011 by the LOPPSI Act II has modified all previous references to "videosurveillance" into "videoprotection". It is important to notice that the scope of application of the LOPSI Act covers all videosurveillance systems, irrespective of whether they include the processing of personal data or not.

Regarding public spaces ("voie publique"), the LOPSI Act provides that video monitoring can be implemented only by the competent public authorities for the following purpose: 1) protection of buildings and public installations and nearby; 2) safeguard of national defence installations; 3) regulation of transportation flows; 4) detection of road traffic offences; 5) prevention of offences against people or goods; 6) prevention of terrorist acts; 7) prevention of natural or technological disasters; 8) emergency assistance to individuals and fire protection; 9) safety of installations in amusement parks.[425]

Regarding publicly accessible premises (whether public or private premises), videosurveillance may be justified "*to ensure the security of people and goods where these premises are particularly exposed to risks of aggression, theft or acts of terrorism*."[426]

[422] Act No. 78-17 of 6 January 1978 on Information Technology, Data Files and Civil Liberties – Loi No. 78-17 Informatique et Libertés du 6 Janvier 1978 – as amended

[423] Act No. 95-73 of 21 january 1995 on homeland security orientation and programming - Loi n°95-73 du 21 janvier 1995 d'orientation et de programmation pour la sécurité intérieure

[424] See CNIL Press Release of June 2012 on best practices in relation to videoprotection and videosurveillance, at http://www.cnil.fr/fileadmin/documents/approfondir/dossier/Videosurveillance/CNIL-DP_Video.pdf

[425] Unofficial translation by the author, see article 10 II. of the LOPSI Act

[426] Unofficial translation by the author: « *Il peut être également procédé à ces opérations [de vidéoprotection] dans des lieux et établissements ouverts au public aux fins d'y assurer la sécurité des personnes et des biens lorsque ces*

Installation of cameras in both public spaces and publicly accessible premises is subject to the prior authorization of the State representative authority ("Préfet") with the opinion of a local commission presided by a Magistrate.[427] In this aim, the controller (owner of the cameras) shall submit a report containing information regarding the purposes of the surveillance system, the number and location of cameras and all necessary information regarding the filming arrangements.[428]

The CNIL reports that there are divergences in the interpretation and implementation of authorizations among local authorities. Some doubts and divergences arose with regard to the scope of application of the LOPSI Act to certain spaces (day nursery) and regarding the zones that may be filmed or not (certain local authority considers that the camera should not film people when they are eating whereas others do).

3.5.3.2 "Videosurveillance" of Non Publicly Accessible Spaces/Premises

Videosurveillance systems of non publicly accessible premises are subject to the Information Technology and Civil Liberties Act, implementing the Data Protection Directive 95/46, and subject to a declaration to the French Data Protection Authority, the CNIL ('Commission Nationale Informatique et Libertés'). The processing of image and sound data must therefore rely on one of the legitimate grounds provided under the national data protection legislation and ensure compliance with all principles (purpose, proportionality et cet…) and obligations (information, declaration et cetera…) enshrined in the law.

3.5.3.3 Role and Competences of the Data Protection Authority

The National Data Protection Authority (CNIL) is competent to ensure the supervision and control of cameras. In 2011, the CNIL proceeded to 150 controls over "videoprotection" systems. Interestingly, the CNIL reports that the main breaches to the laws encountered during controls related to:

- lack of authorisation of the State representative authority for cameras monitoring publicly accessible premises while the CNIL was actually controlling a "videosurveillance system" in non-publicly accessible premises (30% of the controls)
- Lack of declaration to the CNIL in cases of videosurveillance submitted to the national data protection act (60%)
- Insufficient or absence of information of data subjects (40%)
- Wrong orientation of the cameras (20%)
- Excessive retention period of the data (10%)
- Insufficient security measure (20%)[429]

lieux et établissements sont particulièrement exposés à des risques d'agression ou de vol ou sont susceptibles d'être exposés à des actes de terrorisme. »

[427] Article 10 III. of the LOPSI Act

[428] Décret n°96-926 du 17 octobre 1996 relatif à la vidéoprotection pris pour l'application des articles 10 et 10-1 de la loi n° 95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité

[429] See CNIL Press Release of June 2012 on best practices in relation to videoprotection and videosurveillance, *op. cit.*

The CNIL has also issued specific information notices to ensure a better compliance of controllers with their obligations, providing for best practices, recommendations of retention et cet…These "Best Practices notices" provide guidance in relation to videosurveillance in public spaces, at work, in schools, shops, living buildings, and home.[430]

3.5.4 Overview of the Belgian Legal Framework in Relation to Videosurveillanve Activities[431]

The legal framework applicable to videosurveillance in Belgium is complex since it follows from a series of general and sectoral legislations, the articulation of which has raised many questions and issues.[432] Belgium provides for a specific legislation in relation to videosurveillance adopted in 2007[433], and further amended in 2009[434]. Besides this specific legislation, the Privacy Act of 1992[435], implementing the Directive 95/46, remains applicable in several circumstances. About 20 other specific legislations have been identified to be relevant in relation to the installation of cameras.[436] To name a few, the work collective convention (Convention collection de travail n°68), the law relating to security during football matches, the law on the function of police, the law regulating private security and others may be applicable alternatively or additionally to the Videosurveillanve Law. We will present hereunder a summary of the videosurveillance law, because of its relevance as a specific legislation.

3.5.4.1 Scope of Application of the Videosurveillance Law

The Videosurveillance law applies to the installation of "cameras" defined as any system, whether fixed or mobile, aiming at preventing or detecting offences against goods or people, or maintaining the public order and which collect, process or record image data.[437] It must be noticed that the law applies irrespective of whether the cameras record or not image data. The simple processing, without any recording is subject to the law. However, the legislation does

[430] All these information notices are downloadable at http://www.cnil.fr/les-themes/videosurveillance/

[431] Information provided in this section is partly based on CRIDS report URBAN EYES submitted to the Service Publique Fédéral Intérieur regarding videosurveillance

[432] Marie-Sophie Devresse and Jean Pieret (under the dir.), La vidéosurveillance. Entre usages politiques et pratiques policières (Bruxelles: Politeia, 2010) In particular, Frank Dumortier, « Caméras de surveillance: la cohabitation légale reste houleuse…A propos du champ d'application de la loi du 21 mars 2007 et de sa coexistence avec d'autres normes réglant les caméras de surveillance » : 27-47

[433] Loi réglant l'installation et l'utilisation de cameras de surveillance du 21 mars 2007, *M.B.,* 31/05/2007, further referred to as the "videosurveillance law"

[434] Loi visant à modifier la loi réglant l'installation et l'utilisation de cameras de surveillance du 12 novembre 2009, *MB,* 18/12/2009

[435] Privacy Act of 8 December 1992 on the protection of privacy in relation to the processing of personal data – Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *MB*, 18/03/1993

[436] Privacy Commission, Recommandation d'initiative n°04/2012 du 29 février 2012 sur les diverses possibilités d'application de la surveillance par caméras, further referred to as « Privacy Commission Recommendations regarding the Videosurveillance Law of 2012 ».

[437] Unofficial translation of article 2, 4° of the Law on videosurveillance : « *tout système d'observation fixe ou mobile dont le but est de prévenir, de constater ou de déceler les délits contre les personnes ou les biens ou les nuisances au sens de l'article 135 de la nouvelle loi communale, ou de maintenir l'ordre public, et qui, à cet effet, collecte, traite ou sauvegarde des images; est réputée mobile, la caméra de surveillance qui est déplacée au cours de l'observation afin de filmer à partir de différents lieux ou positions* »

not apply to "simulated" cameras.[438] It also applies irrespective of whether the camera processes or not personal data (which is a relevant criterion for the application of the data protection law.)

It does not apply in cases for which a specific legislation exists and to cameras installed at work place in a series of cases.[439] This has led to a series of questions regarding the articulation of the videosurveillance law with other specific legislations.

Furthermore, it is provided that the general Privacy legislation remains applicable, except where it is explicitly contrary to the videosurveillance law. This last applies to cameras aiming at preventing or detecting offences against goods or people, or maintaining the public order. In fact, it is the purpose aimed at by the camera which is relevant to determine whether it is submitted to the videosurveillance law or nor. Any other camera that will not be installed in such aim will fall under the scope of the Privacy Act. And where a camera will find to contribute to several purposes (e.g prevention of theft and control of production process), the camera will be simultaneously submitted to both legislations.

The videosurveillance law distinguishes three categories of places: publicly accessible open spaces, publicly accessible closed premises and non publicly accessible closed premises. This distinction is of great importance because each category of places is submitted to a specific legal regime.

3.5.4.2 Videosurveillance in Publicly Accessible Open Spaces ("Lieu Ouvert"[440])

Following the definition of "lieu ouvert", there are two relevant cumulative criteria: the place must be "open" and accessible to the public. A place will be considered as "open" if there is no visible delimitation.[441] They are considered to include all "public spaces" in general, such as public roads ("voie publique"), market place, streets, squares, public gardens and parks.[442] It has been made clear that the will of the Legislator was not to allow private persons to monitor open public spaces. Therefore the monitoring by cameras of open public spaces must be considered as falling under the competence of public authorities.[443]

The decision to install cameras monitoring one or more publicly accessible open spaces is subject to the positive opinion of the local authority ('Conseil communal') after consultation of

[438] Frequently Asked Questions, Privacy Commission Recommendations regarding the Videosurveillance Law of 2012, p. 4

[439] Article 3 of the Law on videosurveillance

[440] Defined as "*tout lieu non délimité par une enceinte et accessible librement au public*"

[441] Arrêté Royal du 2 juillet 2008 relatif aux déclarations d'installation et d'utilisation de caméras de surveillance, article 4§1 « *pour l'appréciation du caractère ouvert ou fermé d'un lieu, l'enceinte doit au minimum être composée d'une délimitation visuelle légitimement apposée ou d'une indication permettant de distinguer les lieux* »

[442] Privacy Commission Note relative à la loi réglant l'installation et l'utilisation de caméras de surveillance, 20/01/2010, p. 5,

[443] Circulaire ministérielle du 10 décembre 2009 relative à la loi du 21 mars 2007 réglant l'installation et l'utilisation de caméras de surveillance, telle que modifiée par la loi du 12 novembre 2009, M.B., 18/12/2009, as amended on 13 may 2011, M.B., 20/05/2011, further referred to as the « Ministerial Circular of 2009 »

the Chief Police Zone.[444] Notification of the decision to install cameras shall also be notified to the Belgian Data Protection Authority, the 'Privacy Commission'.

The controller should not monitor other places for which it has no competence, as private premises, except with the approval of the person concerned.[445] This means that when a camera monitoring a street will include in its visual angle the entrance of a private habitation or a café, the controller should either obtain the express (and preferably written) consent of the owners of the habitation and café or should mask the said premises by technical means.[446] The videosurveillance system should be announced via a standard pictogram as provided by Royal Decree.[447]

The viewing in real time of images is allowed only under the control of police services and for the purpose of immediate intervention in case of breaches of the law, damages, or nuisances or to maintain public order.[448] The recording of images is allowed only to gather evidence of breaches of the law, damages and nuisances, and for the identification of offenders, witnesses or victims. If the images recorded do not contribute to provide such evidence, they should be deleted after one month.

3.5.4.3 Videosurveillance in Closed Spaces, Publicly Accessible ("Lieu Fermé Accessible au Public"[449]) or Non-Publicly Accessible ("Lieu Fermé Non Accessible au Public[450])

In contrast with "open spaces", all "closed spaces" are actually delimited and therefore basically include all kind of premises/buildings. The law further distinguishes between closed publicly accessible spaces from closed non publicly accessible spaces. Following the definitions provided in the law, the relevant criterion to operate this distinction in practice is whether such place is destined to provide services to the public.[451] As in the French regulation, the fact that the access to a specific space may be subject to conditions (such as a price entrance) is not relevant to consider such a place as non-publicly accessible.

[444] Article 5§2 of the Law on videosurveillance

[445] Article 5§3 last alinea of the Law on videosurveillance : « *Le responsable du traitement s'assure que la ou les caméras de surveillance ne sont pas dirigées spécifiquement vers un lieu pour lequel il ne traite pas lui-même les données, sauf accord exprès du responsable du traitement pour le lieu en question*. »

[446] Ministerial Circular of 2009, point 1.4 "proportionality of images"

[447] Arrêté Royal du 10 février 2008 définissant la manière de signaler l'existence d'une surveillance par caméra, *MB*, 21/02/2008

[448] Article 5§4 of the Law on videosurveillance: "*Le visionnage de ces images en temps réel n'est admis que sous le contrôle des services de police et dans le but de permettre aux services compétents d'intervenir immédiatement en cas d'infraction, de dommage, de nuisance ou d'atteinte à l'ordre public et de guider au mieux ces services dans leur intervention* »

[449] Defined as "*tout bâtiment ou lieu fermé destine à l'usage du public, où des services peuvent lui être fournis*"

[450] Defined as "*tout bâtiment ou lieu fermé destine uniquement à l'usage des utilisateurs habituels*"

[451] Ministerial Circular of 2009, point 1.5.2. "Difference between closed premises publicly accessible and non publicly accessible"

In this framework, shops, banks, metro stations, cafés, restaurants and cinemas must be considered as publicly accessible closed premises. *A contrario*, private homes, habitations buildings will be considered as non publicly accessible premises.

The decision to install cameras monitoring one or more closed spaces whether publicly accessible or not must be notified to the Privacy Commission after consultation and to the Chief Police Zone.[452]

The controller should not monitor other places for which it has no competence. However, it has been interpreted that when the filming of the entrance of a private buildings requires the filming of a little portion of the street, it is not considered that the camera is monitoring an open space. The camera will remain subject to the regime established for closed premises.[453] The cameras should be oriented so as to limit to the maximum extent the filming of the open space.[454] The videosurveillance system should be announced via a standard pictogram as provided by Royal Decree.[455]

Regarding publicly accessible closed premises, the viewing in real time of images is allowed only for the purpose of immediate intervention in case of breaches of the law, damages, or nuisances or to maintain public order.[456] The recording of images is allowed only to gather evidence of breaches of the law, damages and nuisances, identification of offenders, witnesses or victims. If the images recorded do not have such evidential value, they should be deleted after one month. Regarding non publicly accessible closed premises, the law does not provide for the possibility to watch the images in real time.

The Law further provides that the controller only or the person acting under its authority can access to the images.[457] The controller can nevertheless transmit the images to police services.[458] The police services can request the access to images from cameras installed in "closed spaces" whether publicly accessible or not.[459] However, regarding non publicly accessible premises, the law provides that the controller can require the presentation of a judicial mandate in case of access request by the police.[460]

Moreover, the Privacy Commission explained that the viewing in real time by police services of images from cameras installed in closed places (whether publicly accessible or not) is not allowed by the law on videosurveillance, except under specific legal circumstances: during the

[452] Article 6§2 and 7§2 of the Law on videosurveillance

[453] Ministerial Circular of 2009, point 1.4 "proportionality of images"

[454] Article 7§2 of the law on videosurveillance

[455] Arrêté Royal du 10 février 2008 définissant la manière de signaler l'existence d'une surveillance par caméra, *MB*, 21/02/2008

[456] Article 5§4 of the Law on videosurveillance: "*Le visionnage de ces images en temps réel n'est admis que sous le contrôle des services de police et dans le but de permettre aux services compétents d'intervenir immédiatement en cas d'infraction, de dommage, de nuisance ou d'atteinte à l'ordre public et de guider au mieux ces services dans leur intervention* »

[457] Article 9 of the Law on videosurveillance

[458] Article 9 1° of the law on videosurveillance

[459] Article 9§2 of the Law on videosurveillance

[460] *Ibidem*

investigation phase where the police acts upon its explicit competences following all relevant legislations (law on the Function of Police; criminal procedure code) and under the instructions of the competent judiciary authority.[461]

3.5.5 Perspectives for the SALT Framework

The processing of image and sound data is, in general, submitted to general data protection legislations. It implies that all the concepts and principles explained earlier in relation to Directive 95/46 generally finds to apply. Because of its general character, the Directive 95/46 nevertheless fails to address all the specific (and numerous) issues raised by videosurveillance. At Council of Europe level, the adoption of specific legislations has been recommended, in particular with respect to the monitoring of 'public spaces'. The implementation (both in law and in practice) in Member States of the general requirements of the Directive 95/46 to videosurveillance activities is not consistent. Some Member States have adopted specific legislations, which come to apply simultaneously or alternatively to data protection legislations, as in France or Belgium. In UK however, there is no specific legislation applicable. The Working Party 29 has provided some general guidance in order to contribute to harmonize the approach at EU level, but it did not address in details the problems raised by the use of cameras according to the type of places monitored (public, private et cetera…). The reason is that the Directive 95/46 does not provide such competence to the Article 29 Working Party. It is therefore mainly at national level that different categories of spaces have been distinguished in order to frame the use of cameras.

[461] Privacy Commission Recommendations regarding the Videosurveillance Law of 2012, p. 9

3.6 PARIS Use Case 2: a First Look Into Biometric Technologies

If biometric technology exists for a quite long time (e.g. fingerprinting used for law enforcement), new applications are emerging and developing rapidly, notably thanks to the introduction of new biometric technologies and the progressive diminution of its cost.[462] The application of the rules of personal data protection to biometric technologies has required some clarifications to address specific issues. Moreover, the debate relates to the *legitimacy* of the applications of biometric technologies, which are understood to raise specific risks and concerns with regard to the right to respect for private life, but also with regard to the right to a fair trial and the presumption of innocence, freedom of movement and the prohibition of discrimination. Biometrics applications for borders control purposes or national identification systems, such as ID cards, will not be addressed here specifically. Neither will be dealt with biometrics applications for criminal justice purposes. These applications actually require the adoption of specific legislations. Rather we will try to focus on the application of data protection principles to biometric applications that are not under the competence of regulation of the Legislator.

3.6.1 Council of Europe and Biometrics

The Council of Europe generally considers that biometric technology and biometric data are of a special nature, with regard to their biological nature containing possible health-related data and their relative uniqueness.[463] Given the inherently probabilistic character of biometric systems, the Consultative Committee has argued for a not to rapid installation of these systems considering that "*an all too enthusiast rapid introduction may entail unforeseen effects that are hard to reverse*".[464] We have seen earlier in the present chapter that the Court of Strasbourg also raised concerns regarding the possible future uses, yet unknown, of biometric data and gave strong weight to this argument to make fall DNA data under the scope of Article 8.[465] The Parliamentary Assembly further adopted a resolution, calling upon Member States to elaborate a standardised definition of biometric data, revise the existing data protection legislations by adjusting them to the specificities of biometric technologies, recommend the use of biometrics template instead of raw biometrics whenever possible, and promote proportionality in particular promote proportionality in dealing with biometric data, in particular by « *limiting their evaluation, processing and storage to cases of clear necessity, namely when the gain in security or in the protection of public health or of the rights of others clearly outweighs a possible interference with human rights and if the use of other, less intrusive techniques does not suffice*."[466] It is easily understandable that the central issue will be in adopting a proportionate approach in the admissibility of biometrics systems.

[462] Nancy Yue Liu, *op.cit.:* 29-59

[463] Consultative Committee on the Convention for the protection of Individuals with regard to the automatic processing of personal data (T-PD), Progress Report on the application of the principle of Convention 108 to the collection and processing of biometric data (2005)

[464] *Ibidem*, p. 8

[465] *S. and Marper v. the United Kingdom*, *op. cit.*

[466] Council of Europe Parliamentary Assembly, Resolution 1797 (2011) on the need for a global consideration of the human rights implications of biometrics of 11 March 2011

3.6.2 European Union and Biometrics

The Directive 95/46 does not specifically address the issue of biometrics technologies. The Draft Regulation contains specific references to biometrics, providing distinct definitions of 'genetic data' and 'biometrics data'. These last are defined as '*any data relating to the physical, physiological or behavioural characteristics of an individual which allow their unique identification, such as facial images, or dactyloscopic data*'.[467] The Draft Regulation further proposes to establish an obligation to carry out a data protection assessment regarding processing operations of genetic and biometric data.[468] Waiting for the outcome of the legislative process regarding the Regulation proposal, we will present here how biometric data and biometric systems are presently dealt with by the European Union. In particular, the Article 29 Working Party has been led to consider the issue of biometric technologies in several opinions, notably in a first opinion on Biometrics published in 2003[469] and more recently, in a renewed opinion on biometric technologies in 2012.[470] These opinions are of great interest for the purposes of PARIS project, since they contain essential elements regarding the specific risks raised by these technologies, elements regarding the application of Directive 95/46 to these technologies, and recommendations for the carrying out of privacy impact assessments when envisaging the recourse to these technologies. They are therefore of direct interest for the SAlegaIT framework and require a detailed presentation.

3.6.2.1 The Notions of Personal Data and Processing Applied to Biometric Technologies

The Article 29 Working Party provides some definitions, relevant to biometric technologies. These definitions can be considered as an attempt to adopt standardized definitions at EU level and are therefore of interest for all EU Member States. Biometric data are defines 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*."[471] Biometric data will in most cases be personal data. They entail an element of content (A has these fingerprints, B has this face measures) and they can work as identifiers.[472]

In 2003, the Article 29 Working Party defined a Biometric system as "*applications that use biometric technologies, which allow the automatic identification, and/or authentication/verification of a person*."[473] Due to the technological developments in the field of biometric technologies and the fact that they can also now be used for categorisation/segregation purposes, the Working Party suggests that a biometric systems could be defined more broadly including any system "*that extracts and further processes*

[467] Article 4 (11) of the Draft Regulation

[468] Article 33 of the Draft Regulation

[469] Article 29 Data Protection Working Party, *Working Document on biometrics*, 1 August 2003, WP80

[470] Article 29 Data Protection Working Party, *Opinion 03/2012 on developments in biometric technologies*, 27 April 2012, WP193

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

[472] *Ibidem*

[473] WP80 on biometrics, p. 3

biometric data".[474] The extraction of biometric data from a biometric source (human tissue sample) qualifies as collection of personal data. More generally all operations within a biometric system qualifies as processing of personal data (enrolment, storage, matching). However the sources of biometric data (tissue samples, blood samples et cet…) are not personal data as such and their collection, storage and use are in general subject to separate rules.

This leads the Working Party to consider that since in most cases, biometric systems involve the processing of personal data, these systems are submitted to the principles and obligations enshrined in Directive 95/46. The elements of legal analysis provided by the Working Party are of particular interest notably with respect to the general principle of proportionality and the lawful grounds for the processing of biometric data. Besides, any use of a biometric system should follow the recommendations of the Working Party regarding prior internal assessment of the purpose of the system[475], prohibition of further incompatible use and other data quality safeguards.

3.6.2.2 Some Elements to Assess the Proportionality of a Biometric Systems

With respect to biometric systems, once the need (purpose pursued) has been identified accordingly with the principles of 'specificity' and 'legitimacy', the Working Party 29 recommends to give prior consideration to four main factors to assess the proportionality of the biometric system envisaged, which follows in closed terms from the proportionality test of Article 8§2 of the ECHR.

First, one must assess whether the system is necessary to meet the identified need. Convenience and cost effective reasons cannot be considered valid. There must be a demonstration that the system is essential for satisfying that need. Second, one must assess whether the system is likely to be effective in meeting that need and having regard to the specific characteristics of the biometric system envisaged. Third, one must assess the resulting loss of privacy and whether it is proportionate to the anticipated benefit. Basically, if the benefit is minor, the loss of privacy will not be considered appropriate. Finally, one must assess whether less intrusive means could achieve the desired aim (the least restrictive measure test).[476]

3.6.2.3 Lawful Grounds for Processing Biometric Data

Interesting elements of interpretation of the Directive 95/46 when applied in the context of biometrics systems are provided in relation to the lawful grounds that can be invoked (or not) for the installation of biometric systems.[477]

[474] W193 on developments in biometric technologies, p. 5

[475] WP203 on purpose limitation explained earlier in the present chapter

[476] WP193, p. 8

[477] *Ibidem*, p. 10-13

Consent

The consent of the data subject may provide the ground for the processing of his/her biometric data according to specific conditions and circumstances.

First, with regard to the circumstances, the Article 29 Working Party underlines that there are cases of strong presumption of invalid consent because of the imbalance between the data subject and the controller, notably between an employee and his employer. In these cases, the data subject's consent will generally be considered as the weaker lawful grounds for the processing of his/her biometric data. It is extremely unlikely that the data subject's consent will be considered to satisfy the conditions of a freely given consent. The processing of biometric data in the context of employment would therefore preferably be based on another lawful ground.

Second, with regard to the conditions under which the data subject's consent may validly justify the processing of biometric data requires that such consent satisfy the conditions of a freely given and informed consent. It is therefore submitted to two essential conditions. First, a valid alternative to the enrolment in the biometric system should be proposed to data subjects, in order to guarantee the freedom of choice of the data subject. A system that would discourage data subjects from using it would not ensure a freely given consent and would therefore be invalid. For the data subject to freely consent to enrol in the biometric system, he/she must be previously provided sufficient information about system so as to ensure fairness.

Contract

This legal ground can only apply when pure biometric services are provided (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.

Legal obligation

Biometric data in passports, visas and some national identity cards are examples of cases where the processing of biometric data is provided by law.

Legitimate interests of the controller

For the record, 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 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 system 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 "*as a general rule, the use of biometrics for general security requirements of property and individuals cannot be regarded as legitimate interest overriding the interests of fundamental*

rights."[478] The Working Party considers that the security of property and individuals may only validly justify the use of biometric system under two conditions:

1) In presence of high risks situations; there must be evidence of objective and documented circumstances of the concrete existence of a considerable risk. The Working Party provides the example of the use of fingerprint and iris scan verification to control the access of a laboratory doing research on dangerous viruses.
2) After verification of possible alternative measures that could be equally effective but less intrusive (subsidiarity principle).

3.6.2.4 Automated Processing

In certain cases the processing of biometric data may lead to potential discriminatory consequences for the persons rejected by the system. There must be adequate safeguards against such automated decisions that can affect significantly the data subjects.[479]

3.6.2.5 Transparency

The obligation to inform the data subject is a key element to ensure a fair processing. Such a duty of transparency is challenged by current developments in biometric systems which can operate without the active participation of the data subjects. The data subjects may not differentiate cameras equipped with a facial recognition system from those that are not. The Article 29 Working Party considers that "*any system that would collect biometric data without the data subject's knowledge is to be avoided*."[480] Consequently, if a biometric system does not require the active participation of the data subject, this should be compensated by the provision of adequate and relevant information.

3.6.2.6 Sensitive Data

As far as biometric data may reveal sensitive data, such as racial or ethnic origin or data concerning health, additional safeguards should be put in place as required under article 8 of the Directive 95/46.[481] This is essential notably in view to prevent discriminations that are prohibited.

3.6.2.7 Other Safeguards for People with Special Need

The Working Party 29 is particularly concerned by the risks of stigmatisation or discrimination of vulnerable people and or individuals that are unable to enrol in biometric system for several reasons. It is recommended that more stringent measures be in place for those individuals.[482]

[478] *Ibidem*, p. 13
[479] *Ibidem*, p. 14
[480] *Ibidem*
[481] *Ibidem*, p. 15
[482] *Ibidem*

3.6.2.8 Security Principle

It requires that technical and organisation measures be put in place to ensure the security of the personal data processed.[483] According to the circumstances of the processing and whenever possible, the Working Party recommends that biometric data be stored as biometric templates, that centralised storage be avoided (especially where biometric data are used for verification purposes), that the system should allow to revoke the identity link (in order to renew it or to delete it in case of withdrawal of consent for example), that biometric information be always stored in encrypted form and that the decryption keys be only accessible on a need to know basis.[484]

3.6.3 France and Biometrics

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.[485] Other "*automatic processing comprising biometric data necessary for the verification of an individual's identity*" are submitted to the prior authorization of the CNIL.[486] In practice, the CNIL has developed a doctrine distinguishing between two categories of processing of biometrics data: a limited list of processing of biometric data is submitted to a simplified declaration, while all other processing remain subject to prior examination and authorization of the CNIL.

3.6.3.1 Biometric Applications Subject to 'Simplified Declaration'

The CNIL has adopted 'unique authorization' for a series of processing of biometric data, which are therefore 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[487]
- use of fingerprinting exclusively stored in a personal device to control access to professional premises[488]
- use of hand geometry to control access to school restaurants[489]
- use of vein pattern recognition to control access to professional premises[490]

[483] *Ibidem*, p. 14

[484] *Ibidem*, p. 31-32

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

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

[487] 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

[488] 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

[489] 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

[490] 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

- use of fingerprinting in professional laptops.[491]

This implies that for the above-mentioned situations, the use of certain biometric technology has been considered as proportionate by the CNIL, provided these uses also satisfy other data protection requirements, such as security requirements.

3.6.3.2 Biometric Applications Subject to 'Prior Authorization'

All other biometric applications are submitted to the prior authorization of the CNIL. In order to have a global overview of the CNIL policy regarding admissibility of uses of biometric applications, all relevant deliberations should be examined. A quick search into the database of 'Legifrance' containing all CNIL deliberations regarding 'fingerprinting' shows that till now, about 238 deliberations, among which 174 authorizations and 64 refusals, have been adopted regarding uses of fingerprint data since 2005.

The fact that most uses of biometric data (except those submitted to 'simplified declaration') are submitted to the CNIL's prior authorization and that such authorizations/refusals are publicly available constitutes a good opportunity for further research into CNIL's deliberations. Further research would be required to identify the cases that are now submitted to simplified declaration (certain deliberations may concern similar cases before the adoption of 'unique authorization by the CNIL'), but mainly to identify which uses of biometrics are generally authorized or refused in order to identify the underlying *proportionality policy* of the CNIL in this field.

3.6.4 Belgium and Biometrics

If we exclude national identification documents, and biometric applications for criminal justice purposes, there is no specific legislation addressing the issue of biometrics technology on the model of the videosurveillance law. In contrast with the French example, there is little guidance and/or recommendations from the Privacy Commission 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.[492] In general, the Opinion of the Privacy Commission is consistent with the recommendations issued by the Article 29 Working Party in 2012.

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 dealt with biometric data with the same precaution that with personal data.[493] 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

[491] 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

[492] 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)

[493] *Ibidem*, p. 8, point 28

make the processing proportionate.[494] 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 the storage in a card and or in a local device.[495] 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.[496] This approach is quite contrasted with the French one where we have seen that the CNIL has provided some 'unique authorizations' for similar biometric applications. Biometrics systems should not be used only for convenience or costs reasons.[497] Where necessary, its use should be strictly limited to the spaces/premises/services requiring such kind of security measures.[498]

3.6.5 Perspective for the SALT Framework

This brief overview of the issue of protection of personal data applied to biometrics technologies has allowed identifying first principles directly relevant for the SALT framework. The Working Party 29 provides some general guidance at EU level. However, as in the case of videosurveillance, the extent to which biometric applications are considered admissible must primarily be examined at national level. A brief overview of the French and Belgian approaches can already show some divergences. Interestingly, the issue is not always dealt with exhaustively at national level. While only general guidance is available in Belgium, extensive deliberations have been issued by the CNIL in France regarding biometrics applications. These deliberations translate CNIL's proportionality policy in this respect (which however does not imply that it is fully consistent and compliant with ECHR's proportionality policy). As explained, further research would be required to identify the underlying requirements applied by the CNIL during its authorization-making process. Such research could therefore allow to identify further criteria that are taken into account by the CNIL to *accept* or *refuse* a biometrics processing.

[494] *Ibidem*, p. 10, point 39
[495] *Ibidem*, p. 14, point 58
[496] *Ibidem*, p. 17, points 70-11
[497] *Ibidem*, points 72-73
[498] *Ibidem*, point 75

4 Accountability: a Way to Ensure Transparency and Trust

Fanny Coudert (ICRI-KU Leuven-iMinds)

4.1 Introduction

The European Commission has introduced in the proposals of the Data Protection Reform Package, a principle according to which personal data shall be processed under the responsibility and liability of the controller, who shall ensure compliance with the provisions adopted pursuant to these instruments. While not termed expressly, this principle is expected to introduce an accountability-based approach within the European data protection framework.

The principle of accountability has gained importance in the privacy debates since the Opinion of Article 29 Working Party on the principle of accountability (2010).[499] Accountability is approached as a way to put data protection into practice, in which the data controller could be required to demonstrate compliance with the data protection framework to supervisory authorities.

The principle of accountability is however not new to data protection. The fourteenth Principle of the Organisation for Economic Co-operation and Development (OECD) Guidelines of 1981, one of the first data protection instruments, entitled "the Accountability principle" was already stating that "*a data controller should be accountable for complying with measures which give effect to the principles stated above*". As detailed in the Explanatory paragraph, the introduction of this principle was motivated by the fact that "*it is for his benefit that the processing of data is carried out*". Accordingly, it was seen as essential that under domestic law, accountability for complying with privacy protection rules and decisions should be placed on the data controller who should not be relieved of this obligation merely because the processing of data is carried out on his behalf by another party.

The meaning of the term "accountability" is however not always clear and needs to be further refined. Understanding what the concept of accountability entitles and how it can be articulated with other close concepts such as the ones of liability, responsibility and answerability seems however an unavoidable task in the context of PARIS project. The field of political sciences has produced abundant literature in order to grasp the different meanings of accountability. To that end, a review of the most important pieces of the literature will allow us to clarify the concepts and the different elements that should be taken into account when designing accountability mechanisms.

In a second part, this Chapter will focus on how such concept is being approached and introduced within the data protection framework. As mentioned above, the principle of

[499] Article 29 Data Protection Working Party, *Opinion 3/2010 on the principle of accountability*, 13 July 2010, WP 173.

accountability is there closely linked to the ones of responsibility and liability. This will allow us to identify the issues linked to the introduction of an accountability-based approach into the data protection framework, as well as a first list of elements that should be integrated into accountability mechanisms. The findings of this Chapter are also expected to base the definitive list of requirements for the design of accountable policies, procedures and practices in surveillance systems that should integrate the SALT framework, which will be dealt with in Deliverable D.2.2.

4.2 Understanding Accountability

Accountability is the fact of being account-*able*, i.e. the ability to give an account. According to the Oxford Dictionary, being accountable is to be required or expected to justify actions or decisions. Accountability is thus a process which involves an accountor who is called by an accountee to make visible to others the motives and content of its decisions and actions. While the idea lying behind the concept is easy to grasp, accountability relationships exist in many ways and shapes, depending on the parties involved to the process, the relationship established between them and the different obligations stemming from the very process of giving an account. It follows that the concept is not always clearly defined and often confused with other close concepts such as responsibility, answerability, dialogue, control or responsiveness.

The concept of accountability has been mostly the focus of research in the field of public governance, in public administration literature, by political scientists. The goal of accountability procedures is in this context twofold: to promote good governance and to foster compliance. The thorough analysis performed in this field allows us to drawing a clear picture of what should be understood under the concept of accountability and to define its intrinsic features. It also allows to clarifying the critical features that accountability mechanisms should integrate to achieve their goals.

Accountability mechanisms are processes tending to increase visibility, thus transparency and trust. They first act as reflection and learning mechanisms, as long as they provide the necessary feedback about the intended and unintended effects of their practices.[500] As stressed by Bovens[501], "*the possibility of sanctions from clients and other stakeholders in their environment in the event of errors and shortcomings motivates them to search for more intelligent ways of organizing their business. Moreover, the public nature of the accountability process teaches others in similar positions what is expected of them, what works and what doesn't*".

But accountability mechanisms can also act as promoting "proven compliance", mere compliance being no more than "bling trust", while accountability entails "proven trust".[502]

[500] Mark Bovens, "Two Concepts of Accountability: Accountability as a Virtue and as a Mechanism", West European Politics 33-5 (2010): 946 — 967.

[501] *Ibidem*

[502] Paul De Hert, "Accountability and system responsibility: New Concepts in Data Protection Law and Human Rights Law", in *Managing Privacy through Accountability,* ed. Daniel Guagnin, et al. (Palgrave Macmillan: 2012), 199.

Accountability mechanisms will act by "*making bad* – and good- *acts visible*".[503] "*In a scheme of accountability it is possible for a person involved to prove good behavior because he or she took active, assignable steps to achieve a certain good*".[504] However, "*visibility alone does not guarantee compliance*", it only contributes to make compliance easier than violation.[505] In words of Weitzner et al. "*for those rare cases where rules are broken, we are well aware that we may be held accountable through a process that looks back through the records of our actions and assess them against the rules*".[506] This role should however not be minimized as "*the vast majority of legal and social rules that form the fabric of our societies are not enforced perfectly or automatically, yet somehow most of us still manage to follow most of them all the time*".[507] This is because we "*follow rules because we are aware of what they are and because we know there will be consequences, after the fact, if we violate them*".

As shown by De Hert, "*whist not being a straightforward legal concept, there is a relationship with the law and legal arrangements in the sense that the concept is used to challenge existing law or the lack of it*".[508] Legal scholars will tend to focus on a different concept, the one of liability. Liability is the state of being legally responsible for something. But "*a system of legal responsibility or liability can be based either on a logic of compliance or on a logic of account giving (…) an interesting aspect of liability is its capacity for modulation*".[509] The introduction of a principle of accountability within the data protection framework is often accompanied with, on the one hand, the warning that the implementation of accountability mechanisms will not waive data controllers' legal liability from lack of compliance, and on the other hand, with the expressed need to articulate both concepts, i.e. to what extent accountability mechanisms can contribute to demonstrate compliance and thus to modulate data controllers' liability.[510]

That being said, accountability is a concept that can stand on his own and which will take different shapes depending whether it is approached as a normative concept, in its broad and active sense of "organizational virtue" or whether it is approached as a social relation or mechanism, in its narrow or passive sense, as "mechanism of control".[511] Both approaches are of interest for the SALT Framework:

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 with privacy-related legislation, a way to

503 Daniel J. Weitzner et al, "Information accountability", *Communications of the ACM*, Vol.51, N°6, (2008): 84-87

504 Paul De Hert, "accountability and system responsibility …", *op. cit.*

505 Daniel J. Weitzner et al, *op. cit.*

506 *Ibidem*

507 *Ibidem*

508 Paul De Hert, "accountability and system responsibility …", *op. cit.*

509 *Ibidem*

510 See e.g. Colin Bennett, "The Accountability Approach to Privacy and Data Protection: Assumptions and Caveat", in *Managing Privacy through Accountability,* 33-48

511 Mark Bovens, *op. cit.*

exercise constrain or to hold stakeholders liable for their action, is a transparency mechanism whose goal is to increase trust in the design and use of surveillance systems. It can be concerned with the legal procedures directed to enforcement but it can also become a strong asset in the implementation of the principles of transparency or of foreseeability.

Within the SALT framework, the first meaning of accountability will be more fitted to address the need to increase legitimacy of decisions relating to the balance between privacy and surveillance. Procedures based on this first meaning will be directed to decision-makers when opting for the implementation of surveillance systems. By contrast, the second meaning of accountability will operate at a lower level and will rather tend on providing trust in the design and further use of a surveillance system. Accountability mechanisms based on this second meaning and goal will be directed to system developers and operators during the life-cycle of the surveillance system. We examine both concepts in turn.

4.2.1 Accountability as Organizational Virtue: Increasing Legitimacy of Decision-Making.

As showed by Bovens[512], accountability as organizational virtue, i.e. in an active sense of virtous behaviour, is used as a normative concept, as a set of standards for the evaluation of the behaviour of public actors, or as a desirable state of affairs. This understanding can be found in American academic and political discourse as well as in a series of policy documents of the European Commission such as the 2001 White Paper on Governance. For the European Commission, it serves as a synonym for "clarity", "transparency" and "responsibility". Bovens shows that the term is even equated to broader concepts such as "involvement", "deliberation", and "participation". It refers to no more than to a desirable quality of public officials and public organisations, as a norm of good governance which does not entail sanctions. Accountability is in that context understood as answerability of a public organization to its stakeholders for the use of the power granted to it. The active concept of accountability thus appears very hard to define substantively.

As a way of example, One World Trust, a charity that conducts research on practical ways to make global organizations more responsive to the people they affect, has however tried to provide a definition and to set a series of criteria to measure the accountability of transnational actors.[513]

This set of criteria is contained under "The Global Accountability Framework" which proposes norms of good corporate governance in the global arena. The framework is also used to annually assess the capabilities of 30 of the world's most powerful global organizations from the intergovernmental, non-governmental, and corporate sectors to be accountable to civil society, affected communities, and the wider public (The Global Accountability Report). This framework became a reference for transnational actors as shown, for example, by the

[512] *Ibidem*

[513] Monica Blagescu, Lucy de Las Casas and Robert Lloyd, "Pathways to accountability, A short guide to the GAP framework", *One World Trust* (2005), available at: http://www.who.int/management/partnerships/accountability/PathwaysAccountabilityGAPFramework.pdf

"Accountability Frameworks in the United Nations System" study (2011) which takes this methodology as a basis to draft their own assessment methodology.[514]

The One World Trust defines accountability as: "[…] *the process through which an organisation makes a commitment to respond to and balance the needs of stakeholders in its decision-making processes and activities and delivers against this commitment*".[515] This definition emphasises the need for organisations to balance their response to accountability claims and prioritise between different stakeholder groups according to organisational missions and criteria such as influence, responsibility and representation. Importantly, an organisation must do this through a conscious, verifiable, transparent process, which, given the dynamics of external circumstances, needs to be repeated in a cyclical manner. This focus put on dialogue with stakeholders makes it highly relevant for the research conducted under PARIS.

In this context, accountability mechanisms are not approached as a mechanism of control but rather as a process for learning. "*Being accountable is about being open with stakeholders, engaging with them in an ongoing dialogue and learning from the interaction*".[516] According to One World Trust, "*first and foremost accountability is about engaging with, and being responsive to, stakeholders; taking into consideration their needs and views in decision-making and providing an explanation as to why they were or were not taken on board*."[517] The ultimate goal of accountability mechanisms is to generate ownership of decisions and projects and to enhance the sustainability of activities.

4.2.1.1 Criteria to Operationalize Accountability

The Global Accountability Framework provides guidance to organizations on how to operationalize this understanding of accountability.[518] Five dimensions should be taken into account when designing accountability mechanisms: the accountability strategy, transparency, participation, evaluation, and complaint and response mechanisms.

The Accountability Strategy dimension refers to methods that allow the leadership of the organisations to effectively guide and manage the organisation's approach to accountability.[519] In the other four dimensions, two main aspects are taken into account: policies and systems. "Policies" refer to the documents or policies issued by an organization through which it makes a commitment to the value and principles of each of the other dimensions. They enable this organization to foster a consistent approach and they enable stakeholders to hold organisations to account for stated commitments. "Systems" refers to the management strategies and resources through which an organisation encourages, enables and supports the

[514] Mounir Zahran, Accountability Frameworks in the United Nations System, doc. JIU/REP/2011/52011, Geneva, 2011, available at: https://www.unjiu.org/en/reports-notes/JIU%20Products/JIU_REP_2011_5.pdf

[515] http://oneworldtrust.org/climategovernance/sites/default/files/publications/testmanager/OWT%20128%20-%20The%20Global%20Accountability%20Framework%202011.pdf

[516] Mark Bovens, *op. cit.*

[517] Monica Blagescu, Lucy. de las Casas, Robert Lloyd, *op. cit.*

[518] *Ibidem*

[519] *Ibidem*

implementation of the commitments made in policy or supports the issue more broadly. Indicators in this category include leadership, training and accessibility.[520]

To be deemed accountable, an organisation must integrate these five dimensions into its policies, procedures and practice, at all levels and stages of decision-making and implementation, in relation to both internal (e.g. staff) and external (e.g. policy makers) stakeholders. We describe each of these dimensions in turn, as understood by One World Trust.

The Accountability Strategy

The Accountability Strategy "*displays the awareness, extent of understandings and commitment to accountability relationships with recognised stakeholders*".[521] It provides evidence on the position of an organisation's ability to exercise leadership on accountability and related reforms. This includes the definition of the mission of the organization, the identification of the stakeholders to whom this organization is accountable as each of these is likely to have different expectations, and the different forms of responsiveness and accountability which can be inferred from these relationships.

As a way of example, in the 2012 The Global Accountability Report[522], the International Bank for Reconstruction and Development (IBRD), was found not to have an overarching accountability strategy. This is because while the IBDR seemed to have an understanding of whom its stakeholders are (as indicated through various internal documents) but the process of stakeholder mapping and prioritisation was very decentralised, with each department undertaking their own processes in this regard. This was interpreted as the IBRD not having a global perspective of its stakeholders and the mechanisms that are in place to deliver accountability to each stakeholder group.

Transparency

Transparency requires "*the provision of accessible and timely information to stakeholders and the opening up of organizational procedures, structures, and processes to their assessments*".[523] Doing so enables stakeholders to monitor an organisation's activities and hold it to account for its commitments, actions and decisions. Organisations benefit from transparency by avoiding challenges of secrecy and distrust in view of their public impact. Transparency for instance encompasses responsibilities to articulate the values, evidence and purpose of the organization.[524]

As a way of example, The World Bank's Policy on Access to Information (AI policy) scored quite high on this requirement (80%) as it was found to be broadly in line with best practice

[520] *Ibidem*

[521] Michael Hammer and Brendan Whitty, *Accountability principles for policy oriented research organisations. A guide to the framework and online database*, One World Trust, 2011.

[522] Michael Hammer, IBRD Accountability Assessment, Briefing, 20 July 2012, One World Trust, http://oneworldtrust.org/climategovernance/sites/default/files/publications/Michael%20Hammer/PEAGCCG%20IBRD%20Acc%20Assess%20summary%20briefing%20July%202012%20v3.pdf

[523] Michael Hammer and Brendan Whitty, *op. cit.*

[524] *Ibidem*

principles, and many of the management systems supporting the policy are also exemplary.[525] However, key weaknesses were identified such as the lack of formalization in the job descriptions of the responsibilities of key staff members tasked with implementing the AI policy are not formalised in their job descriptions, and the a lack of incentives to encourage staff to behave in an open and transparent manner.

Participation

Participation requires "*the active engagement of both internal and external stakeholders in the decisions and activities that affect them*". At a minimum, participation must include opportunities for stakeholders to influence decision making, and not just possibilities for approval or acceptance of a decision or activity. Participation strengthens ownership and buy-in for what organisations do by those they affect.[526]

As a way of example, the IBRD scored quite low (39%) in that matter.[527] While it does have Operational Policies (OPs) related to engagement with indigenous peoples, which meet many principles of best practice, policies of this type need to be extended to all priority external stakeholder groups. There are guidelines for engaging with civil society, but these were not been formalised as Bank policy.

Evaluation

Evaluation requires that the organization "*monitors and reviews its progress against goals and objectives, feeds learning from this into future planning, and reports on the results of the process*". Evaluation ensures that an organisation learns from and is accountable for its performance.

The IBRD scored reasonably high in that regard (70%).[528] The IBRD's evaluation policy and quality management systems meet many best practice principles, although it was found there was some room for improvement, particularly in terms of incentivising staff to reflect on and learn from evaluations. The IBRD's evaluation activities are carried out through staff monitoring and self-evaluations, and through the In-dependent Evaluation Group (IEG), which is an independent evaluation oversight body reporting directly to the Board of Executive Directors.

Complaint and Response Mechanisms

Complaints and response mechanisms require "*channels developed by organisations that enable internal and external stakeholders to file complaints on issues of non-compliance with the organisation's own policy frameworks or against its substantive decisions and actions, and which ensure that such complaints are properly reviewed and acted upon. Transparency, participation, and evaluation processes are used to minimise the need for complaint mechanisms. Complaint and response mechanisms are accountability processes of last resort but also a test for how serious organisations are about their accountability, and take interest in learning from their own mistakes*." This describes ways in which an organisation invites

[525] Michael Hammer, IBRD Accountability Assessment, *op. cit.*

[526] Michael Hammer and Brendan Whitty, *op. cit.*

[527] Michael Hammer, IBRD Accoutability Assessment

[528] *Ibidem*

feedback, comments and critique of its activities through a first party system. It captures how an organisation is answerable to its stakeholders.[529]

The IBRD scored reasonably high in that regard (66%). There are two channels through which external stakeholders can lodge complaints with the IBRD. The Inspection Panel (IPN) handles complaints (referred to as 'requests for inspection') from any person who believes that they may have been negatively impacted by IBRD or IDA activities. The Integrity Vice Presidency (INT) investigates allegations of fraud and corruption made by any stakeholder. The IBRD's policy in this dimension exhibits many elements of best practice, although the lack of stakeholder consultation on the policy is a key weakness. Similarly, some of the management systems in place, such as the quality management systems, are exemplary, whilst others, such as those relating to roles, responsibilities and leadership and building staff capacity, are weaker.

4.2.2 Accountability as a Mechanism of Control: Providing Trust, Fostering Compliance.

The narrow or passive sense of accountability refers to the fact for an organization to be called to account by some authority for its actions.[530] This second meaning of accountability should be understood as a mechanism of oversight by a third party over the activities of the accountor against a predefined set of standard behaviour. It fosters trust in the accountor's behaviour as long as it ensures the verifiability of the compliance of its activity against a pre-defined set of rules. It fosters compliance in that it is a *"process of transparent interaction in which that body seeks answers and possible rectification" .*[531] The narrow sense of accountability is often identified with the core meaning of the concept.

As stressed by Bovens[532], accountability is here seen as a social 'mechanism', "*as an institutional relation or arrangement in which an actor can be held to account by a forum*". Hence, the focus of accountability studies is not whether the agents have acted in an accountable way, but whether they are or can be held accountable ex post facto by accountability forums and on how accountability relationships operate.[533]

Within PARIS project, this second meaning of accountability will aim at assuring that system developers and operators have integrated the relevant privacy standards and requirements into the design and use of their surveillance systems. This process of accountability will thus aim at ensuring trust and compliance.

In this section, we first examine the core elements that should include any accountability mechanism. We then focus on the different dimensions that underlie any accountability relationships and which will have an influence on the way it will be operationalized.

---

529 Michael Hammer and Brendan Whitty, *op. cit.*

530 Colin Bennett, "International privacy standards: can accountability be adequate?", *Privacy Laws and Business International* 106 (August 2010): 21-23

531 *Ibidem*

532 Mark Bovens, *op. cit.*

533 *Ibidem*

4.2.2.1 Core Features of Passive Accountability

There is consensus that accountability in its narrow sense should comply with three main requirements:

- It should be external, i.e. it should involve a third party to whom the organization is being held accountable;
- This third party should have rights of authority of the organization being called to account, meaning that it can require the organization to give an account and to impose sanctions or ask for rectifications according to a predefined line of behaviour (a code);
- The process of accountability should involve a dialogue between the organization and the third party, i.e. the nature of the account given can be challenged and verified by the third party.

We examine these core features that should be included in any accountability process, distinguishing accountability from other close concepts such as responsibility, responsiveness, control or dialogue.

Accountability is external

The account should first be given to some other person or body outside the agent. This requirement is compatible with accountability procedures internal to an organization, i.e. to hold the staff liable for their actions based on internal codes of conducts. It however implies the existence of a relationship between the accountor and the accountee. It excludes any "self-accountability" mechanisms in which one is accountable to oneself only.

Accountability should thus in that sense be distinguished from "**responsibility**". As pointed out by Bennett, one can always act "responsibly" without reference to anyone else.[534] Responsibility is thus more related to the "*ethical territory of personal liability, freedom of action and discretion, that is to the more internal aspects of an organization's activity*".[535] Responsibility is left to cover the 'internal' functions of personal culpability, morality and professional ethics.[536]

Rights of authority

Accountability implies rights of authority of the third party to whom the account is given over the agent, in that those calling for an account are asserting rights of superior authority over those who are accountable, including the rights to demand answers and to impose sanctions.

This requirement first means that the actor is obliged to inform the forum about his or her conduct, by providing various sorts of data about the performance of tasks, about outcomes, or about procedures.[537] It also means that the forum may pass judgment on the conduct of the

[534] Colin Bennett, "International privacy standards …", *op. cit.*

[535] Robert Mulgan, "Accountability': An Ever-Expanding Concept?", *Public Administration* Vol. 78-Issue 3, (Autumn 2000): 555–573

[536] *Ibidem*

[537] Mark Bovens, *op. cit.*

actor. It may approve of an annual account, denounce a policy, or publicly condemn the behaviour of an official or an agency. In passing a negative judgment, the forum frequently imposes sanctions of some kind on the actor. The possibility of sanctions – not the actual imposition of sanctions - makes the difference between non-committal provision of information and being held to account. The actor may face consequences.[538]

Accountability is thus more than "responsiveness". The person to whom the entity is responsive has an option of choosing another entity and no right to demand that the private provider offer services that meet his or her perceived needs.[539] Responsiveness relates more widely to the organization compliance with stakeholders demands, for whatever motive. It relies on a voluntary process while accountability relies on a coercitive process where the accountee is being called to give an account by a third party which can require an answer and eventually impose sanctions.

Accountability mechanisms share the goal of **control mechanisms** in that it is grounded in the general purpose of making the accountor act in accordance with the wishes of the third party. The coercitive role of external pressure is pivotal. Accountability is however only one way to exercise control. In words of Mulgan[540], "*a reasonably clear distinction may still be maintained between accountability and control by which accountability remains merely one means, or set of means, for enforcing control, through the demand for explanation and the imposition of sanctions."* In that sense, Mulgan warned against the identification of accountability and control mechanisms: "*from this perspective, institutions of accountability include all institutions that are aimed at controlling or constraining government power, for instance legislatures, statutory authorities, and courts.*" Law itself should not be approached as an accountability mechanism as the legal accountability mechanism only refers to that part of the law which lays down enforcement procedures and which involves the existence of a dialogue (the provision of information upon request). It follows that only a few institutions, such as audit offices, ombudsmen and administrative tribunals, are properly described as 'institutions of accountability' because their primary function is to call public officials to account.

This is why legal scholars, within the debates revolving around the introduction of the principle of accountability into the data protection framework, have been very wary to warn against the risks of equating accountability with liability and have stressed the need to specify the value of the reports produced by accountability mechanisms in procedures engaging the liability of the actor.

Accountability involves a dialogue

Finally, accountability involves social interaction and exchange, in that one side, that calling for the account, seeks answers and rectification while the other side, that being held accountable, responds and accepts sanctions. Accountability thus implies a dialectical activity in that it involves an open discussion and debate about matters of public interest. "*Calling people to account means inviting them to explain and justify their actions within two competing logics,*

538 *Ibidem*

539 Robert Mulgan, *op. cit.*

540 *Ibidem*

that of consequences and that of appropriateness."[541] As stressed by Mulgan, "*even where apparently 'bare' information is sought, such as in financial accounting, the information will only make sense within an explanatory and justificatory framework assumed by the questioner and accepted, or contested, by the respondent. The various discourses of accountability, including assumptions of institutional and personal responsibility, are an important aspect of accountability and worth careful academic investigation*."[542]

Accountability does however not equate to dialogue as it is based on an authority relationship, thus on an unequal relationship between the agent and the third party calling into account. The agent is exposed to the possibility to be asked to take direction from the third party and to accept sanctions, if necessary for unsatisfactory performance.[543]

Understanding that the dialogue between the parties to the process is key for any accountability mechanism highlights the importance of the nature of account given. There needs to be a possibility for the forum to interrogate the actor and to question the adequacy of the information or the legitimacy of the conduct.[544] Raab points out that "*the account must also, and essentially, include descriptions and explanations of the actions*."[545] The account given pursues a series of objectives, namely:

- To enable the third party to better understand the organisations' intentions and its understanding, or theory, of its own situation or how it might act in it.
- To give visibility to the organization called into account's actions. As such actions are by nature invisible to the third party, they have to be re-presented, through stories or accounts, explanations, and justifications. Important here is what counts as information in the accountability process but also the "*possibility for the audience to have the means to redefine the concepts and categories in terms of which the account is expressed, to propose alternative perspectives, and to back these up with evidence that might not be found in the organization's own account. In turn, the audience must be able to defend its alternative through the same rules*."[546]

Raab concludes that "t*here is more to accountability than the production and receipt of an account as a proxy, in symbols, for the performance of the company in making things and in selling and so on-and in protecting personally identifiable information*".[547] Based on this analysis, Raab suggests some additional requirements to be looked upon when designing accountability procedures, namely:

- what the rules and procedures might be
- Whether they are rooted in data
- How they might be open to testing

[541] *Ibidem*

[542] *Ibidem*

[543] *Ibidem*

[544] Mark Bovens, *op. cit.*

[545] Charles Raabs, The Meaning of 'Accountability' in the Information Privacy Context, in Managing Privacy through Accountability, 15-32

[546] *Ibidem*

[547] *Ibidem*

- How they might be amenable to the sceptical search for alternative explanations
- Whether they invite dialogue with those who are not only an 'audience' but a constituency or a citizenry who are acted upon by the organization or, indeed, a government or a data controller, and for whom the action that is reported in the account is consequential".

4.2.2.2 Accountability Relationships

Understanding accountability mechanisms as social relations enables to classify them based on the dynamics driving the relations and thus to adjust its features when designing such mechanisms.[548]

Raab suggests approaching the concept of accountability through the one of stewardship, "*by which is meant that one party entrusts another with resources and/or responsibilities*".[549] To that end, he relies on the definition provided by Andrew Gray and William Jenkins which reads as follows: "*to be accountable is to be liable to present an account of, and answer for, the execution of responsibilities to those entrusting those responsibilities. Thus accountability is intrinsically linked to stewardship. Stewardship involves two manifest parties: a steward or accountor, that is, the party to whom the stewardship or responsibility is given and who is obliged to present an account of its execution, and the principal or accountee, that is, the party entrusting the responsibility to the steward and to whom the account is presented. There is however, a third party in this relationship: the codes on the basis of which the relationship is struck and by which it is maintained and adjudicated. Codes may be explicit or more often implicit*."

This approach seeks to make patent the rationale behind most accountability relationships, i.e. "*the allocation of responsibility or vesting of authority which occurs prior to the accountability relationship being established*". Accountability relationships do not stand on their own, but are instituted as "checks" against potential misuses of power by the accountor.

In that sense, the Office of the Auditor General of Manitoba has articulated accountability around two key elements: the conferring of responsibility and authority, and the answering for the use of that authority. According to this Office, "*Having responsibility means having the authority to act, the power to control and the freedom to decide. It also means that one must behave rationally, reliably and consistently in exercising judgment. Answering for the use of authority means reporting and explaining actions, assuming obligations, and submitting to outside or external judgement*."[550]

In order to understand the rationale underlying accountability relationships, three parameters should be taken into account: 1) the parties to the relation (who? To whom?), 2) the motivation driving the relation (why?) and finally 3) the nature of the account given (what?).

[548] Mark Bovens, *op. cit.* and R. Mulgan, *op. cit.*

[549] Charles Raabs, *op. cit.*

[550] Joseph Alhadeff, Brendan Van Alsenoy and Jos Dumortier, The Accountability Principle in Data Protection Regulation: Origin, Development and Future Directions, in *Managing Privacy through Accountability*, 49-82

Stakeholders (who? To whom?)

The first question to be asked is: ***who* should render account? Who is the *actor* required to appear before the forum**? In legal procedures, it is often the organisation as a corporate entity, which is held to give an account. We then talk about "corporate" or "organizational" accountability. This will be the case most often encountered in the SALT framework, therefore the one to which we will give priority.

The second question to answer is: to whom is the account to be rendered? This will yield a classification based on the type of forum to which the actor is required to render account. It could refer to political, legal, administrative or social accountability. This is a key question as this will usually define the type of authority the accountee has over the accountor and the kind of sanctions that can be imposed on the actors in case it is found to be in breach of the rules.

Motivation (Why?)

The motivation underlying the accountability relationship is also an important element to take into account when designing or assessing the accountability procedures in place. The question to be answered here is "***why* the actor feels compelled to render account"**. This relates largely to the nature of the relationship between the actor and the forum, and in particular to the question of why the actor has an obligation to render account. This will subsequently lead to classifications based on the nature of the obligation, for example obligations arising from a hierarchical or principal agent relationship, a contractual agreement, or which have been voluntarily entered into.

Nature of the account to be given (What?)

Finally, the last aspect to take into account is the nature of the account given. This aspect will allow to define the scope of the accountability relationship and thus to define the essential elements to be included into the account given. It will influence the elements to include into the report to be given and thus the content of the procedural mechanisms put in place by the accountor.

In that regard, Bennet makes a clear distinction between accountability mechanisms directed to policies, procedures and practices[551]:

- Accountability mechanisms focused on policies will look at the stated policy, compare it with what is said publicly by the organization (e.g. on its website), or in a code of practice, to a reference norm. It will mainly consist in an analysis of words.
- Accountability mechanisms focused on procedures will look at whether the organization have an effective complaint handling process, whether there is a responsible person or a dedicated management framework or staff training.
- Accountability mechanisms focused on practices will review whether the policies work in practice, whether they manage to achieve their goals.

4.2.3 Relevance for the SALT Framework: Criteria for Efficient Accountability Mechanisms

[551] Colin Bennet, *op. cit.*

Section 1 and 2 show that irrespective of whether accountability is approached from its broad sense as "answerability" or from its narrow sense as mechanism of control, both share common features that will shape accountability relationships. The main difference relies on whether the third party to whom the account is given owns rights of authority over the agent and thus whether the accountability process can end up in the imposition of sanctions or the agent been required to integrate corrections to its actions or decisions and in the value of such request. While in accountability process in the broad sense the impact of the whole process is largely defined by the agent itself, accountability processes in the narrow sense will end up in the agent having to enforce the decision of the third party with regard to the accountability mechanisms in place.

While, as will be elaborated in the next section, accountability is being introduced within the data protection framework in its narrow sense, as a way to ensure compliance, the broad understanding of accountability can still be of interest for the SALT Framework as far as decision-makers are concerned. It leads to a greater involvement of the stakeholders to the decision-making process.

As explained in Chapter 3, decision-makers -which in the data protection terminology will often be referred to as data controllers-, when deciding to implement a new surveillance system, will have to make a balance between security and privacy interests. As explained in chapter 3, this balance will most of the time result in carrying out a proportionality assessment which consists in a three-part test:

- the 'suitability' test, which defines whether the measure is reasonably likely to achieve its objectives;
- the 'necessity' test, which evaluates whether there are other less restrictive means capable of producing the same result;
- the proportionality test *stricto sensu*, which consists of a weighing of interests with which the consequences on fundamental rights are assessed against the importance of the objective pursued.

When applying these criteria to the specificities of their case, the deciders will necessarily need to engage with their stakeholders, e.g. to check their perceptions of privacy or their views on alternative means capable to achieve the same results.

As a way of example, a mayor who wants to reduce petty thefts in his city through the installation of a video surveillance system in the most affected areas could decide to engage into a dialogue with citizens, NGOs active in the field and security companies to obtain their views on the options taken and on acceptable alternative means in order to give more legitimacy to the final decision taken. In order to achieve this goal, the mayor will need to set up procedures that comply with the criteria explained above.

The design of accountability processes should thus start by defining the following elements:

1. **Identify the stakeholders**, i.e. whom the organization is answering to. Different stakeholders will have different expectations, generating different types of relationships and thus accountability processes should be adjusted to these different expectations. As a way of example, an accountability process directed to address citizens' concerns about the impact of a surveillance system on their right

to privacy will focus on the provision of assurance that a series of privacy safeguards have been taken into account into the design of the system. By contrast, an accountability process directed to involve citizens' in the decision of whether to implement a given surveillance system will rather tend to focus on the gathering and weighting of the different views of citizens in order to fully take them into account in the final decision taken. If the accountability processes is directed to provide a data protection authority with sufficient elements to check compliance with the applicable data protection framework, thus to the verifiability of the action taken by the agent in that perspective, the accountability process will tend to the production of evidence of compliance with such framework.

2. Make explicit the **motivation** underlying the accountability process, i.e. why the organization decides to engage into such procedure. A first reason can be that the organization is subject to the authority to which the account is given and thus is bound to its requests. Such is the case when an organization decides to self-certify to a standard or voluntarily code which implies regular audits by third parties or the possibility for the supervision authority to inspect the agent's practices in case of external complaint. Alternatively, the agent could seek to more largely involve its stakeholders in its activities in order either to give added-value to its products or greater legitimacy to its decisions.
3. Identify the **nature of the account** that should be given, i.e. what should be the content and extent of the accountability procedure. This last element relates to very object of the accountability relationship established between the accountor and the accountee. Coming back to the idea of conceiving accountability relationships as stewardship ones, this comes to defining which kind of responsibility or power has been entrusted to the agent and thus what this agent should be answerable for. As stressed above, this for instance can involve that the accountability mechanisms will bear exclusively on the policies drafted by the organization, on the procedures implemented to make these policies work in practice, or on the practices of the organizations against their accountability commitments.

Once the basic characteristic features of the accountability relationship have been clearly defined and identified, the methodology proposed by the Global Accountability Framework to set up accountability mechanisms can then be used as guideline. For the organization which wants to implement internally such accountability mechanisms or which want to be able to answer obligations stemming from an accountability relationships imposed externally, this means to set up:

- An **Accountability strategy** which identifies the stakeholders to the process, their expectations, the mission statement of the organization for this process (motivation/intentions) and the mechanisms put in place.
- **Transparency mechanisms** which gives visibility for the stakeholders of the actions taken in view of the obligation to give an account
- **Participation mechanisms** which allow stakeholders to involve into a dialogue with the organization, obtain the information required, ask further explanation, contest the narrative given by the agent.
- **Evaluation mechanisms** which allows the agent to obtain feedback over their own accountability mechanisms in view of further improvements
- **Complaint and response mechanisms**, which allows an interaction with their stakeholders, so they can provide feedback on the accountability process.

Whenever policy-makers, business organisations or others collective entities decides to integrate accountability mechanisms in the legislative framework, code of conducts or standards, they should keep in mind these different features to ensure that the proposed accountability mechanisms are actually able to meet their goals.

4.3 Implementing Accountability Within the Data Protection Framework

This section focuses on the principle of accountability as introduced and articulated in the data protection framework. The principle of accountability is not new to data protection. It was introduced in one of the first international data protection instruments in 1981, the OECD Guidelines on the protection of Privacy and Transborder Flows of Personal Data. However, it is only recently that this principle has gained renewed interest. It is seen as a way to improve trust in data governance practices and to apply data protection rules in a more efficient and less burdensome way. This section proceeds to a review of the different initiatives taken place in the data protection arena, to further extract meaningful criteria to be used in the SALT framework.

4.3.1 OECD Guidelines

The Fourteenth 1981 OECD Guidelines provides that "*A data controller should be accountable for complying with measures which give effect to the principles stated above*". Its role is to give effect in practice to all the other data protection principles.[552] It relies on the idea that the data processing activities are carried out in the benefit of the data controller, which is by way of consequence entrusted with a specific responsibility, the one of adequately protecting and handling the personal information subject to data processing. This responsibility is not waived when the data controller delegates part or all data processing activities to a third party. The explanatory memorandum lists for instance the need to hold the data controller liable for breaches of confidentiality obligations, to subject him to legal sanctions (legal liability) or to accountability mechanisms established by codes of conducts.

These guidelines however let to the participating countries the freedom to decide upon the best way to operationalize this principle into their legislative framework. It is also worth noticing that OECD Guidelines are primarily directed to international data flows.

4.3.2 The Madrid Resolution

Issued in 2010, the Madrid Resolution on International Standards adopted in 2009 at the International Conference of data Protection and Privacy Commissioners tries to undertake the task to agree on minimum data protection principles at international level. It is not aimed, as the OECD guidelines, to regulate international data flows but to promote a more internationally uniform approach to data protection.

[552] Joseph Alhadeff, Brendan Van Alsenoy and Jos Dumortier, *op. cit.*

Section 11 of the "Joint Proposal for a Draft of International Standards on the protection of Privacy with regard to the processing of Personal Data" introduces an Accountability principle. It provides that:

"*Accountability principle. The responsible person shall:*

a. *Take all the necessary measures to observe the principles and obligations set out in this Document and in the applicable national legislation, and*
b. *Have the necessary internal mechanisms in place for demonstrating such observance both to data subjects and to the supervisory authorities in the exercise of their powers […]"*

The concept of accountability is there closely linked to the one of (legal) compliance. It however goes further than the principle as worded in the OECD Guidelines imposing upon data controllers ("the responsible person") to implement internal mechanisms to demonstrate they are compliant. It is worth noticing that compliance should not only be demonstrated to supervisory authorities, which held supervision powers in terms of legal liability, but also to data subjects. This choice of words makes explicit the assumption on which data protection frameworks rely on, namely the transfer of power from the data subject to the data controller entailed by the transfer of personal information. Data controllers are answerable to the very entity conferring him such power, namely the data subject.

The Madrid International Standards goes one step further than the OECD Guidelines by including a list of measures aimed at promoting better compliance (Article 22), namely:

- The implementation of procedures to prevent, detect and react to data breaches,
- The appointment of one or more data protection or privacy officers,
- The periodic implementation of training, education and awareness programs among the members of the organization,
- The periodic conduct of transparent audits by qualified and preferably independent parties,
- The adaptation of information systems and/or technologies for the processing of personal data to the applicable laws on the protection of privacy with regard to the processing of personal data (privacy by design).
- The implementation of privacy impact assessments prior to implementing new information systems and/or technologies for the processing of personal data, as well as prior to carrying out any new method of processing personal data or substantial modifications in existing processing.
- The adoption of codes of practice the observance of which are binding and that include elements that allow the measurement of efficiency as far as compliance and level of protection of personal data are concerned, and that set out effective measures in case of non compliance.

4.3.3 APEC Privacy Framework

The Ministers of the Asia-Pacific Economic Cooperation adopted the APEC Privacy Framework in 2005 to both encourage the development of appropriate information privacy protections as well as to ensure the free flow of information within the Asia pacific Region. This framework is

largely based on OECD Guidelines. Its Preambule stipulates that "*data controllers should be accountable for complying with measures that give effect to the Principles*".

The Framework specifies what the principle of accountability should mean within the context of APEC data flows. Principle IX, par. 26, stipulates that domestic and international data transfers should be based on the consent of the individual or the data controller should exercise due diligence and take reasonable steps to ensure that the recipient person or organization will protect information consistent with the Principles.

The introduction of the principle was followed by more practical work undertaken in the context of the APEC Pathfinder projects.[553] The main objective of the Pathfinder projects is to develop a system that provides for "*accountable cross-border data flows within the APEC region*"[554] for the protection of consumers while facilitating business access to the benefits of electronic commerce. This goal is to be achieved by developing and implementing a Cross-Border Privacy Rules (CBPR) system, consistent with the APEC Privacy Framework.

The Pathfinder projects aims at building a system that allows businesses to create their own CBPRs and consumers and regulators to rely upon "accountability agents" in the APEC region to make sure businesses are held accountable to their privacy promises.[555] Accountability agents are any organisation that either certifies the compliance of business developed CBPRs with the APEC framework; and/or provides an efficient dispute resolution service to provide an avenue for consumers to address privacy complaints with business. An accountability agent may be a regulator, such as a privacy commissioner. The term also includes privacy trustmarks, which are already well established in a number of APEC economies, as well as other organisations, for example, government agencies or ministries that may be distinct from a regulator but which fulfils this role.

In order to operationalize such system, the Data Privacy Pathfinder project is still considering broader policy issues raised by the development of a CBPR system, most particularly in relation with the development of templates for businesses and the role of certification authorities, their recognition, their interaction with regulators and their integration within the policy framework.

4.3.4 The Accountability Projects

In 2009, the Center for Information Policy Leadership (CIPL), together with a number of Privacy enforcement agencies (European data protection authorities, the Japanese Consumer Affairs agency and the US Federal Trade Commission) and a series of experts from the private sector, NGOs and academia[556], launched a series of projects collectively referred to as 'the Accountability Projects'. As stressed by Alhadeff et al., "*these projects were initiated as a result*

[553] *Ibidem*

[554] APEC Data Privacy Pathfinder Projects Implementation Work Plan – Revised, Submitted by Australia, 2009/SOM1/ECSG/SEM/027, First Technical Assistance Seminar on the Implementation of the APEC Data Privacy Pathfinder, Singapore, 2009, http://www.apec.org/About-Us/About-APEC/Fact-Sheets/APEC-Privacy-Framework.aspx

[555] *Ibidem*

[556] Represent ants from companies such as Oracle, Google, Intel, HP, Microsoft, IBM or TRUSTe participated and from Privacy International for NGOs. The academic world was also represented.

of discussions on the topic of accountability which had taken place in the context of APEC and the International Conference of Data Protection and Privacy Commissioners".[557] The focus is on accountability as a mechanism for global governance of data.

The content of the different phases of the Accountability projects were driven by the concerns expressed by the different stakeholders in view of reaching a consensus on what it meant for an organization to be accountable[558], namely:

- Businesses expressed concerns about what might be expected of them in an accountability system, how their effort to meet these expectations would be measured and how the rules related to accountability would be defined and enforced
- Privacy enforcement agencies ask how accountability might work under local law, how do enforcement agencies measure an organisation's willingness and capacity to protect information when it is no longer in the privacy protection agency's jurisdiction, how does the agency work with and trust agencies in other jurisdictions
- Consumer advocates worry that accountability would lessen the individual's ability to make his own determination about appropriate use of information pertaining to him.

The project was thus articulated around three main questions[559]:

- What will be expected of companies in an accountability system?
- How will enforcement agencies monitor and measure accountability?
- How can the protection of individuals be ensured?

To the date of today, the project has been running into four phases each focusing on a specific aspect of an accountability-based system for data protection. First of all, the "Galway project" led by the Irish Data Protection Authority set out to define the essential elements of accountability, to consider the issues raised by stakeholders, and to suggest additional work necessary to establish accountability as a trusted mechanism for information governance; particularly in the context of global data flows. The "Paris project" hosted by the CNIL followed and went into further detail identifying common fundamentals of an accountable organization. The third Accountability project, the "Madrid project", was hosted by the Spanish Data Protection Commissioner. This project investigated more specific issues related the measurement and validation of accountability (e.g., costs of compliance, types of validation). The Fourth Accountability project, which took place in 2012, in view of the evolution of accountability into an accepted, practical approach to privacy and data protection (in the EU, Canada, OECD, APEC), set as goal the development of a tool that would assist organisations in evaluating the steps they have taken internally to establish the conditions for accountability and in demonstrating them to data protection authorities or their recognized third-party agents.

Accountability is defined as "*a demonstrable acknowledgement and assumption of responsibility for having in place appropriate policies and procedures, and promotion of good*

[557] Joseph Alhadeff, Brendan Van Alsenoy and Jos Dumortier, *op. cit.*

[558] The Centre for Information Policy Leadership (acting as secretariat to the Galway project), "Data Protection Accountability: The Essential Elements", October 2009, available at: http://www.huntonfiles.com/files/webupload/CIPL_Galway_Accountability_Paper.pdf

[559] *Ibidem*

practices that include correction and remediation for failures and misconduct."[560] The definition gathers the essential elements of the narrow concept of accountability in that an organization should commit to implement specific policies, procedures and practices for which it is answerable for failure and misconduct. Whom this organization is answerable to is not taken into the definition. The different options have however been further explored in the third phase of the project.

An accountability-based approach is seen as an "*infrastructure that fosters responsible decision-making, engenders answerability, enhances transparency and considers liability*."[561] An accountability-based approach to data protection is expected to promote the implementation of practical mechanisms and to translate legal requirements and guidance into effective protection for data.

The vision underlying these projects is thus not to redefine privacy or to replace existing laws and regulation but rather to "*shift the focus of privacy governance to an organisation's ability to demonstrate its capacity to achieve specified privacy objectives. It involves setting privacy protection goals for companies based on criteria established in law, self-regulation and best practice, and vesting the organization with both the ability and the responsibility to determinate appropriate, effective measures to reach those goals*."[562] Most particularly, it is aimed at compensating situations where data subjects cannot exercise an effective control over data use as "*accountability requires that organisations make responsible, disciplined decisions about data use even in the absence of traditional consent*".[563]

The project expects that the adoption of an accountability-based approach will bring a strong added-value in the following areas[564]:

- **Greater flexibility** in the implementation of data protection framework as long as it is expected to allow the organization to adapt its data practices to serve emerging business models and to meet consumer demands. Allowing for greater flexibility will enable organisations to more effectively conserve scare resources allocated to privacy protection.
- **Bridging disparate regulatory systems**. Accountability relies less on the rule that exist where the data is processed and more on where the obligation is first established. It is expected to help bridge approaches across disparate regulatory systems by allowing countries to pursue common data protection objectives through very different – but equally reliable- means. It will also heighten the confidence of individuals that their data will be protected wherever it is located.

[560] The Centre for Information Policy Leadership (acting as secretariat to the Paris project), Demonstrating and Measuring Accountability, Accountability Phase II – The Paris Project, October 2010, available at: http://www.huntonfiles.com/files/webupload/CIPL_Accountability_Phase_II_Paris_Project.PDF

[561] *Ibidem*

[562] The Centre for Information Policy Leadership (acting as secretariat to the Galway project), "Data Protection Accountability: The Essential Elements, *op. cit.*

[563] *Ibidem*

[564] The Centre for Information Policy Leadership , "Accountability: data governance for the evolving digital marketplace", 2011, available at: http://www.huntonfiles.com/files/webupload/CIPL_Centre_Accountability_Data_Governance_Paper_2011.pdf

- **Introduction of a risk-based approach**. Accountability relies less on specific rules but instead requires that organisations adopt policies that align with external criteria found in law –generally accepted principles and best practices – and foster a level of data protection commensurate with the risks to individuals raised by loss or inappropriate use of data. The risks should be assessed and measured based on guidance from regulators, advocates, individuals and other members of industry. It will raise the quality of data protection, by allowing use of tools that best respond to specific risks and facilitating the rapid updating of those tools to respond quickly to new business models and emerging technologies.
- **Shift of the primary responsibility for data protection from the individual to the organization collecting and using data**. An accountability-based approach is a proactive approach as long as accountability does not wait for system failure, rather it requires that organization be prepared to demonstrate upon request by the proper authorities that is securing and protecting data in accordance with the essential elements.

4.3.4.1 Data Protection Accountability: the Essential Elements

The first Accountability project focused around the fundamental question of how an accountability-based system might be designed in view of the establishment of accountability as a practical and credible mechanism for information governance.

The Galway project found out that for an organization to implement accountable data governance practices, five essential elements should be present. These essential elements articulate the conditions that must exist in order that an organisation establishes, demonstrates and tests its accountability[565]:

1. **Organisation commitment to accountability and adoption of internal policies consistent with external criteria**. An organization must implement policies linked to appropriate external criteria (found in law, generally accepted principles or industry best practices) and designed to provide the individual with effective privacy protection, deploy mechanisms to act on those policies and monitor those mechanisms. They must be approved at the highest level of the organization and performance against those plans at all levels of the organization must be visible to senior management. Important is to allocate sufficient and appropriate staff and to obtain the review and endorsement by members of the organisation's executive committee or board of directors.

2. **Mechanisms to put privacy policies into effect, including tools, training and education**. The organization must establish performance mechanisms to implement the stated privacy policies. Such mechanisms might include tools to facilitate decision-making about appropriate data use and protection, training about how to use those tools and processes to assure compliance for employees who collect, process and protect information.

[565] The Centre for Information Policy Leadership (acting as secretariat to the Galway project), "Data Protection Accountability: The Essential Elements", *op. cit.*

3. **Systems for internal, ongoing oversight and assurance reviews and external verification**. Using risk management analysis, enterprises that collect and use personal information must monitor and measure whether the policies they have adopted and implemented effectively manage, protect and secure the data. It is argued that accountable organisations have traditionally established performance systems based on their own business culture. In that sense, the project highlights a series of characteristics that ensure successful performance systems:
    - they are consistent with the organisation's culture and integrated into business processes
    - they assess risks across the entire data life cycle
    - they include training decision tools and monitoring
    - they apply to outside vendors and other third parties to assure that the obligations that come with personal data are met no matter where data is processed
    - they allocate resources where the risk to individuals is greatest
    - they are a function of an organisation's policies and commitment.

The organization should also periodically engage or be engaged by the appropriate independent entity to verify and demonstrate that it meets the requirements of accountability (internal audit department, assessment by privacy enforcement or third-party accountability agents provided external verification is trustworthy and affordable).

4. **Transparency and mechanisms for individual participation**. Successful communications provide sufficient transparency such that the individual understands an organizations data practices as he or she requires (through privacy notices, icons, videos and other mechanisms).

5. **Means for remediation and external enforcement.** They are means to address harm to individuals caused by failure of internal policies and practices. An individual should be appointed to serve as first contact point. Organisations must establish processes by which those complaints are reviewed and addressed.

4.3.4.2 Demonstrating and Measuring Accountability

The second phase of the project focused on fundamental conditions that accountable organisations should be prepared to implement and demonstrate to regulators.[566] It further considered how and under what circumstances organisations would measure accountability by introducing the concept of "validated accountability".

Design of an accountability program

Accountability requires that an organization stands ready to demonstrate its program if asked to do so by a data protection authority. The Accountability project identified nine common fundamentals that an accountable organisation should be prepared to implement and demonstrate to a regulator. Such fundamentals should however be applied in a flexible way

[566] The Centre for Information Policy Leadership, Demonstrating and Measuring Accountability, Accountability Phase II, *op. cit.*

and tailored to the organization business model, data holdings, technologies and applications and the risks to privacy they raise for individuals.[567]

The applicability of the fundamentals will depend on two main questions that each organization should answer before putting in place an accountability-based approach, mainly for what and to whom the organization is accountable.[568]

Organisation can be accountable for (what?):

- Existing law and regulation
- Private sector oversight programs
- Privacy promises
- Ongoing risk assessment and mitigation

Organisation can be accountable to different stakeholders (whom?):

- Individuals who expect their data to be secured and to be used and managed responsibly
- Regulators who require that organisations comply with applicable law and regulation
- Business partners.

Based on the "what" and "whom" questions, the design of the accountability program can take into account all or several of the nine elements identified below[569]:

1. **Policies.** Existence of binding and enforceable written data privacy policies and procedures that reflect applicable laws, regulations and industry standards
2. **Executive oversight.** Internal executive oversight and responsibility for data privacy and protection
3. **Staffing and delegation.** Allocation of resources to ensure that the organisation's privacy program is appropriately staffed by adequately trained personnel
4. **Education and awareness.** Existence of up-to-date education and awareness programs to keep employees and on-site contractors aware of data protection obligations
5. **Ongoing risk assessment and mitigation**. Implementation of a process to assist the organization understanding the risks to privacy raised by new products, services, technologies and business models and to mitigate those risks.
6. **Program risk assessment oversight and validation**. Periodic review of the totality of the accountability program to determine whether modification is necessary
7. **Event management and complaint handling**. Procedures for responding to inquiries, complaints and data protection breaches
8. **Internal enforcement**. Internal enforcement of the organisation's policies and discipline for non-compliance
9. **Redress**. The method by which an organization provides remedies for those whose privacy has been put at risk.

General vs. validated accountability

[567] *Ibidem*

[568] *Ibidem*

[569] *Ibidem*

This project also introduces a distinction between "general accountability" and "validated accountability". While general accountability will cover programs implemented by organizations in view of improving their data governance in general, "validated accountability" involves the will of an organisation to be recognized and validated as accountable.

Validated accountability refers to the certification of an organization's practices. Several reasons could ground such wish: to engage into certain activities, to make certain assertions or to be relieved of certain regulatory requirements (if provided as such by the regulatory framework). As a way of example, it is suggested that validated accountability could bring recognized qualification to engage in cross-border data transfer and data teaming, relief from specified administrative requirements, recognized Binding Corporate Rule status, mitigation of enforcement sanctions when appropriate.[570] In such case, more formal review and measurement by a supervisory authority or a third-party accountability agent recognized by the supervisory authority may be required.

More concretely, the project identified different stages in the measurement of an organisation's accountability program. These may or may not occur sequentially but represent an ongoing process of education, risk assessment, self-certification, review and enforcement:

1. The organization takes appropriate measures to establish processes and procedures that implement its privacy policies
2. The organization self-certified that it meets the requirements of accountability
3. The supervisory authority or recognized accountability agent reviews such filings and provide some form of acceptance of the certification
4. The organization submits to enforcement by the supervisory authority or recognized accountability agent
5. Supervisory authorities, recognized accountability agents, trade associations and government agencies engage in raising the awareness of organizations about the obligations that an accountable organization must meet, and the benefits that flow from being accountable.

4.3.4.3 Issues Pending of Resolution

At the end of the Galway[571] and Paris projects[572], a series of pending issues were identified as pivotal to encourage roust adoption of an accountability-based approach:

- Policy makers and stakeholders should address questions about **how accountability would work with existing legal regimes** and whether reinterpretation or amendment of existing laws might be required to make it possible to hold organization accountable.
- Stakeholders must also articulate the way in which the **credibility of third party accountability programmes** is established and tested for them to supplement the work of government agencies, most particularly how accountability is measured to ensure meaningful oversight. This means to define 1) how will remediation work in

[570] The Centre for Information Policy Leadership, "Accountability: data governance for the evolving digital marketplace, *op. cit.*

[571] The Centre for Information Policy Leadership, "Data Protection Accountability: The Essential Elements", *op. cit.*

[572] The Centre for Information Policy Leadership, "Demonstrating and Measuring Accountability*", op. cit.*

an accountability approach, 2) how do organisations determine the appropriate validation mechanisms and 3) on what basis are third-party accountability agents recognized.

- Finally, small- and medium-sized enterprises that wish to demonstrate accountability will face specific challenges that must be addressed such as questions of **scalability**.

In the following sections, we will see how and to what extent the work carried out under the Accountability projects has influenced the debates revolving around the deployment of an accountability-based approach in the EU and Canadian legal frameworks. Works under the Accountability projects have been concomitant to policy discussions around the introduction of the accountability principle in the EU data protection framework, and to its specification into detailed guidelines in Canada. As mentioned above, Canadian and European privacy enforcement authorities have taken an active part to the Accountability projects.

4.3.5 Canada: PIPEDA

Canada is, to the best of our knowledge, the first country to have introduced explicitly an accountability principle into its legislative framework and to have started to operationalize the principle. The Personal Information Protection and Electronic Documents Act (PIPEDA) sets out ground rules for how private sector organizations may collect, use or disclose personal information in the course of commercial activities. PIPEDA also applies to federal works, undertakings and businesses in respect of employee personal information.

4.3.5.1 The Principle of Accountability in PIPEDA

The Personal Information Protection and Electronic Documents Act (PIPEDA) adopted in 2000 introduces as first data protection principle, the accountability principle. "*The accountability principle has been interpreted as requiring responsible organizations to take all reasonable steps to protect personal information under their control, regardless of where it is processed… In particular, organization are considered to remain responsible for the actions by third parties to whom the data has been transferred*".[573] In words of Alhadeff et al, "*the obligation flows with the information*".[574] The offices of the Privacy Commissioner of Canada, Alberta and British Columbia acknowledged Accountability in relation to privacy as the acceptance of responsibility for personal information protection.[575] For an organization to be accountable, "*it must have in place appropriate policies and procedures that promote good practices which, taken as a whole, constitute a privacy management program. The outcome is a demonstrable capacity to comply, at a minimum, with applicable privacy laws."*[576] Organizations are responsible for both personal information in its possession or custody and when such information is transferred to a third party who will process information on their behalf. In the latter case, organisations are

[573] Jospeh Alhadeff, Brendan Van Alsenoy and Jos Dumortier, *op. cit.*

[574] *Ibidem*

[575] Office of the Information and Privacy Commissioner of Alberta, Office of the Privacy Commissioner of Canada, Office of the Information and Privacy Commissioner for British Columbia, Guidelines: Getting Accountability right with a Privacy Management Program, 2012, available at: http://www.priv.gc.ca/information/guide/2012/gl_acc_201204_e.asp#e

[576] *Ibidem*

expected to exercise due diligence "*in choosing third parties who will process information on their behalf and to negotiate sufficient contractual safeguards, including audit rights, to ensure a comparable level of protection"*.[577]

But not only does the PIPEDA introduces a principle of accountability, it also identifies a variety of measures that responsible organisations must implement in order to comply with the principle of accountability. Clause 4.1 of Schedule 1 requires organisations to designate one or more individuals who shall be accountable for the organisation's compliance. This individual will be both responsible for the internal oversight of information practices but also to act as a point-of-contact towards external parties.

More concretely, art. 4.1.4. of Schedule 1 mandate organizations to implement policies and practices to give effect to the principles, including (a) implementing procedures to protect personal information; (b) establishing procedures to receive and respond to complaints and inquiries; (c) training staff and communicating to staff information about the organization's policies and practices; and (d) developing information to explain the organization's policies and procedures.

4.3.5.2 Privacy Management Programs

In 2012, the Offices of the Privacy Commissioners of Canada, Alberta and British Columbia have issued guidelines for organisations to implement Privacy Management programs.[578] Setting up a sound Privacy Management program is seen as a way to "get accountability" right and thus to comply with PIPEDA obligations in that regard. It is expected that "*with a solid privacy management program, organizations will be able to identify their weaknesses, strengthen their good practices, demonstrate due diligence, and potentially raise the protection of personal information that they hold to a higher level than the bare minimum needed to meet legislative requirements*".[579]

This document puts forward a series of benefits for organisations when developing and deploying a Privacy Management Program:

- **Ensure compliance**
- **Foster a culture of privacy throughout an organization**. As explained by the Commissioners, senior management support is vital in that it provides the needed resources to ensure appropriate training and education, risk assessment and monitoring, and auditing. It also sends a clear signal that privacy is vital to the organization. In turn, a culture of privacy encourages employee support and reinforces the privacy protections the organization puts in place.
- **Enhance trust and companies' reputation** towards their customers and clients
- **Optimize business processes**. In the longer term, a privacy management program that is scaled to the organization's needs is expected to save money and make good business sense.

[577] Joseph Alhadeff, Brendan Van Alsenoy and Jos Dumortier, *op. cit.*

[578] Guidelines: Getting Accountability right with a Privacy Management Program, *op. cit.*

[579] *Ibidem*

- Minimize privacy breaches as privacy breaches are expansive for organizations both in terms of "clean up" and reputation repair

Privacy Management Programs are formed of three building blocks: 1) Organizational Commitment, 2) Program controls and 3) Maintenance of the Privacy Management program.[19]

1. **Organizational commitment**, i.e. development of an internal governance structure that fosters a privacy respectful culture. Not only should an organization develop program control to ensure compliance with the laws, but also to have a governance structure in place, with processes to follow and the means to ensure that they are being followed. This is what was referred to in the first part of this deliverable as an Accountability strategy. Concretely, this entails:
    - **Buy-in from the top**, i.e. Senior management support is key to a successful privacy management program and essential for a privacy respectful culture. Senior management needs to actively champion the privacy program. It should:
        - appoint the privacy point person(s) (Privacy Officer);
        - endorse the program controls; and
        - monitor and report to the Board, as appropriate, on the program.
        - Allocate sufficient resources
    - **Privacy Officer**, i.e. Organizations must appoint someone who is responsible for the privacy management program. In large organizations, the Privacy Officer may need to be supported by a Privacy Office with dedicated staff. He/She will:
        - establish and implement program controls;
        - coordinate with other appropriate persons responsible for related disciplines and functions within the organization;
        - be responsible for the ongoing assessment and revision of program controls;
        - represent the organization in the event of a complaint investigation by a privacy commissioner's office; and
        - advocate privacy within the organization itself
    - **Reporting**, i.e. Reporting mechanisms need to be established, and reflected in the organization's program controls. The organization needs to establish internal reporting mechanisms to ensure that the right people know how the privacy management program is structured and whether it is functioning as expected. Organizations should establish some form of internal audit and assurance programs to monitor compliance with their privacy policies. There will be times when privacy issues need to be escalated, for example, when there is a security breach or when a customer complains. Escalation means both involving people of relevant responsibility and ensuring that all the needed persons in the organization are included in the resolution of the issue. To ensure that related processes are being followed, organizations will need to monitor whether the needed steps are being taken when triggered. An effective reporting program:
        - clearly defines its reporting structure (in terms of reporting on its overall compliance activities) as well as employee reporting structures in the event of a complaint or a potential breach;

- tests and reports on the results of its internal reporting structures; anddocuments all of its reporting structures.
- documents all of its reporting structures

2. **Program controls.** These help ensure that what is mandated in the governance structure is implemented in the organization.
    - **Personal Information Inventory.** An organization needs to know what personal information it holds, how it is being used – and whether it really needs it at all. Every organization needs to determine:
        - what personal information it holds and where it is held (within the organization or by third parties, for example) and document this assessment;
        - why it is collecting, using or disclosing personal information and document these reasons; and
        - the sensitivity of the personal information it holds.
    - **Policies.** Organizations must develop and document internal policies that address obligations under the law. These policies need to be available to employees, and employees need to periodically sign off on them. These policies should be documented and should show how they connect to the applicable privacy legislation. Organizations should also incorporate privacy compliance requirements in other policies of the organization as appropriate. For example, in contract management policies, procurement policies, human resources policies and policies dealing with the disclosure of personal information to regulatory bodies, law enforcement agencies and internal security departments. The key policies that organizations must have in place are the following:
        - Collection, use and disclosure of personal information, including requirements for consent and notification;
        - Access to and correction of personal information;
        - Retention and disposal of personal information;
        - Responsible use of information and information technology, including administrative, physical and technological security controls and appropriate access controls;
        - Challenging compliance. Individuals have the right to challenge an organization's compliance with applicable privacy legislation. Organizations should therefore have internal policies in place for staff to follow in the event that individuals wish to complain about the organization's personal information handling practices
    - **Risk Assessment tools**. Privacy risks evolve over time. Organizations should develop a process for identifying and mitigating privacy and security risks, including the use of privacy impact assessments and security threat risk assessments.
    - **Training and education requirements**. A sound privacy management program requires all members of an organization to be aware of, and be ready to act on privacy obligations. Up-to-date training and education requirements for all

employees, tailored to specific needs, are key to compliance. For privacy training and education to be effective, it must:

- be mandatory for all new employees before they access personal information and periodically thereafter;
- cover the policies and procedures established by the organization;
- be delivered in the most appropriate and effective manner, based on organizational needs; and
- circulate essential information to relevant employees as soon as practical if an urgent need arises.

- **Breach and incident management response protocols**. Organizations should have a procedure in place and a person responsible for managing a personal information breach. For larger organizations, a collaborative approach may be required, with employees from different parts of the organization working together. Responsibilities for internal and external reporting of the breach must be clear.
- **Service providers management**. At a minimum, privacy requirements for service providers should include the following:
  - privacy provisions in contracts setting out requirements for compliance including binding the service provider to the policies and protocols of the organization and requiring the organization to be notified in the event of a breach;
  - training and education for all service provider employees with access to personal information;
  - sub-contracting;
  - audits; and agreements with service provider employees stating that they will comply with the organization's privacy policies and protocols.
- **External communication.** Organizations also have to develop a procedure for informing individuals of their privacy rights and the organization's program controls. This external communication should be clear and understandable and not simply a reiteration of the law. It should:
  - provide enough information so that the public knows the purpose of the collection, use and disclosure of personal information as well as how it is safeguarded and how long it is retained;
  - notify individuals if their personal information is being transferred outside of Canada;
  - include information on who to contact with questions or concerns; and
  - be made easily available to individuals.
  - Individuals should be made aware of their ability to access their personal information held by the organization, and how to request correction or to complain about the organization's privacy compliance, including the right to challenge the organization's actions by submitting a complaint to the Privacy Commissioner.

3. **Ensuring the maintenance of the Privacy Management Program** to ensure ongoing effectiveness, compliance and accountability. In order to properly protect privacy and

meet legal obligations, organizations must monitor, assess and revise their framework to ensure it remains relevant and effective.

- **Develop an Oversight and Review Plan.** An oversight and review plan will help the organization keep its privacy management program on track and up to date.
- **Assess and revise program Controls.** The effectiveness of program controls should be monitored, periodically audited, and where necessary, revised. Monitoring is an ongoing process and should address at a minimum the following questions:
    - what are the latest threats and risks?
    - are the program controls addressing new threats and reflecting the latest complaint or audit findings, or guidance of the privacy commissioners?
    - are new services being offered that involve increased collection, use or disclosure of personal information?
    - is training occurring, is it effective, are policies and procedures being followed, and is the program up to date?

The expectation is that an organization conducts assessments of its program controls in a focused, continuous and thorough manner. Based on the results of the assessment process, the Privacy Officer must consider whether to take action to update and revise the program controls. The role of Privacy Officers is key. In short, the following actions will need to be undertaken by the Privacy Officer:

- monitor and update personal information inventory continuously to keep it current and identify and evaluate new collections, uses and disclosures;
- review and revise policies as needed following assessments or audits, in response to a breach or complaint, new guidance, industry-based best practices, or as a result of environmental scans.
- treat privacy impact assessments and security threat and risk assessments as evergreen documents so that the privacy and security risks of changes or new initiatives within the organization are always identified and addressed.
- review and modify training and education on a periodic basis as a result of ongoing assessments and communicate changes made to program controls.
- review and adapt breach and incident management response protocols to implement best practices or recommendations and lessons learned from post-incident reviews.
- review and, where necessary, fine-tune requirements in contracts with service providers.
- update and clarify external communication explaining privacy policies.

4.3.6 The Data Protection Reform in the European Union

4.3.6.1 Opinion 3/2010 of Article 29 Working Party

In the context of the review of the EU Data Protection framework, Article 29 Data Protection Working Party put forward a proposal for the introduction of a principle of accountability.[580] This principle would require data controllers to put in place appropriate and effective measures to ensure that the principles and obligations set out in the new framework are complied with and to demonstrate so to supervisory authorities upon request.

More concretely, this Working Party suggested to wording the principle as follows:

> "*Article X – Implementation of data protection principles*
>
> 1. *The controller shall implement appropriate and effective measures to ensure that the principles and obligations set out in the Directive are complied with.*
> 2. *The controller shall demonstrate compliance with paragraph 1 to the supervisory authority on its request*."

This proposal is motivated by the fact that EU data protection principles and obligations are often insufficiently reflected in concrete internal measures and practices. This Working Party fears that "*unless data protection becomes part of the shared values and practices of an organization, and responsibilities for it are expressly assigned, effective compliance will be at considerable risk, and data protection mishaps are likely to continue*." The deployment of accountability mechanism is thus seen as a means to ensure compliance with the legal framework.

Article 29 Working Party thus approaches the principle of accountability from its narrow sense. Accountability is approached from the perspective of showing "*how responsibility is exercised and making this verifiable".*[581] Trust is an important element of accountability mechanisms because "*only when responsibility is demonstrated as working effectively in practice can sufficient trust be developed*."[582] Focus is therefore put on the measures which should be taken or provided to ensure compliance in the data protection field.[583]

As proposed in the Opinion, the legal architecture supporting accountability mechanisms would comprise two levels:

1. **A basic statutory requirement** binding upon all controllers and which would consist in the implementation of measures/procedures and the maintenance of evidence thereto. The legal text would however not specify the types of measures to be implemented which should be the object of subsequent guidance given by national data protection authorities, by the Article 29 Working Party or by the Commission only for certain specific cases. However, while not contained in the proposal it is also envisaged to include an illustrative lists of measures that could be implemented by data controllers to comply with this

[580] WP173, *op. cit.*

[581] WP173, §21

[582] *Ibidem*

[583] *Ibidem*, §23

mandate, providing them with an indicative toolbox.[584] Another alternative would consist in the assignment of clear internal responsibilities within each organization and the training of staff involved in the processing operations, such as the appointment of a Data Protection Officer as contemplated in article 18 of the 95/46/EC Directive. Finally, controls of the effectiveness of the measures taken should be organized by the data controller through monitoring, internal and external audits.

2. **Voluntary accountability systems** that go above and beyond the minimum legal requirements by providing higher safeguards than those required under the applicable rules or by implementing requirements that provide a higher effectiveness. In that sense, Binding Corporate Rules are seen as providing a first example of accountability-based mechanism.

One main concern of the Article 29 Working Party is to word the principle of accountability in such a way as to provide legal certainty, while at the same time allowing for scalability, i.e. "*enabling the determination of the concrete measures to be applied depending on risk of the processing and the types of data processed*." This means that the wording of the principle should be precise enough as to give sufficient guidelines to data controllers when translating the principle into their information practices, but at the same time it should be broad enough as to allow its implementation to take into account the specifics of the data controller and of the data processing activities. Based on the criteria used to define security measures prescribed by article 17 of the Directive 95/46, tailoring the measures to be implemented would include aspects such as the size of the data processing operation/s, the intended purposes of the processing and the number of envisaged data transfers may determine the level of risk, the type of data, including whether they are sensitive or not. Indeed, the same measures cannot be preconized for health data processing activities and the ones motivated by the follow-up of customers' purchases, or for video surveillance systems and the management of associations' memberships. Similarly, Article 29 Working Party suggests using as criteria to assess the effectiveness of the measures implemented a) the risks of the data processing activity and b) the nature of the data processed.

Examples of common accountability measures are provided as a way of example, namely:

• Establishment of internal procedures prior to the creation of new personal data processing operations (internal review, assessment, etc);

• Setting up written and binding data protection policies to be considered and applied to new data processing operations (e.g., compliance with data quality, notice, security principles, access, etc), which should be available to data subjects.

• Mapping of procedures to ensure proper identification of all data processing operations and maintenance of an inventory of data processing operations,

• Appointment of a data protection officer and other individuals with responsibility for data protection;

• Offering adequate data protection, training and education to staff members. This should include those processing (or responsible for) the personal data (such as human resources directors) but also IT managers, developers and directors of business units. Sufficient resources should be allocated for privacy management, etc.

[584] *Ibidem*, §42

• Setting up of procedures to manage access, correction and deletion requests which should be transparent to data subjects;

• Establishment of an internal complaints handling mechanism;

• Setting up internal procedures for the effective management and reporting of security breaches;

• Performance of privacy impact assessments in specific circumstances;

• Implementation and supervision of verification procedures to ensure that all the measures not only exist on paper but that they are implemented and work in practice (internal or external audits, etc)

Legal certainty is expected to be provided through the issuance of guidelines and the development of a *model data compliance program* which could be used by medium and large data controllers as a baseline upon which to draft their particular programs, a methodology already used for BCRs. In addition, certification schemes are seen as a tool to give data controllers assurance with regard to the adequacy of the accountability mechanisms put in place. This is however only possible if Data Protection Authorities can act over such certification scheme, either as "certifier of certifier" or by issuing enforceable models or referentials.

Article 29 Working Party also suggests to develop a reflection on the need to impose certain obligations to the data processor or to the designers and/or manufacturers of ICT (information and communication technologies) could also be developed at the light of this accountability principle.

This Working Party finally briefly touches upon the relation between accountability mechanisms and legal compliance to clearly separate both notions. Failure to implement adequate accountability mechanism should be subject to sanction, irrespective of the possibility to impose sanction for the violation of other data protection principles. It is argued that having implemented the required accountability mechanisms does not necessarily mean that a data controller complies with the substantive principles set forth in the Directive, i.e., it does not offer a legal presumption of compliance nor does it replace any of those principles. Accordingly, adopting measures to observe the principles must not in any case exclude data controllers from being subject to enforcement actions by data protection authorities. However, the Article 29 Working Party opens the door to the possibility that, when assessing sanctions related to data protection violations, data protection authorities could give weight to the implementation (or lack of it) of measures and their verification.[585] For this system to work, data protection Authorities should also be empowered to give precise instructions to data controller over their compliance systems. As explained above, this is an important part of any accountability relationship.

[585] *Ibidem*, §38

4.3.6.2 The EC Communication "A comprehensive Approach on Personal Data Protection in the European Union"

Following the Article 29 Working Party, the EC identified in the 2010 Communication on "A comprehensive approach on personal data protection in the European Union"[586] the need to enhance data controllers' responsibility as a way to ensure more effective data protection. This means to spell out more clearly their obligations in the legal framework, including in relation to internal control mechanisms and cooperation with Data Protection Supervisory Authorities. The goal is to ensure that data controllers put in place effective policies and mechanisms to ensure compliance with data protection rules. The introduction of an accountability principle is approached as a way to achieve this goal.

In that sense, three lines of actions were defined:

- Mandatory appointment of independent Data Protection Officers and harmonization of the rules related to their tasks and competences;
- Obligation for data controllers to carry out a data protection impact assessment (hereafter, "DPIA") in specific cases, for instance, when sensitive data are being processed, or when the type of processing otherwise involves specific risks, in particular when using specific technologies, mechanisms or procedures, including profiling or video surveillance;
- Promotion of the use of PETs (Privacy Enhancing technologies) and the possibilities for the concrete implementation of the concept of "Privacy by Design", which means that "privacy and data protection are embedded throughout the entire life cycle of technologies, from the early design stage to their deployment, use and ultimate disposal"[587]

In addition, the EC wished to foster the establishment of EU certification schemes in the field of data protection("privacy seals") for "privacy-compliant" processes, technologies, products and services, a need already identified in the context of the fostering of Privacy Enhancing technologies[588], as a way to enhance data controllers' responsibility. The EC argues that by opting for certified technologies, products or services could help to prove that the controller has fulfilled its obligations. The trustworthiness of such privacy seals should be ensured and their relation with the legal obligations and international technical standards should then be defined.

4.3.6.3 Proposal for a Regulation

On 25 January 2011, the European Commission published a proposal for a Regulation of the on the protection of individuals with regards to the processing of personal data and on the free movement of such data (hereafter "Draft Regulation"). At the date of writing, the proposal is still awaiting the first reading of the European Parliament. Several Committees of the European Parliament have already tabled a long list of amendments, most notably contained in the so-

[586] Communication From The Commission, *A comprehensive approach on personal data protection in the European Union*, 2010, *op. cit.*

[587] Communication from the Commission to the European Parliament and the Council on *Promoting Data Protection by Privacy Enhancing Technology (PETs)* - COM(2007) 228)

[588] *Ibidem*

called Albrecht Report.[589] The EDPS[590] and Article 29 Working Party[591] have also published their Opinion on the proposal. We however only will refer to those amendments that modify in a substantial way the content of the new provisions introduced in the Draft Regulation.

Accountability as general principle of the data protection framework

The Draft Regulation does not introduce an explicit principle of accountability as such but, in line with the EC Communication, it looks to enhance data controllers' responsibility and liability.

The Draft Regulation implements as general principle "a comprehensive responsibility and liability of the controller" which includes an obligation to demonstrate compliance with data protection rules. The Draft Regulation therefore introduces accountability in its narrow sense, i.e. as a way to ensure compliance with a set of rules, namely the principles set forth in the Regulation. Article 5 (f) states that:

> "[*personal data must be] processed under the responsibility and liability of the controller, who shall ensure and demonstrate for each processing operation the compliance with the provisions of this Regulation*."

This article should be read together with Recital 60 which stipulates that:

> *"Comprehensive responsibility and liability of the controller for any processing of personal data carried out by the controller or on the controller's behalf should be established. In particular, the controller should ensure and be obliged to demonstrate the compliance of each processing operation with this Regulation*"

The Albrecht report, following the recommendation of the EDPS[592], has tabled two amendments (40 and 97) to introduce an explicit reference to accountability in recital 60 and in the text of article 5 (f). It is worth noticing that the amendment to Recital 60 is intended to make clear that accountability only entails an obligation to be able to demonstrate compliance on request.

Measures tending to operationalize accountability

This general principle is further specified in a series of articles contributing to the implementation of the accountability principle in the data protection framework, namely:

1. **Adoption of policies and implementation of appropriate measures to ensure and be able to demonstrate compliance with data protection rules, and to ensure that the**

[589] European Parliament, Committee on Civil Liberties, Justice and Home Affairs, Draft Report on the proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)), doc num. PE501.927, 17 December 2012, available at: http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/pr/922/922387/922387en.pdf

[590] EDPS, Opinion on the data protection reform package, 7 March 2012, available at: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-03-07_EDPS_Reform_package_EN.pdf

[591] Article 29 Data protection Working Party, Opinion 01/2012 on the data protection reform proposals, 23 March 2012, WP 191.

[592] EDPS, Opinion on the Data Protection Reform Package, *op. cit.*, §160

effectiveness of the measures is verified (article 22(1) and (3)). Both the EDPS[593] and Article 29 Working Party[594] have stressed the importance to reflect into the text the need for scalability of this general obligation in practice.

These measures should include at minima:

- **Keeping documentation of all processing operations.** This obligation replaces the general obligation to notify individual processing operations to the supervisory authorities contained in the Directive 95/46. Article 28 provides a list of documentation that should be kept by data controllers which should be made available on request to the supervisory authority. It is worth noticing that this obligation also extends to data processors. While the EDPS[595] and the Article 29 Working Party expressed their doubts about the feasibility of the implementation of this obligation in an increasingly dynamic environment, the amendments (43 and 188) introduced in the Albrecht Report rather seek to merge this article with Article 14 which details the information to be provided to the data subject. This report considers that both articles are two sides of a same coin and such an approach would reduce administrative burdens for data controllers at the time it would make it easier for individuals to understand and exercise their rights
- **Implementing data security requirements**. Amendment 193 of the Albrecht Report proposes to extend the scope of the article from technical measures to procedures. The EDPS[596] made two additional suggestions which were not taken into account. First, the EDPS stressed the need to explicitly refer to the three basic principles of security, namely confidentiality, integrity and availability. Second, the EDPS contended that the Regulation should also oblige the controller to adopt an information security management approach within the organization, including the implementation of an information security policy specific to the data processing performed, where appropriate.
- **Performing data protection impact assessments.** DPIA are only mandatory where processing operations present specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes. A list of data processing operations considered as such is provided for by Article 33.2. This includes profiling, the monitoring of publicly accessible areas, especially when using video surveillance on a large scale and the processing of genetic or biometric data in large scale filing systems. The Albrecht Report follows the critics formulated by both the EDPS and Article 29 Working Party over the use of vague terms such as "large scale" and tables amendments to replace it by the following wording "*where personal data are made accessible to a large number of persons or if high volumes of personal data about the data subject are processed or combined with other data*". Another amendment also seeks to broaden the scope of application of this article by replacing the reference to video surveillance by a reference to "optic-electronic or other sensory devices".
- **Complying with requirements for prior authorization or prior consultation of the supervisory authority wherever relevant**. The Albrecht report suggests to

[593] *Ibidem*, §174

[594] WP191, p. 15

[595] EDPS, Opinion on the Data Protection Reform Package, *op. cit*., §190

[596] *Ibidem*, §193

extending this obligation by referring not only to the supervisory authority but also to Data Protection Officers (Amendment 171).

- **Designating a Data Protection officer (DPO).** Data controllers must appoint DPOs where the processing is carried out by a public authority or body; the processing is carried out by an enterprise employing 250 persons or more; the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects. The role of DPOs is to monitor internal compliance with the Regulation, monitoring the implementation and application of the policies and appropriate measures adopted by the controller.

In addition, the Albrecht Report introduces amendments directed to compel data controllers to publish a regular report of their activities (Amendment 174) and to establish transparent information and communication to and with the data subject (Amendment 172).

2. **Notification of security breaches** (Articles 31 and 32)

3. **Obligation to introduce the principles of data protection by design and by default in the design of new systems** (Article 23). Concretely, this article entails that data controllers shall implement appropriate technical and organizational measures and procedures in such a way that the processing will meet the requirements of the Regulation and ensure the protection of the rights of the data subject. Such mechanisms should ensure an effective application of the data minimisation principle, the purpose specification principle and include access-right controls. The Albrecht Report put forwards amendments to further specify the content of the article (Amendments 41, 177, 178, 98). Amendment 98 is worth noticing as it suggests to introduce in article 5 a new general principle that would require producers of automated data processing systems (i.e. hard- and software) to take into account the principle of privacy by design and by default, even if they do not process personal data themselves. This means elevating the principles of privacy-by-default and privacy-by-design to the rank of general data protection principles.

4. **EU certification mechanism and data protection seals and marks (**Article 39). Such schemes should allow data subjects to quickly assess the level of data protection provided by controllers and processors and contribute to the proper application of the Regulation, taking into account the specific features of the various sectors and different processing operations. The EC is furthermore authorized to lay down technical standards for certification mechanisms and data protection seals and marks and mechanisms to promote and to recognize certification mechanisms and data protection seals and marks. Several amendments (51, 237, 238) contained in the Albrecht report seeks to further specify the conditions and characteristics of such schemes.

4.3.6.4 Proposal for a Directive

On 25 January 2011, the European Commission published a proposal for a Directive on the protection of individuals with regard to the processing of personal data by competent

authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data (hereafter, the "Draft Directive"). At the date of writing, the proposal is still awaiting the first reading of the European Parliament. Several Committees of the European Parliament have already tabled a long list of amendments, most notably contained in the so-called Droustsas Report.[597] The EDPS[598], Article 29 Working Party[599] have also published their Opinion on the proposal. We however only will refer to these amendments in so far as they modify in a substantial way the content of the new obligations. We also highlight the differences between the text of January 2012 and the leaked text which circulated in November 2011 as the latest version considerably waters down the initial provisions relating to the accountability principle.

Likewise the Draft Regulation, the principle of accountability is not introduced as such but through a new general principle of comprehensive responsibility and liability of the data controller (Article 4 (f)), who should ensure compliance with the provisions of the Directive. The wording does not reflect the obligation to demonstrate compliance as was initially contained in the leaked text from November 2011. All references explicitly made to the principle of accountability and to the obligation to demonstrate compliance in the explanatory memorandum of the proposal have also disappeared in the proposal of January 2012. This is thus a lighter version of the principle of accountability which has been opted for. This has been heavily criticised by both the EDPS[600]and Article 29 Working Party[601] who called for the reintroduction of the provisions to make them consistent with the text of the Draft Regulation. The Droustsas report has put forward several amendments to reintroduce this obligation into the text of the Draft Directive (Amendments 24, 56 and 91).

This general principle is further specified in a series of articles contributing to the accountability principle in the data protection framework, namely:

- **Obligation to adopt policies and mechanisms for ensuring and demonstrating compliance** (Article 18) which include:
    - **Obligation for controllers and processors to maintain documentation of all processing operations under their responsibility**, instead of a general notification requirement to the supervisory authority (article 23)
    - **Keeping of records** (Article 24)
    - **Implementation of security requirements** (Article 27)
    - **Designating a Data Protection Officer** (Article 30)
    - **Requirements for prior consultation of supervisory authorities** (article 26)

[597] European Parliament, Committee on Civil Liberties, Justice and Home Affairs, "Draft Report on the proposal for a directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data", doc num. PE 501.928v02-00, 20 December 2012, available at: http://www.europarl.europa.eu/sides/getDoc.do?type=COMPARL&mode=XML&language=EN&reference=PE501.928

[598] EDPS, Opinion on the Data Protection Reform Package, *op. cit.*

[599] WP191

[600] EDPS, Opinion on the Data Protection Reform Package, §310

[601] WP191, p. 27

- **Notification of personal data breaches** (article 28) and to communicate, in qualified circumstances to the data subject (article 29)
- Member States must ensure the compliance of the controller with the obligations arising from the principles of **data protection by design and by default** (Article 19)

In this sub-section, we only focus on the outstanding differences between the Draft Regulation and the Draft Directive.

The general obligation of responsibility of the controller.

Article 18.1 only introduces the obligation for data controllers to adopt policies and to implement appropriate measures to ensure that the processing is performed in compliance with the provisions of the Draft Directive. This article does not contain any obligation to demonstrate compliance upon request. Again, this provision is a watered down version of the one contained in the leaked draft which not only included an obligation to be able to demonstrate compliance but also extended this obligation to the assignment of internal responsibilities and the training of staff involved in the processing operation.

Finally, it worth noticing that article 18 (former article 20) initially contained an obligation for data controller who publish a report (wherever this publication was voluntary or required by law) of its activities, that such report would contain the controller's policies in relation to the protection of personal data, the risks linked to data processing by the controller and the measures taken to mitigate such risks. Exception was provided in cases when such publication was likely to jeopardize the protection of public interests or the security of processing. This obligation has been deleted from the proposal published in January 2012.

Obligation to keep documentation

While the wording of the obligation to keep documentation is similar to the one included into the Draft Regulation, there is no obligation to maintain documentation on time limits for the erasure of the different categories of data, nor on the verification mechanisms implemented, as the obligation to be able to demonstrate compliance has been suppressed from the proposal.

The leaked text was much more comprehensive and included the obligation to keep documentation on two additional items:

- An indication of the parts of the controllers' or processor's organization entrusted with the processing of personal data for a particular purpose
- An indication of the legal basis of the processing operation for which the data are intended

The Amendments contained in the Droustsas report first seek to reintroduce the items that have been suppressed from the leaked draft (Amendments 99, 100, 101, 104) and to extend the obligation to keep documentation on information about (a) the existence of profiling, of measures based on profiling, and of mechanisms to object to profiling, (b) the logic involved in any automated processing, (c) transfers to third countries and the legal ground on which the data is transferred.

The Droustsas report also looks to widen the scope of the information to be provided to the supervisory authority, to the categories of data subjects and of personal data processed, and a general indication of time limits for erasure, as suggested by the EDPS[602].

Obligation to keep records

The Draft Directive imposes on data controllers to record all processing operations of personal data for purposes of verification of the lawfulness of the data processing, self-monitoring and for ensuring data integrity and data security. Records should be kept for at least the following processing operations: collection, alteration, consultation, disclosure, combination or erasure. These records should show the purpose, date and time of such operations and as far as possible the identification of the person who consulted or disclosed data.

The requirement to make this information available on request to the supervisory authority has been removed from the January 2012 proposal. The Droutsas report, following the EDPS recommendation[603], puts forward a specific amendment for its reintroduction (Amendment 107), completed by a new recital (Amendment 26). Finally, amendment 106 looks to introduce the obligation to record the identity of the recipient of such data (as was worded in the leaked text) and to suppress the nuance introduced by the use of the term “as far as possible”.

Implementation of data security requirements

Article 27 of the Draft Directive contains a list of measures to be implemented by data controllers or processors, following an evaluation of the risks of the processing. These measures should be designed to:

- deny unauthorised persons access to data-processing equipment used for processing personal data (equipment access control);
- prevent the unauthorised reading, copying, modification or removal of data media (data media control);
- prevent the unauthorised input of data and the unauthorised inspection, modification or deletion of stored personal data (storage control);
- prevent the use of automated data-processing systems by unauthorised persons using data communication equipment (user control);
- ensure that persons authorised to use an automated data-processing system only have access to the data covered by their access authorisation (data access control);
- ensure that it is possible to verify and establish to which bodies personal data have been or may be transmitted or made available using data communication equipment (communication control);

Amendment 114 and 115 of the Droutsas report foresees to align the text of the article with the one of the Draft Regulation and to extend this obligation to procedures and to data processors.

602 EDPS, Opinion on the Data Protection Reform Package, §394

603 *Ibidem*, §396

Prior consultation of the supervisory authority

The Draft Directive introduces an obligation of prior consultation of the supervisory authority for processing of personal data which will form part of a new filing system where sensitive data are processed and where the type of processing, in particular, using new technologies, mechanisms or procedures, holds otherwise specific risks for the fundamental rights and freedoms, and in particular the protection of personal data, of data subjects. Member States may provide for the supervisory authority to make a list of the data processing activities which should be subject to prior consultation.

The EDPS considers that the scope of the consultation procedure is too limited and should be aligned with the content of the Regulation[604]. However, taking into account that the scope of the obligation contained into the Regulation is based on the existence of DPIA which are absent from the text of the Directive, the EDPS suggests there should be an obligation for the controller or the processor to consult systematically the supervisory authority where a new processing operation is introduced in an existing filing system. In view of the EDPS, only an obligation to carry out a DPIA allows for the evaluation of risks and thus enables the assessment of whether prior consultation is required or not. The Droustsas report follows this recommendation and it tables two amendments in that sense (Amendment 28 and 111).

Initially, supervisory authorities had the obligation to make proposals to remedy potential incompliance with the provisions of the Directive and could be consulted in the preparation of a legislative measure to be adopted by the national parliament in order to ensure compliance and to mitigate the risks involved for data subjects. Both measures were deleted in the proposal of January 2012 and are reintroduced in Amendments 112 and 113 of the Droustas report.

Designating a Data Protection Officer

While the provisions relating to the appointment of Data Protection Officer were much more detailed in the leaked text, in line with with the text of the Draft Regulation, the proposal put forward by the European Commission in January 2012 was much more concise. The Droutsas report tables a series of amendments (amendments 119 to 122) to reintroduce the original text and to ensure consistency with the text of the Draft Regulation.

Data protection by design and by default

The obligation to implement appropriate technical and organizational measures and procedures in such a way that the processing will meet the requirements of provisions adopted pursuant to the Directive which initially mirrored the text contained in the Draft Regulation has also been watered down. The obligation is now limited to implement mechanisms for ensuring that, by default, only those personal data which are necessary for the purposes of the processing are processed (article 19.2). References to the data minimization principle are deleted, as well as the requirement to ensure that the data are not made accessible to an indefinite number of individuals, by default. Amendment 93 of The Droustsas report, following

[604] *Ibidem*, §403

the critics formulated by the EDPS[605] and Article 29 Working Party[606], looks to reintroduce these aspects.

Data Protection Impact Assessments

Finally, the provisions for performing mandatory data protection impact assessments contained in the leaked text of November 2011 have disappeared from the proposal submitted on the 25 January 2012. The EDPS[607] points out that there is absolutely no justification for such deletion, more particularly when the specific nature of the processing operations carried out by law enforcement authorities makes it even more necessary to carry out such impact assessment[608]. Such instrument further contributes to the practical implementation of the principles of "privacy by design" and "privacy by default". In that sense, Article 29 Working Party reminds that "*one aspect of privacy by design is determining the risks of processing early on in the process and being able to mitigate those risks*" and it urges to insert in the Directive provisions requiring a Data Protection Impact Assessment, including during the legislative procedure[609]. The Report Droustsas introduces a series of amendments that seek to reintroduce Data Protection Impact Assessments (Amendments 27, 92).

4.3.7 Relevance for PARIS: Preliminary Criteria to Design Accountability Mechanisms in the SALT Framework.

The review of these different initiatives revolving around the introduction of an accountability-based approach in the data protection framework shows how they all converge on a series of basic features that should base any accountability mechanisms. In that sense, the Accountability projects, while mainly addressed to private organizations to overcome the difficulties proper to cross-border data exchanges, is valuable in that it systematizes the essential elements. It thus provides a sound basis on which building the design of accountability-based systems.

This work should however be adjusted to the specifics of surveillance and it should be completed by studies carried out on privacy-by-design. As explained by Cavoukian et al, "*privacy by design and accountability go together like innovation and high productivity. You can have one without the other, but it is hard*."[610] While privacy-by-design and accountability are autonomous concepts that can operate independently, accountability relationships regulating data governance will greatly benefit from the tools provided by the privacy-by-design approach. Similarly, the privacy-by-design approach will surely develop more efficiently in a context where the organization is accountable to an external third party for its data governance policies, procedures and practices. In that sense these authors show how the seven principles of privacy by design drawn by Dr. Cavoukian can be linked to the essential elements of accountability

[605] *Ibidem*, §387-389

[606] WP191, p. 29

[607] EDPS, Opinion on the Data Protection Reform Package, §385

[608] *Ibidem*, §400

[609] WP191, p. 29

[610] Ann Cavoukian, Scott Taylor and Martin E. Abrams, "Privacy by Design: essential for organizational accountability and strong business practices", *Identity in the Information Society* vol. 3-issue 2 (August 201): 405-413, available at: http://link.springer.com/article/10.1007%2Fs12394-010-0053-z

identified by the Galway Project. Both approaches (accountability-based approach and privacy-by-design) share the same goals and characteristics:

1. They are both proactive not reactive; preventative not reactive.
2. They set privacy as the default
3. They seek to embed Privacy into the design of systems, procedures, policies
4. They tend to match the different interests at stake to reach a result which is a positive sum of all, not a zero sum. Both approaches allow for a better understanding of the risks to both the organization and to individuals.
5. They take an end-to-end lifecycle protection approach.
6. They aim at increasing visibility and transparency of data governance practices to individuals and other relevant stakeholders. The accountable organization stands ready to demonstrate that it is open about what it practices, stands behind its assertions and is answerable when questions arise.
7. Respect for User Privacy is at core of both approaches.

Within the data protection framework, accountability is approached as implementation and enforcement mechanism of existing legal obligations. This is probably the reason why the EU rather uses the terms “responsibility” and “liability” than the one of accountability. It is however still to be seen how this accountability-based approach will be articulated with traditional enforcement mechanisms and which role it could play in making the legal framework more flexible without reducing its efficiency. Questions such as the ones raised by the Accountability project about how accountability would work with existing legal regimes, how to establish the credibility of third party accountability programs and to ensure scalability for SMEs, remain pending of resolution. It is however already possible to draw the general features of the system to be incorporated to the European legal framework. This system relies on four main streams:

1. Adoption of policies and measures to demonstrate compliance with the rule which includes: keeping documentation of all data processing operations; implementing data security requirements; Data protection Impact Assessments; prior consultation/authorization of supervisory authorities; appointment of data protection officers
2. Notification of security breaches
3. Data protection by design and by default
4. EU certification mechanisms and data protection seals and marks.

As mentioned above, while, the introduction of the principles of data protection by design and by default does not generate accountability relationship, contrary to the other three streams, they however form important tools for the introduction of sound accountable data governance practices within an organization.

It is however too early to see how the accountability-based approach will be operationalized in practice. This becomes even more blurry when looking at the Draft Directive, applicable to law enforcement, which only contain a watered-down version of the accountability-based approach included into the Draft Regulation. It is however worth noticing that the approach taken by the European Union is likely to end up introducing within the legislative framework the principles of privacy by design as a core tool for the introduction of an accountability-based approach to data protection, even if not explicitly.

As regard the operationalization of the principle of accountability, the most accomplished work in the field is certainly the one performed in Canada where the principle of accountability is already and clearly introduced into the data protection framework. This principle is accompanied by an obligation of due diligence every time the data are transferred to third parties on behalf of the data controller. In addition, the legal framework contains the basic features of what an accountability-based approach should entail in the context of data processing operations (namely, to appoint "one or several individuals accountable for organizations' compliance –privacy officers; to implement policies and practices to protect personal information, procedure to handle complaints and inquiries, staff training and communication to explain policies and procedures). This has allowed the Canadian supervisory authorities to develop very specific and detailed guidelines to implement Privacy Management Programs. These guidelines not only integrate all basic elements identified in the Accountability projects but they also go further into the details of what should be a sound Privacy Management Program.

These guidelines are however not designed with surveillance practices in mind and while forming a valuable basis for the definition of criteria for the SALT framework, they should be adapted to the specifics of such technologies. As mentioned above, this issue will be dealt with in the next PARIS deliverable (D.2.2).

Based on the review of the initiatives which aim at introducing an accountability-based approach within the data protection framework, a series of preliminary criteria can be extracted for the design of accountability schemes.

Organisations willing to implement an accountability-based approach for their personal data governance will first need to identify clearly what they are accountable for and to whom. As mentioned above, organizations can be accountable for existing law and regulation, private sector oversight programs, privacy promises, ongoing risk assessment and mitigation. They can be accountable to different stakeholders such as individuals who expect their data to be secured and to be used and managed responsibly, regulators who require that organisations comply with applicable law and regulation and business partners. Answers to these questions will condition the scale and nature of the measures to be implemented in the Privacy Management Programs. Such Programs should be seen as a way for accountable organizations to ensure they are able to give account of their data governance policies, procedures and practices whenever requested. They are therefore called to play a core role in any accountability scheme or relationship

Privacy management Programs should be articulated around three main lines:

- **Policies and commitments.** Organizations should design and implement privacy policies and procedures to enforce them, which ensure compliance with the data protection framework and other obligations stemming from voluntary standards or contractual relationships. This also means to obtain high-level commitment to protect individual privacy (senior management support), to appoint someone who is responsible for the program (such as a Data Protection Officer), to ensure meaningful transparency mechanisms (i.e. to communicate clearly to stakeholders such as data subjects about

the content of the policies and procedure) and finally to show willingness to demonstrate capacity to uphold promises and obligations.

- **Implementation mechanisms.** Procedures should be implemented to ensure that the commitments taken by organisations 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)
- **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.

Finally, as framed by the Accountability projects, it is worth reminding that when introducing an accountability scheme within the legal framework, such scheme can be modulated into several stages, depending on the organisation's level of commitment/rights of authority given to the accountee. The first two stages could be approached as accountability relationships in their broad sense, in that the accountor (who should be identified but is likely to be incardinated into citizens and consumers) does not have any right of authority over the accountor, in the sense of imposing sanctions. The last two stages reflect accountability relationships understood in their narrow sense, where the accountor should abide by the decisions made by the accountee.

1. First stage.- The organization takes appropriate measures to establish processes and procedures that implement its privacy policies
2. Second stage.- The organization self-certified that it meets the requirements of accountability
3. Third stage.- The supervisory authority or recognized accountability agent reviews such filings and provide some form of acceptance of the certification
4. Fourth stage.- The organization submits to enforcement by the supervisory authority or recognized accountability agent. .

4.4 Main Notions in a Graph

The graph below shows, in a simplified way and with the only purpose of illustrating the different notions used in this Chapter, how accountability relationships in surveillance systems could arise and intertwine. The different actors part to these relationships appears either on the first line, if they act as accountors (Who gives the account), or in the second line if they act as accountees (To whom is the account given). The third line indicates what can be the object of the account. Finally the fourth line indicates whether this relationship is likely to be framed as an accountability relationship understood in its broad or narrow sense (respectively, as "answerability" or "compliance").

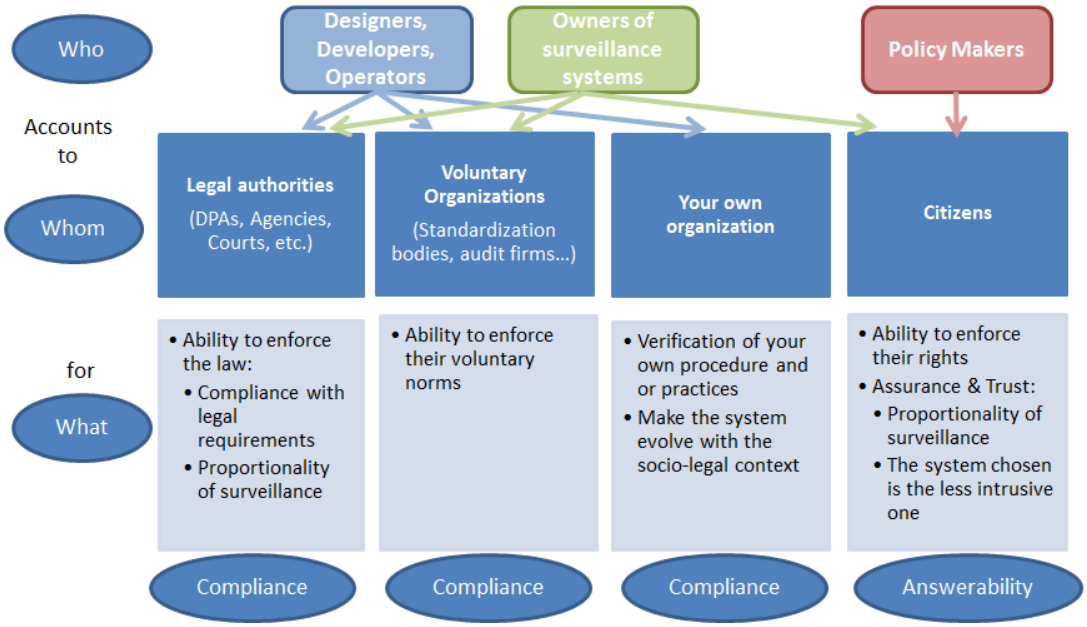

Figure 4: Accountability relationships

5 Privacy from a Computer Engineering Perspective

Antonio Maña and Francisco Jaime (UMA), Zhendong Ma and Bernhard Strobl (AIT), Víctor Manuel Hidalgo (Visual Tools) and Mathias Bossuet (Thales)

5.1 Principles of Privacy in ICT Systems

Some of the most common principles for privacy in ICT systems are summarized in OECD's Privacy Principles document[611]. There are eight OECD principles that correspond in great part to the legal requirements explained in the preceding section:

1. Collection limitation: there should be limits to the collection of personal data, preferably with data subject's consent.
2. Data quality: personal data should be relevant to the usage purpose, accurate, complete and up-to-date.
3. Purpose specification: purpose of data collection should be specified and fulfilled.
4. Use limitation: personal data should normally not be disclosed, or used for purposes other than those specified.
5. Security safeguards: personal data should be protected by security safeguards.
6. Openness principle: there should be a policy of openness about developments and practices of personal data.
7. Individual participation: an individual should have the right to obtain information from a data controller on data related to him.
8. Accountability: a data controller should be accountable for complying with the principles.

A similar set of principles has also been proposed for privacy in databases[612], called "Hippocratic databases". Specifically, the principles are:

1. Purpose specification.
2. Consent.
3. Limited collection.
4. Limited use.
5. Limited disclosure.
6. Limited retention.
7. Accuracy.
8. Safety.
9. Openness.
10. Compliance.

[611] OECD, "Annex to the Recommendation of the Council of 23rd September 1980: OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (Part 2)," www.oecd.org

[612] R. Agrawa, J. Kiernan, R. Srikant, and Y. Xu, "Hippocratic databases," In VLDB '02: Proceedings of the 28th international conference on Very Large Data Bases (2002), pp. 143-154.

From the two sets of privacy principles, it is obvious that the centrepiece of privacy is personal data. The stakeholders around personal data are the individuals (data subjects), data controllers and third parties such as law enforcement actors. Hence the privacy principles provide guidelines on the handling of personal data and the interaction (i.e., "rule of the game") among the stakeholders.

From a system development point of view, privacy can be regarded as a non-functional requirement of ICT systems. Hence, two issues need to be taken into account when applying these principles:

A balance between privacy and system functionality: privacy might have an inadvertent effect on a system's performance and the capability. There should be a balance between the measures and resources for a system's functional requirements and those non-functional requirements like privacy.

A balance between security and privacy[613]: security and privacy are both non-functional requirements. Privacy is closely related to security. Security is the baseline to fulfil many privacy objectives. However, privacy can also create conflicting system requirements with respect to security. For example, anonymity sometimes conflicts with identification and authentication for security.

Conceptually, there are many links between privacy principles and information security, typically modelled as a triad of Confidentiality, Integrity, and Availability (CIA). As shown in Figure 1, the eight OECD privacy principles[614] can be loosely related to the information security triad around confidentiality and integrity, except for security safeguards, which are for both privacy and security.

5.2 Concepts Related to ICT Privacy

The privacy principles establish an overarching framework for many activities that address privacy challenges at the technological level. Within the framework of these principles, the researcher community has developed a comprehensive list of concepts related to ICT privacy. The most representative list is presented as privacy terminologies[615]. We list the relevant ICT privacy concepts below:

Anonymity: anonymity of a subject means that the subject is not identifiable with a set of subjects, the anonymity set. Hence, we can derive that a subject is anonymous it its anonymity holds.

[613] Security is understood here from the point of view of 'data security'

[614] We use the most representative OECD privacy principles.

[615] A. Pfitzmann and M. Hansen et al., "A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management," Tech. Report, v0.34, Aug. 2010, http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.34.pdf

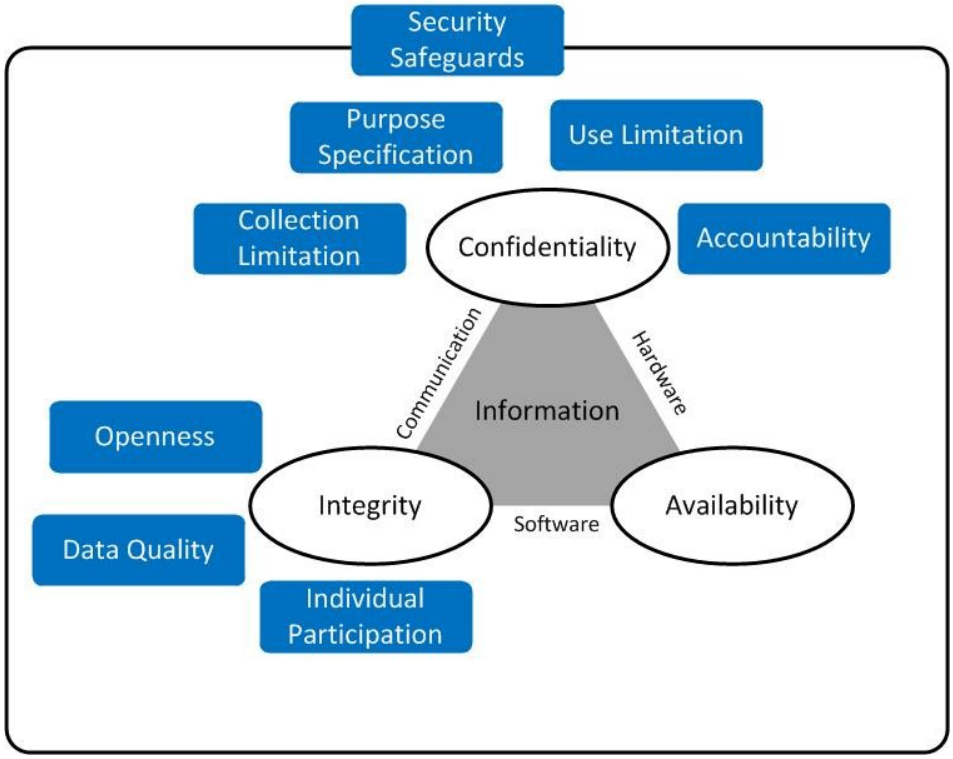

Figure 5. Privacy Principles and Information Security Triad

Pseudonymity: a pseudonym is an identifier of a subject other than the subject's real name. The subject is pseudonymous if a pseudonym is used as identifier instead of one of its real names. Pseudonymity is the use of pseudonyms as identifiers.

Unlinkability: unlinkability of two or more items of interest (e.g., subjects, messages, actions, etc.) from an attacker's perspective means that within the system, the attack cannot sufficiently distinguish whether these items of interest are related or not. Linkability is the negation of unlinkability.

Undetectability and unobservability: undetectability of an item of interest from an attacker's perspective means that the attacker cannot sufficiently distinguish whether it exists or not. Unobservability of an item of interest means undetectability of the item of interest against all subjects uninvolved in it and anonymity of the subjects involved in the item of interest even against the other subjects involved in that item of interest.

From a technical point of view, to achieve privacy in an ICT system usually means to achieve one or more of the above concepts. For example, when privacy is of concern, we do data anonymisation for the records in a database, aim for anonymity or pseudonymity for an identity management system, or achieve anonymous usage of location-based services. Table 1 below gives a short description of ICT systems examples and the privacy concepts involved.

Example systems	System description	Privacy concept in the application domain
Database system	A database is a collection of structured data. A database captures and represents real-world information with abstract records and the relationships between records. Database system is a system for the storing, manipulation,	Data privacy K-anonymity L-Diversity T-Closeness

	retrieving of data and the management of database.	(c,t) – Isolation[616]
Identity management System (IdM)	Identity management systems (IdM) are information systems and technologies for identity management, including the management of identities, their roles and privileges within one or cross multiple security domains.	ID privacy Anonymous identity Pseudonym
Location-based Services (LBS)	Information services that use a user's location data (spatial and temporal) for location related, tailored services. Typically a user interacts with a service provider with his mobile device.	Location privacy Anonymous ID or Pseudonym Location anonymisation

Table 1. Example ICT Systems and the Privacy Concepts Involved

5.3 Concepts of Privacy-Enhancing Technology

The privacy principles and concepts do not automatically achieve privacy in ICT systems. To enforce privacy in ICT systems, we need measures that reduce personal data disclosure and ensure only authorized party can process or access personal data. These ICT measures are referred to as Privacy-Enhancing Technologies (PET). The following table provides an overview of the existing PETs.

PET	Description
Encryption	Data can be encrypted such that only one with the right decryption key can read the original data. Data encryption achieves data privacy during communication and data storage.
Access control	Privacy is about an individual's control over the collection and access to his personal data. Access control controls who can access data and how the data can be accessed according to defined access policies.
Privacy policy specification and enforcement	Privacy policy defines a set of privacy rules on how personal data is handled throughout the data lifecycle in a system. Coupled with right policy enforcement mechanisms, privacy can be achieved according to the system designer and user preferences.
Anonymisation	Data anonymisation removes identity information in personal data such that it is not possible to link a data item to an identifiable person.
Pseudonym	Pseudonyms are used where identification is needed. Pseudonyms can be chained to provide conditional anonymity, i.e., an authorized party can link a pseudonym to a real person under certain circumstance.
Privacy proxy	A privacy proxy acts on behalf of a user to interact with an untrusted third party to hide the real identity of the user.
Obfuscation	A technique to deliberately degrade the quality of a data set such that the data can no longer be linked to an identifiable person.
Mix network/mix zone	A mix network is a store-and-forward network that conceals a user's identity and action by relaying a user's messages within the network before forwarding them to the final destination. A mix zone applies the same concept to conceal a user's movement.

Table 2. Overview of Existing PETs

[616] B. Fung, K. Wang, R, Chen, and P. Yu, "Privacy-Preserving data publishing: a survey of recent developments," ACM Computing Surveys, 42(4), 2010.

5.4 Privacy Concepts Used in Videosurveillance

Video surveillance technology has gained significant progress in recent years in terms of video capabilities (e.g., high zooms, automatic controls, night vision, and video analytics) and storage capacity. At the same time, video surveillance becomes more pervasive as the coverage of surveillance systems increases. This makes video surveillance privacy very challenging.

To address the challenges, the following concepts have been proposed in the past:

Decoupling personal data from video data. As proposed by A. Cavarello[617], advanced video signal processing capability can be embedded into smart cameras such as separate data stream: a metadata stream describing instance, trajectories, and a video stream capturing personal data, are sent to different locations in the system, where surveillance operators can only see the rendered metadata stream. The implementation of the concept can be done at the source of the data flow, i.e., the cameras.

Differentiated access to video data. Other authors[618] propose a privacy-preserving video console. The system design is based on six basic questions related to a video privacy model: (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 system controls the data presentation and the rawness of that data. The system manages operator access to different versions of video-derived data according to an access control list defined using the video privacy model. The implementation of the concept requires a system-wide design and many enforcement points.

The privacy concepts applied in video surveillance systems also use those PETs for non-video ICT systems, for example[619]:

Privacy information identification. Privacy-related information is identified in the video data, such as a person's face, his or her clothing with specialties (e.g. cloth color), etc.

Data obfuscation. Video obfuscation techniques are then used to modify, replace, or remove the privacy information from video data. Such obfuscation techniques include black box, pixilation, blurring, and object replacement and removal.

Privacy data management. As unmodified video data is also needed in video surveillance systems. A challenge is how to manage privacy data, i.e. how to provide a mechanism to enable legitimate users (e.g. law enforcement) to access privacy information in video data.

In addition, technical concepts aiming at qualifying the quality of the video-stream and its usability to extract privacy data have been standardized. The most used is the rotakin factor, commonly used e.g. to specify minimal characteristics of a video-surveillance system to allow identification of a filmed person by a human operator.

[617] A. Cavallaro, "Privacy in video surveillance," IEEE Signal Processing Magazine [168], 2007.

[618] A. Senior, S. Pankanti, A. Hampapur, L. Brown, Y. Tian, A. Ekin, J. Connell, C. Fe Shu, and M. Lu, "Enabling Video Privacy through Computer Vision," IEEE Security and Privacy, 3(3), 50-57, May 2005.

[619] A. Senior (Ed.), "Protecting privacy in video surveillance," Springer, 2009.

5.5 Privacy by Design and PIAs in Surveillance Systems

4.5.1 Privacy by Design

Privacy by design has gained a wide recognition in the privacy research community in recent years. How to embed privacy and data protection throughout the entire life cycle of video surveillance systems, from design to deployment, operation and ultimate disposal is a very challenging issue.

A large amount of uncertainties exists in the life cycle of a video surveillance system. For example, from customer requirements to system designer's decision on technology and actual hardware and software. This is only in the design time. More issues arise during the system run time. These issues can be very dynamic. For example, who should be allowed to access video data besides the operator, or how can we ensure privacy if the owner or operator of a surveillance system uses video data other than real-time monitoring of events in their perimeter? Many issues are hard to foresee during design time.

Having privacy by design as an ultimate goal, our research in the PARIS project aims to come up with an implementable privacy by design practice based on the "State-of-the-Practice" and the combined expertise of the PARIS consortium. The privacy by design practice will be developed to cope with the uncertainties, to some extent, during the video surveillance system life cycle.

4.5.2 Privacy Impact Assessment and Computer Engineering

Privacy Impact Assessment (PIA) refers to systematic processes intended to evaluate the impact upon Privacy of a technological tool or a technological system. The PIA approach is based on systematic auditing methods and can for this reason be compared to risk assessment. The system under assessment is submitted to a predefined listed of questions related to Privacy harms and Privacy protections.

PIA is most of the time applied before the deployment of a system to ensure that new projects comply with information privacy principles and to identify the potential effects that a proposal may have upon individual privacy. PIA is often referred to as an "early warning system".

PIA is a new approach to privacy and is mainly held by governmental organizations and applied to whole systems. PIA is not well taken into account in the computer engineering field.

5.6 Advances in New Technologies and their Impacts on Privacy

The different advances made in technology have led to an increased probability of user's privacy to be breached. Several trends within the technological world have made this possible.

The first trend regards to the constant improvements made to hardware. On one hand, these hardware improvements have resulted in an increase of the speed at which information can be analyzed. On the other hand, the amount of information that can be recollected and stored has also significantly increased.

The second trend is related to the increasing connectedness of the hardware over networks, which enhances the processing capacity. In this way, different hardware devices connected through Internet can process the information.

The third trend is the outstanding software advances. These advances have greatly improved the algorithms for extracting information stored both, locally and remotely on the network.

Finally, the fourth trend relates to the creation of companies and organizations responsible for collecting, organizing and analyzing the information they have, or which third parties have provided.

At present, there are technologies that enable various companies and organizations to collect, aggregate, analyze and share information of people with different objectives. For example, Global Positioning System (GPS) locators attached to trucks can provide near-real-time information on their whereabouts and even their speed, giving truck-shipping companies the opportunity to monitor the behaviour of their drivers.

5.6.1 Hardware Advances

During the last years, hardware technology has increased exponentially. This growth has greatly increased the computation speed. Thanks to this, computational tasks that were too complex for being processed in an acceptable time by ancient computers can now be tackled easily.

For example, CPUs have made a great performance improvement, and memory size has been multiplied by a factor of 100 or more. All this has resulted not only to a higher computation speed, but also to the ability to handle large amounts of data, which was not possible in the past. Furthermore, it is important to highlight the expansion of capabilities to store information. As a consequence, data can be stored for longer periods of time. A good example of this is shown by the capacity to store video streams in high quality, which can take up several megabytes of storage for each second of video. In the past, this was just too much information to be stored for long periods. All these improvements are linked to a reduction in costs, allowing different organizations to rapidly increase their capabilities in processing and data storage.

With more data (including more kinds of data) being kept in its raw form, arises the following concern: every electronic transaction a person ever enters into can be kept in readily available storage, and audio and video footage of all public activities of that person could also be available. This information, originally gathered for purposes of commerce, public safety, health care, or for some other reasons, could then be available for other uses than those originally intended. The fear lies in the temptation to use all of this information, either by a governmental agency, by private corporations or even individuals, which is so great that it will be nearly impossible to guarantee the privacy of anyone from some sort of prying eye, if not now, then in the future.

Another important hardware trend is the evolution of specific devices. These devices have moved from analog to digital data generation, from devices on specialized networks to those connected to larger networks, and from expensive and specialized devices only deployed under rare circumstances, to cheap and ubiquitous devices either too small or too common to be generally noticed. Examples of this kind of devices are cameras, biometric devices, mobile phones, global positioning sensors, etc.

With the increase in hardware performance, more data can be processed, and this together with an improved storage has allowed for storing much more details about individuals than before. Besides, the connection of different devices to the network enables generated data to

move around it. As a consequence, due to the increase of processing and storage capacity, and the possibility of exchanging different data among different devices, it is possible to get more information about people.

5.6.2 Software Advances

Once we have seen the different hardware advances, we will see the software related advances that impact over people's privacy. Software has reached significant improvements, especially in the area of information fusion or data integration techniques, data mining and new algorithms. All these techniques have greatly facilitated the capacity of data extraction. Besides, distributed computing and parallel techniques have led to the possibility of having several devices working together to solve a problem that could not previously be solved by a single machine due to different constraints.

Information fusion is the process that combines different sources of information in order to obtain more accurate, reliable and robust information. This information will be used to make better decisions than those obtained from a single data source. A good example of these techniques is the information that hospitals handle related to their patients. Hospitals can share their patients' information in order to make new findings by the analysis of the fused information. However, since patient privacy must be kept, the exact information should not be shared, unless the information disclosed by any hospital keeps their patients anonymity.

Data mining is the computational process of discovering patterns in large data sets involving methods at the intersection of artificial intelligence, machine learning, statistics, and database systems. The overall goal of the data mining process is to search, analyze and aggregate different data in order to extract information from a data set and transform it into an understandable structure for further use. A good example about how this kind of technique could affect people's privacy can be read in this report[620]. According to this report, some important companies found suitable to expand its data mining to combine users' personal data across all their accounts and services, including mail, internet searching, map and location information, and photo sharing, with no way for individuals to opt out.

Finally, thanks to the algorithm progress we are able to obtain information that was unthinkable a few years ago due to hardware limitations or lack of knowledge. Besides, hard work in algorithms optimization has made them faster. For example, advances in computer vision have allowed tracking several persons at the same time basing on different features such as the colour of their clothes, heights or motion detected in the image.

As a result of the improvements in both speed and efficiency of software and hardware, computation tasks that were unthinkable only a short time ago are now possible on low-cost, commodity hardware running commercially available software. Some of these new tasks involve the extraction of information about the individual from data gathered from a variety of sources. A concern from the privacy point of view is that—given the extent of the ability to aggregate, correlate, and extract new information from seemingly innocuous information—it is now difficult to know what activities will in fact compromise the privacy of an individual.

5.6.3 Advances in Connectivity and Ubiquity

If we combine advances in software and hardware together with connectivity in the digital age, a multiplier effect is obtained. In this way, a computer connected to Internet can take

[620] http://www.guardian.co.uk/technology/2012/oct/15/google-privacy-policy?newsfeed=true

advantage of other devices in terms of computational power, storage capacity and the data stored in them.

Connectivity has an important link with hardware, since improvements in network technology have made possible that data transferred over the network had increased considerably. As a result, the network has become a common and very useful way for exchanging data among different systems. From the privacy point of view, interconnectivity simplifies information access from anywhere in the world, allowing different devices and organizations to share information related to people. If in addition to connectivity we add hardware improvements and enhancements in software techniques, individuals' privacy can be seriously affected.

5.6.4 Conclusions

As a conclusion, the use that organizations or some individuals make of technology has the potential to threaten the privacy of people. Once the data are collected and stored, they are available for analysis. In addition, computers connected to the network can share any data and aggregate them to its source of information. Such process generates more data on an individual, and this information at the same time can be stored and shared with other devices.

The new surveillance is less visible and more continuous in time and space, provides fewer opportunities for targets to object to or prevent the surveillance, is greater in analytical power, produces more enduring data, is disseminated faster and more widely, and is less expensive. Essentially, all these changes represent additional surveillance capabilities at a lower cost, and exploitation of these changes would bode ill for the protection of privacy.

5.7 Applications

In this section we are going to examine the different surveillance technologies that can have an impact on the privacy of the user.

We can classify the different surveillance systems based on their technology. Based on that, we can divide the different surveillance technologies in: visual surveillance, biometrics, dataveillance, communications surveillance, sensors, and location technologies. Here, it is important to highlight that we are going to do a special emphasis on video surveillance and biometrics since the SALT concept is going to be validated for these technologies.

5.7.1 Visual Surveillance

We can divide this group in five areas: video surveillance, imaging scanners, UAVs, satellites and photography.

5.7.1.1 Video Surveillance

This type of surveillance uses video cameras for the purpose of observing an area. Data collected by theses cameras is usually recorded and may be watched by the surveillance system operator (or law enforcement officer). For this reason, they are commonly connected to a recording device or an IP network. Cameras and recording equipment used to be relatively expensive in the past, and they required human personnel to monitor camera footage. But analysis of footage has been made easier by automated software that organizes digital video footage into a searchable database, and by video analysis software. The amount of footage has also been drastically reduced by motion sensors, which allows recording only when motion is detected. With cheaper production techniques, nowadays surveillance cameras are simple and

inexpensive enough to be used even in home security systems, as well as for everyday surveillance.

5.7.1.2 Imaging Scanners

Imaging scanners are systems that generate visible images based on the detection of non-visible waves of the electromagnetic spectrum. For this purpose, these systems can use infrared scanners, sonar imaging, thermal imaging, x-ray imaging, radiation or millimetre wave imaging. A good example of these systems is the use of infrared barriers to detect intrusion in restricted areas at the outer. Another good example of the use of these systems can be found in how authorities have followed the attacks in the Boston marathon (2013), since police used thermal cameras to detect the presence of the suspect in a boat.

These devices can be easily made and they can reproduce the images on a computer screen through walls from across a street. Some of these devices are portable and can be attached to drones or helicopters. However, others are fixed in place. Each one of these systems can detect chemical components and weapons, while some of them also incorporate privacy enhancing technology (PET) elements, such as remote operator workstations or software filters that blur sensitive areas of the body.

While infrared, thermal and other types of portable imaging scanners have been available to law enforcement agencies for some time, the use of body scanners in airports and other locations is relatively recent, but increasingly widespread. Body scanners are widely used in airports of different countries such as The Netherlands, USA, Canada, Spain, Russia or Australia. Besides airports, body scanners are also being used in other contexts, such as border crossings and security purposes (weapons, drugs or other prohibited materials). Thermal and infrared imaging scanners may also be used for disaster relief or emergency response (searching for survivors) and by various government, law enforcement and security authorities to search for suspects or gather information about the number and location of occupants inside a building.

5.7.1.3 UAVs

An Unmanned Aerial Vehicle (UAV), commonly known as drone, is an aircraft without a human pilot on board. Its flight is controlled either autonomously by computers in the vehicle, or under the remote control of a pilot on ground or in another vehicle. These vehicles can accommodate different devices as cameras, sensors or other information gathering equipment. UAVs are typically used for military operations. However, they can also be used in civilian applications. UAVs are designed for dangerous works, and so avoid endangering the lives of pilots. Another important characteristic about UAVs is that they can be very difficult to detect by their target because they can work in silence.

We can find some examples of use of this kind of devices in policing, border control, emergency response and monitoring environmental hazards. Police forces use these devices to monitor individuals such as squatters, festivalgoers, hooligans, and demonstrators and undocumented workers.

5.7.1.4 Satellites

Earth observation, communication and other satellites have been orbiting the Earth since the beginning of the space program. Initially, these satellites were used for military purposes. More recently, such satellites have been used for civilian applications. Satellites have helped law enforcement in intercepting or obtaining information from mobile phones, radio transmissions, emails, IP addresses or file transfers. Satellites also assist the army and other state authorities

in reconnaissance operations, and can take static photographs or video of places or people. Satellites also provide services such as location based services for mobile phones, satellite navigation services for cars or other vehicles, vehicle location tracking and recovery services, tracking of individuals, emergency services, environmental management (such as erosion tracking), disaster response services and images for entertainment. Drivers, employees, smart phones' owners and others who use location services can be strongly affected.

5.7.1.5 Photography

Photos of different individuals can be taken from several devices at different locations. The most historic device that performs this function is the portable camera. Nowadays, we can find different portable devices, such as mobile phones, which can take and store photos of people. Even these photos can carry related data associated with the place where they were taken and/or the time when they were shot. These photos can be used to identify people or objects, which may later disclose information relating to individuals (i.e. number plates). For example, police uses a radar system for vehicles in order to detect when a car exceeds certain speed limits. When this happens, the system takes a photo in order to identify the owner's vehicle through its number plate.

Photography can be used for identification purposes including, but not limited to, mug shots, passports, driving licenses and other identity documents. Police or other authorities may also use this type of surveillance to monitor traffic offenses such as speed cameras, red light cameras, bus lane cameras, etc. Finally, this surveillance system may be used for less conventional forms of surveillance such as "happy slapping" by young people.

5.7.2 Biometrics

In recent years, biometric systems have considerably grown and we can see how a large number of people use them every day. A good example of these systems lies on those that allow us to enter in rooms with restricted access, or those that allow companies to monitor the time their employees spend on their work places.

In any case, before talking in more detail about biometric technology, it is very important to have a clear idea about these systems behaviour. For this reason, we are going to see some basic definitions in order to facilitate this task.

The word **Biometric** comes from ancient Greek words *Bios* for life and *Metron* for measure. According to its origin, we can understand the biometric word as the measures of different data related to life. But, what do we understand by biometric data?

> **Biometric data:** "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"[621].

Based on the above definition, we know that biometric data are unique and we can measure them through some specific system with a very particular purpose. These systems are called biometric systems and they can be defined as follow:

> **Biometric system:** "application that uses biometric data in order to allow the automatic identification, and/or authentication/verification, and/or categorization of a person"[622].

[621] Article 29 Working Party, WP136, p. 8, WP193, p. 3 (Available at: - http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf)

[622] Article 29 Working Party, WP193, p. 5 (Available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf)

Once we have seen what a biometric data and a biometric system mean, we will show the requirements a biometric data must satisfy to define a system as a biometric system:

Universality: All the individuals should own the characteristic.

Uniqueness: The characteristic should be enough to distinguish any individual.

Permanence: The characteristic should be invariant over time.

Measurable: The characteristic has to be measured qualitatively.

In theory, the previous requirements are the only necessary ones. However, in practice we have to take into account some other requirements:

Performance: Refers to the level of accuracy and speed of recognition of the system, taking into account the operational and environmental factors involved. In these systems, accuracy is frequently defined in terms of the percentage of false positives and false negatives.

Acceptability: Refers to the extent of the population that would be predisposed to accept the identification system.

Resistance to circumvention: Refers to how easy it would be to cheat the system with fraudulent techniques.

Once we have seen the main characteristics that any biometric data must have, we are going to introduce the main different phases in which a biometric data is processed within a biometric system. These four phases are: acquisition, enrolment, storage and matching.

Acquisition: In this phase, the biometric system gets the biometric data via some type of sensor (e.g., camera, finger print reader…).

Enrolment: In this phase the biometric system extracts the specific features from a biometric data. These features are used to generate a template, which is then linked to an individual. A good example of this could be an access control using a face recognition system in order to allow people to enter in a specific room. Everybody who is going to have enough permission to go into the room needs the system to previously obtain their appropriate data during the enrolment process.

Storage: The features obtained in the enrolment phase must be stored (i.e. a centralized database).

Matching: The next time someone uses the system, after the individual enrolment and data storage phases, the system will generate a template for the current individual that will be compared against the database data in order to know whether the individual is accepted or not.

The goal of all these phases is to know whether the individual is going to be accepted or not. Therefore, these systems have two traditional basic operations: identification and verification/authentication. In addition, due to the latest technological developments, is also possible to perform another operation mode: categorization/segregation.

Identification: The system attempts to detect the identity of an individual without that individual claiming a particular identity. In this case the template generated by the biometric system is compared with all the templates previously stored.

Verification/authentication: The biometric system authenticates an individual's claimed identity. For that, the template generated by the biometric system is only compared against the enrolled template corresponding to the desired person.

Categorization: In this operation mode it is not important to identify or verify the identity of the person, but if his/her biometric data belongs to a specific group. For example, if the user is a woman or a man, the system will behave in a different way.

After explaining the main concepts of biometrics and the different features that biometric data must satisfy, the following question arises: why are biometrics used?

If we don't use biometric systems, the mechanisms that a person has to verify his/her identity or to identify himself/herself are: using a password, a cryptography key, a smart card or something similar. But this kind of methods is associated to some security problems. For example, the password, cryptography key or smart card could be forgotten, lost, stolen or even the own user could share them with others. As a consequence, the integrity of the system could be put at risk. Biometrics exploits the fact that certain biological characteristics are unique and unalterable and are also impossible to miss, transfer or forget. Furthermore, they require the presence of the person at the moment of the identification. This makes them more reliable and secure than passwords.

Biometric systems can be used in numerous contexts such as security, e-commerce, law enforcement, health, social services and surveillance. Below, we are going to assess the current technologies that can be found in the market.

5.7.2.1 Fingerprint Recognition

This technology is based on identifying an individual through its fingerprint. The skin on the surface of a fingerprint consists of raised folds of skin, known as ridges, which are separated by valleys. Its operation takes a fingertip image and then reduces such image to a template (mathematical representation of the fingerprint). Next, a biometric device stores this template. Furthermore, the template is linked with something that associates the user with the fingerprint, such as an identification number or the user's name. Then, each time the person needs to be identified, for example to record his/her hours of admission, or to return to work, he/she places his/her finger on the reader.

Some of the features used to establish the mathematical representation of the fingerprint are the core, the delta and the minutiae. The core is the centre point of a particular fingerprint, the delta is a point where three patterns are deviated and the minutiae can be ridge endings or ridge bifurcation. A ridge ending is where a ridge stops and a ridge bifurcation is where a ridge is separated in two. In the following figure, we can see an image with the core, the delta, and the minutiae.

Figure 6. Core, Delta and Minutiae

It is important to highlight that this technology is the most used biometric system in the current market, which is due to its flexibility to be adapted to numerous systems. It usually is suitable for verification systems and small-to- medium-scale identification systems. One of the problems of this type of systems is that it requires a big amount of computational resources. Besides, these systems also show another important inconvenient: the possibility of an identification or verification failure, which may be due to environmental or occupational reasons (i.e. cuts…).

5.7.2.2 Iris Recognition

The iris is the annular region of the eye bounded by the pupil and the sclera (white of the eye) on either side. The human iris is a unique structure for each individual. It is a very complex system and it remains unalterable for the individual's life. To make possible the recognition, the individual looks at a camera and his/her iris is illuminated through an infrared light. After that, the algorithm creates a mathematical representation of the iris. This representation will be stored and linked to a person, if we are in the enrolment process, or it will be compared against the templates previously stored in the identification or verification phase.

It is important to highlight that the system operates well in both, identification and verification/validation applications. These systems are used in many contexts, such as airports or border controls. Their main advantage is their reliability.

5.7.2.3 Face Recognition

These systems consist on automated or semi automated processes that extract facial characteristics in order to compare the spatial geometric features for user identification or verification. The source for the identification can be both, photographic images and video. The identification can be done in 2D, 3D, or a combination of both. Normally, in the first stage of the process (enrolment), the system builds the template by taking multiple photos of the user. The next time the system tries to identify or verify a user, the new extracted features are compared with the previously stored. It is possible for the system to never find an identical template stored. For this reason, the matching process will consider the most similar template, or all the templates that exceed a specific threshold will be selected and sent to a human operator, who will establish the final correspondence.

These systems have two well-defined parts. First of all, the system has to locate a face within the image. Once the face has been located, the system is able to carry out the analysis. The features extracted are related to the location and shape of the facial attributes such as eyes, eyebrows, nose, lips and chin, and their spatial relationships.

This kind of biometric systems is also very used. Face recognition is a nonintrusive method and facial images are probably the most common biometrics used in the identification mode. However, it presents some drawbacks. The first one is that the captured view could be drastically different from the one taken during the enrolment process. Another problem refers to the illumination conditions in which the photo is taken, since they can affect a lot the outcome of the analysis.

5.7.2.4 Hand Recognition

Hand geometry recognition systems are based on a number of measurements taken from the human hand. The recognition of the hand can be done in two and three dimensions.

Two-dimensional systems look at palm lines patterns, which are used to establish the template. However, three-dimensional ones are based on the dimensions of the hand (finger length, hand height, etc.…) in order to create the corresponding template.

Although it is not the most secure biometric technique, the use of the palm as a mean of authentication has proved an ideal solution for medium security applications, where convenience is considered more important than safety or precision.

Commercial hand systems are usually used as verification systems. They have been installed in hundreds of locations around the world. The technique is very simple, relatively easy to use, and inexpensive. Environmental factors such as dry weather or individual anomalies such as dry skin do not appear to have any negative effects on the verification accuracy of hand geometry-based systems. However, personal jewelries, such as rings, or limitations in dexterity can quite hinder the extraction of the required features. Another important drawback is the length of the sensor, which prevents its installation within an embedded device.

5.7.2.5 Vein Recognition

This system captures veins of the hand distribution because their distribution under the skin is relatively distinct among individuals and stable. To achieve this purpose the system uses a camera and infrared light in order to detect the visible blood vessels. The main features extracted to generate the template are blood vessel branching points, vessel thickness and branching angles.

Vein patterns are unique to each individual and, apart from their size, the pattern does not change over time. In addition, veins are extremely difficult to misuse, since they are not visible to naked eye. For these reasons, vein recognition systems are one of the most secure biometric systems.

5.7.2.6 Ear Geometry Recognition

This type of biometric recognition is based on analyses of the shape of the outer ear, the ear lobes, bone structure and the distance between salient points on the pinna from a landmark location on the ear.

As in the face recognition system, we find two well-defined parts in this algorithm. First of all, it needs to locate the ear on the image. Secondly, the algorithm extracts the features of the biometric data. Some things that the algorithm has to take into account are the differences in skin tone due to lighting variation, the presence of earrings and the hair occlusions. This kind of things can make the recognition more difficult.

The main problem of this system is that extracted features are not very distinctive for authentication purposes. Generally, ear recognition is used as a supplementary biometric technique.

5.7.2.7 Palm Print Recognition

The palm of the hand contains patterns of ridges and valleys, much like the fingerprints. Human palms also contain additional distinctive features such as principal lines and wrinkles that can be captured even with a low-resolution scanner. These patterns of the palm are used to create the template. The template can be representative of the entire palm surface or it can be confined to specific smaller regions of the palm surface, depending on the performance requirements.

Similarly to fingerprints, palm prints are susceptible to fail due to cuts or similar things. Palm print recognition is considered to be highly accurate, though the quality of the images can affect the error rates because the area of the palm is longer than the finger's, therefore palm prints are theoretically more distinctive than fingerprints. However, this advantage becomes in a disadvantage if we take into account the system cost, since this sensor is more expensive and longer than fingerprints'. Decisions to implement palm print recognition systems must balance the need for accuracy against the cost and the interoperability issues associated with this technology. This kind of technology is increasing in commercial and law enforcement applications.

5.7.2.8 Retina Scan

The retinal vasculature is rich in structure and is supposed to be a unique characteristic of each individual and each eye. The retina recognition is done comparing the complex blood vessels located in the eye. The acquisition requires a person to lean into an eyepiece and look at a specific point. An infrared light, which is invisible to the user, illuminates the eye and it is reflected back to the sensor. Then, the algorithm creates a template based on the blood vessel. Retina recognition systems are expensive and tend to have low acceptance levels. They are not widely utilized outside high security and national security applications.

Retinal recognition is a very accurate system for both, verification and identification modes. In fact, as it is very difficult to change or replicate the retinal vasculature, it is considered the most secure biometric system. Some people consider that retina scan is invasive and health concerns have been raised relating to potential thermal damage to the eye. In addition, this system can reveal some medical conditions, e.g., hypertension. For these reasons retina recognition does not have a large acceptance among people.

5.7.2.9 Gait

Gait is the peculiar way one walks. Gait is enough discriminatory to use in low security systems working in verification mode. Another important characteristic is that gait is not universal, since not all individuals are able to walk. Gait may not remain invariant, due to changes in body, weight, injuries, or due to inebriety. These systems are generally widely accepted. Some specific conditions such as illumination and shadows can significantly affect to its accuracy.

For data acquisition, the system uses a camera to get images in order to generate a relationship between different points of the movement of the body. These points together with other characteristics such as shape and cadence generate the template.

5.7.2.10 Voice Recognition

This system tries to recognize an individual by his/her voice. The voice of people can be distinguished based on the shape and size of the appendages (e.g., vocal tracts, mouth, nasal cavities, and lips). The acquisition of biometric data is carried out through a microphone. There are two different types of voice recognition: text dependent and text independent. In the text dependent mode, the user must read a predetermined phrase. In this case, during the enrolling phase the user should repeat the phrase a specific number of times for the system to create the template. On the other hand, in the text independent mode, the user's voice is analyzed regardless of what he/she is saying.

One disadvantage is that an individual's voice may vary, due to speech changes because of age, physical conditions (such as common cold) or even the emotional state. Another disadvantage is that these systems are especially sensitive to a number of factors such as background noise or the state of the microphone and the communication channel. Another important characteristic is that human voice is not universal since not all individuals are able to talk. Voice biometrics are usually used in verification-based applications, and have been implemented in the financial services sector, especially e-commerce and e-banking (e.g. in banks these systems are used to allow users to access their accounts, and also in the law enforcement sector for forensic purposes).

5.7.2.11 Signature Recognition

The way a person signs his or her name is considered a characteristic of that individual. These systems assess some characteristics points of the signature, as well as the speed, direction and pressure of writing among other things. In the enrolment phase the user should provide several signatures in order to create a more representative template.

Signature is not universal, since there is a big amount of people who are unable to write. Besides, signatures are not considered very distinctive. However, they have been accepted as a mean of verification for various governments, as well as for legal, financial and commercial transactions. This kind of systems is primarily used in verification mode. One important disadvantage is that signature recognition is not very accurate.

5.7.2.12 DNA

Deoxyribonucleic acid (DNA) is the one-dimensional (1–D) ultimate unique code for one's individuality— except for the fact that identical twins have identical DNA patterns. Despite the fact that DNA is one of the most effective methods, since the performance of DNA matching is highly accurate, its utility is limited for different reasons. First of all, it cannot be conducted in real time, i.e. it takes a few hours. Secondly, for privacy issues: DNA contains information of a person concerning certain diseases. If the genetic information of the DNA samples was transferred to third parties such as insurance companies or employers, it could lead to discriminating measures against individuals with a specific genetic. DNA is usually used in identification systems. It has limited commercial uses. This technology is mostly used for paternity tests, criminal identification and forensics.

5.7.2.13 Multimodal Systems

The use of several biometrics can solve some of the problems presented by some biometric systems. Such systems, known as multimodal biometric systems, are expected to be more reliable. Multimodal biometric systems make much more difficult for an intruder to simultaneously spoof the multiple biometric traits of a legitimate user. They are normally used in the authentication mode.

These systems have three operation modes: serial mode, parallel mode, and hierarchical mode.

Serial mode: the output of one biometric is used to narrow down the number of possible identities for the next biometric system.

Parallel mode: information from multiple traits is simultaneously used to perform recognition.

Hierarchical mode: the different results of biometric data are combined in a tree structure.

Multimodal biometric systems integrate information presented by multiple biometric indicators. For this reason, they have some techniques to enable data fusion. Multimodal systems can be used in one of the following scenarios:

1. Multiple sensors are used to sense the same biometric identifier.
2. Multiple biometrics. In this case different biometric systems are combined (e.g. face and fingerprint recognition).
3. Multiple units of the same biometric. For example, one image from each of the two irises of a person may be combined.
4. Multiple snapshots of the same biometric. For example, several images of the face of a person could be combined.
5. Multiple representations and matching algorithms for the same biometric. It combines different representations and matching algorithms to improve the recognition accuracy.

One disadvantage of multimodal systems is that the cost of the system increases because of the use of multiple sensors (e.g., when combining fingerprints and face recognition). However, their use is very recommendable for high security applications, large-scale identification systems, and negative identification applications, which will increasingly use multimodal biometric systems.

5.7.3 Dataveillance

Dataveillance or *data surveillance* is the process that recollects personal information based on electronic data traces from different sources to investigate or monitor people's daily activities and their interactions. Some examples about dataveillance are: employers can monitor employees' calls and e-mails; cellular phone companies can have access not only to the calls but also to the location of their customers; credit card companies know their clients' online and offline shopping habits.

We can distinguish two types of dataveillance: mass data surveillance, which refers to the monitoring of a group of people, and personal data surveillance, which refers to the monitoring of one specific person. The following are some of the different techniques applied to obtain personal information.

5.7.3.1 Data Mining

Data mining is the computational process of discovering patterns or correlations in large data sets in order to transform a big amount of information into an understandable structure for further use. For example, US government uses data mining in order to stop terrorist programs. As it has been discussed above, some authors have discussed[623] how this kind of technique could affect people's privacy.

When these patterns or correlations are used to identify or represent people, they can be called profiles. The main goals of profiling are criminal profiling and the analysis of risks for insurance companies. Data mining is typically the first step in this process, as it defines the classes ("suspects or prospects") where users can then be profiled in. Profiling then attempts to predict, or at least pre-empt, individual future behaviour by relying on the stereotypes learned during the data mining step, ultimately classifying individuals as potential risks or commercial windfalls.

5.7.3.2 Data Fusion

We define information fusion as the process that combines different sources of information in order to obtain more accurate, reliable and robust information to make better decisions than those obtained with just a single data source.

A good example of data fusion is a tracking system. Let's imagine a system with several cameras, each one associated to a tracking algorithm. On this environment, the system has to cope with many objects moving in the scene at the same time and with events. This system should be able to track each target in order to understand the behaviour of every actor. Thus, when the system detects a possible suspect outside of the range of vision of the camera 1, and then it appears on the camera 2, the system can merge content from the two tracking systems in order to know that it is tracking the same person.

5.7.3.3 Cyber Surveillance

The term cyber surveillance typically refers to the tracking of online behavior, which in most cases is synonymous with browser activity (i.e., Web surfing). In a broader sense, however, it can also include the monitoring of all Internet traffic, i.e., including e-mail, peer-to-peer connections, VoIP…

Maybe the most prevalent form, although limited, of cyber surveillance, is represented by the cookies. Many companies try to track users by using cookies across two or more seemingly unrelated websites to learn about the user's surfing preferences.

5.7.4 Communication Surveillance

Throughout history, all kind of communications has been treated to be intercepted. Almost as soon as a new technology appears, big efforts are done in order to intercept communications.

First of all we will explain some interesting concepts. *Electronic eavesdropping* is the interception of electronic conversations without the knowledge or consent of at least one of the participants. *Wiretapping* is a subset of electronic eavesdropping where a wire is involved in the communication.

[623] http://www.guardian.co.uk/technology/2012/oct/15/google-privacy-policy?newsfeed=true

These types of communication can be intercepted at numerous points along the path: in one of the devices used by the communication users, or also at various locations along the way.

In the context of surveillance, the following technologies are relevant:

5.7.4.1 Telephone Lines

Telephony has changed a lot from 1970. The most important changes are based on technology. Below, we are going to see these improvements:

- The move to digital signal.
- The replacement of optical fibre and the former continental copper cables for intercontinental communication satellites.
- The transition from electromechanical circuit switching to computer-based switching.

These shifts also changed the nature of wiretapping. Digital wiretaps work remotely and they are usually installed in the telephone company's switch. However, if the conversation travels with a strong encrypted method, the only possibility to know the message lies in wiretapping either the telephone itself, or the target's organization before the device that encrypts the signal.

5.7.4.2 Mobile Phones

Mobile phones include many security measures. Some of these measures are challenge-response authentication, frequency hopping and strong encryption algorithms. All these measures allowed a secure signal transmission over the air for a long time. However, it has been possible to break these communications in the recent years, although it still requires strong computation resources.

It is also important to understand how the mobile phone communications work. The communication is encrypted between the mobile phone and the base station. Next, it travels unencrypted through the mobile provider's core network. Then, it is encrypted again between the other telephone and its respective base station. As an example, it is important to mention the Greek case in 2005 by which cellular phones of government and military officials had been illegally wiretapped for over half a year.

5.7.4.3 Voice-Over-IP

The "Voice over Internet Protocol" makes the communication possible by using Internet as a medium instead of using telephone lines. This system usually uses the RTP protocol. Data is cut in different small packages, which can be sent via different paths to their destination. This fact makes VoIP calls very difficult to wiretap.

The voice is not necessarily encrypted. However, the standard H.235.6 defines an encryption mechanism. Though, when the exchange of the key (to encrypt the message) between the different involved devices is done, interception can be performed with a man-in-the-middle attack at the VoIP provider –this is the foreseen mechanism for lawful interception. A good example of VoIP is the well-known application Skype. Here, the key exchange is done in a peer-to-peer manner among the partners. Because of this, the only way of wiretapping a communication is before the voice encryption.

5.7.4.4 Call Logging

Eavesdropping into a communication along the line is difficult and expensive, and often impossible. Call logging is the cheaper and easier alternative, since it only records the time and duration of the conversation, as well as the identities of the communicating parties.

Analyzing who is communicating with whom, when the content is not accessible, has military roots. British intelligence, for example, after intercepting (but not decoding) German Air Force transmissions in 1941, was able to infer that a unit was composed of nine and not twelve planes as previously assumed, leading to a reassessment of the German Air Force's overall strength.

5.7.4.5 Monitoring Text-Based Communication

Another kind of surveillance on communications is based on text. Examples of messages than can be intercepted are e-mail or instant messaging (IM). Text-based messages can be intercepted either in one of the end-user devices or along their path.

5.7.5 Sensors

Sensors represent another type of surveillance technology with a growing market in relation to security, although every type of sensor usually performs only one specific task. For this reason sensing systems can be composed by several different sensors. Then, we are going to see the different kind of sensors used in security.

5.7.5.1 Heat Sensors

The two main types of sensors are passive infrared sensors and infrared cameras.

Passive infrared sensors are small devices. These systems are connected to an integrated circuit, and when the temperature changes, the sensor induces a current that closes a second circuit. This second circuit is responsible for another function. These sensors are used to detect human presence. It is very common to find them in systems to prevent theft.

Infrared cameras are devices that form an image by using the different levels of infrared radiation. The different levels of infrared radiation are represented as follows: low levels of infrared are cold colours, and high levels of radiation are warmer colours. Infrared cameras are used in many domains. A good example in the area of surveillance is the recently monitoring of the attacks in the Boston marathon (2013), since police had used thermal cameras to detect the presence of the suspect in a boat. Besides, these systems are CCTV complement in some domains such as border crossing.

5.7.5.2 Explosive and Drug Detectors

We can distinguish two main categories: bulk detection and trace detection. Bulk detection of explosives or drugs uses the same technology as the previously discussed imaging scanners. On the other hand we have the trace detection categories. These detectors have the goal to detect and identify residual traces that indicate either the presence of specific chemicals or someone's recent contact with chemicals such as drugs or explosives. For that purpose, first of all a sample is collected, then the sample is analyzed, and finally the results go through a comparing process.

In the decade after 2000, several US airports have introduced portals for trace detection of explosives.

5.7.5.3 Metal Detectors

Metal detectors are in charge of detecting the presence of metals. For that purpose, they use electromagnetic technology. These systems can work with a very low frequency or use pulse induction. Both types create electromagnetic fields and detect either the presence of a magnetic object, or the alteration of the original electromagnetic field due to the presence of metal.

Traditionally, they have been used at airports. During the last years, metal detectors have also been used at railway stations, museums and sport events.

Apart from these sensors, there are more sensors coupled with new investigations, which are focused on obtaining more information of individuals to study their behaviours. For example, suspects can be identified through the use of remote cardiovascular or respiratory sensors. Furthermore, multimodal systems formed by several sensors can also be generated.

5.7.6 Location

Nowadays, we have quite a lot of location systems. But we can classify them in: triangulation, proximity sensing or scene analysis.

Triangulation is a technique that uses the geometric properties of triangles to estimate the target localization. It can be divided into two derivations: lateration and angulation. Lateration technique estimates the position of a target according to its distances from multiple reference units. On the other hand, the angulation technique estimates the localization by computing angles relating to multiple reference points.

Proximity sensing systems try to know the proximity of an object to a specific point. The location is a consequence of the neighbourhood relation with a known spot. An example of this technique is the use of Radio Frequency Identification (RFID) to determine the presence of an RFID tag near a given antenna. Another example is an existing connection between an electronic device and a Wi-Fi antenna to determine the device's presence within the range of the Wi-Fi antenna.

Scene analysis infers the position of an entity from a neighbourhood relation. For example, we can use this technique together with a vehicle license plate recognition system. A recognized plate implies the proximity of the corresponding vehicle to the checkpoint.

Below we will see in more detail the predominant localization systems.

5.7.6.1 GPS (Global Positioning System)

The Global Positioning System (GPS) is a space-based satellite navigation system that provides location using time-of-arrival-based triangulation.

The GPS location is computed on the receiver's side only. A GPS receiver calculates its position based on the time it takes to get a signal sent by a satellite. Satellites are continuously sending messages. These messages include the time the message was transmitted and the satellite

position at time of message transmission. The receiver uses the messages received to determine the transit time of each message and computes the distance to each satellite using the speed of light. Each of these distances and satellites' locations defines a sphere. The receiver is on the surface of each of these spheres when the distances and the satellites' locations are correct. These distances and satellites' locations are used to compute the location of the receiver using navigation equations. In typical GPS operation, four or more satellites must be visible to obtain an accurate result. Four sphere surfaces do not typically intersect.

GPS has become a widely deployed and useful tool for commerce, scientific uses, tracking, and surveillance. For example, in the US, police has planted hidden GPS tracking devices in people's vehicles to monitor their movements, without authorization.

5.7.6.2 Triangulation for Mobile Phones

Mobile phones can be located using a simple proximity sensing or via triangulation between several cell towers. With the proximity technique, it is possible to determine the grid cell in which individual mobile phones are situated. With triangulation technique, mobile position can be known with much greater accuracy.

This system is used to improve responses to emergency calls, but also to better locate suspected criminals. Regulators have asked mobile telephony operators in the US to be able to locate mobile telephones within 150 meters.

5.7.6.3 RFID Positioning

RFID or Radio-frequency identification is the wireless non-contact use of radio-frequency electromagnetic field to transfer data, for the purposes of automatically identifying and tracking tags attached to objects.

RFID tags can be either passive, active or battery assisted passive. An active tag has an on-board battery and periodically transmits its ID signal. A battery assisted passive (BAP) tag has a small battery on board and it is activated when in the presence of an RFID reader. A passive tag is cheaper and smaller because it has no battery. Instead, the tag uses the radio energy transmitted by the reader as its energy source.

On the other hand, we can classify the Readers in: Passive Reader Active Tag (PRAT) and Active Reader Passive Tag (ARPT). A PRAT system has a passive reader, which only receives radio signals from active tags. On the other hand, an ARPT system has an active reader, which transmits interrogator signals and also receives authentication replies from passive tags.

These tags can be used to identify products, passports, vehicles, tracking people, etc. RFIDs can also be used to locate tags instead of physical objects and thus be explicitly used for positioning. For example, a tag embedded in a shoe could serve as a de facto identifier for the person who wears it.

6 Preliminary Recommendations for the SALT Framework

All partners:

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

In all the previous chapters, preliminary recommendations have been expressed in order to help in identifying the relevant criteria for the design of the SALT framework and to prepare the next steps of this research project, and more precisely of this work package 2 dedicated to the definition of the concepts for a Socio-political, ethicAI, Legal and Technical framework (SALT framework) and analysis of the concept of accountability and of its rationale. As presented in Figure *7*, all chapters have highlighted the main concerns and issues addressed by the project.

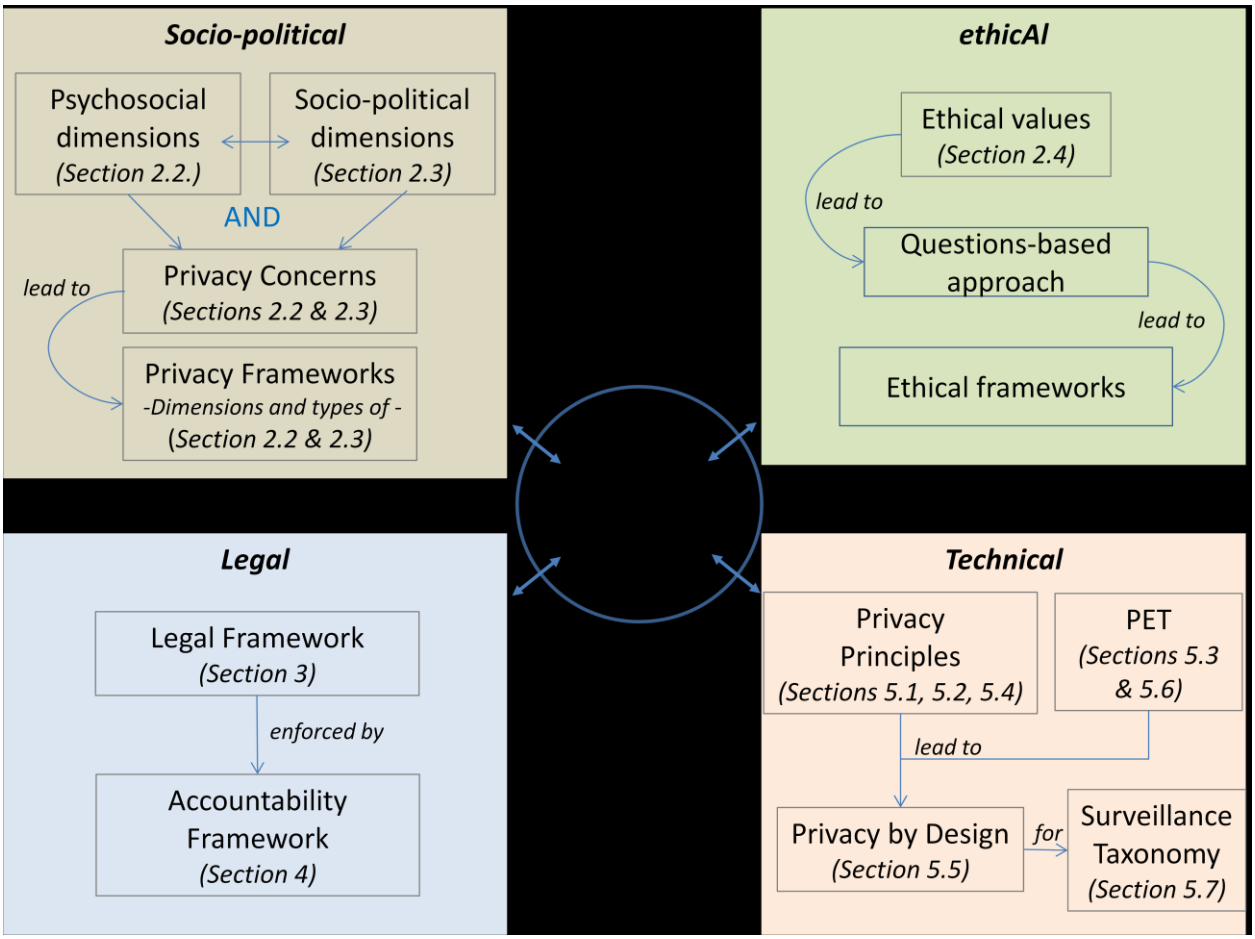

Figure 7 Overview of Results Achieved in this Document

According to all results mentioned in Figure *7*, this last chapter brings together those preliminary recommendations for the design of the SALT framework.

Chapter I (Introduction: A Multidisciplinary Approach to Privacy) aimed at providing a general introduction of the deliverable. After recalling its objectives and scope, it starts with a section which is dedicated to terminology where conceptual remarks needed for the well understanding of the progression of this study are made. First ones concern the important notion of "privacy". Second ones concern the notion of "surveillance". Third ones concern privacy-surveillance paradigms. Different rationales are exposed regards to the balance between surveillance and privacy. Following a section devoted to the concept of privacy-by-design, the risks and the challenges of this approach. Then, as a result of those precedent remarks, a set of observations concerns the prism through which the SALT Framework is developed and offers the opportunity to underline the uniqueness of the SALT framework compared to other privacy frameworks used for the privacy by design of a system-to-be. Finally, a final round of remarks concern the multidisciplinary approach adopted in this text.

It's worth mentioning that different reasons, both theoretical and methodological, for **the re-wording of the initial formulation of the SALT framework**, as presented in the description of work of PARIS' project. Initially, **SALT** sands for **S**ocio-political, **A**nthropological, **L**egal and **T**echnological dimensions of privacy. The arguments presented were sufficient to make us choose another word to anchor the **A** of the SALT Framework. Two main constraints guide this choice. (1) The first one is to avoid the use that has been made by academic knowledge in favour of social acceptability paradigms and the methodological bias that have been induced by such a posture. (2) The second one is to inform about individual and collective dimensions of privacy. For all those reasons, from now on, the **SALT Framework** refers to the **S**ocio-political, ethic**A**l, **L**egal and **T**echnical dimensions of privacy.

Several challenges for the future steps of this research project were identified.

(1) The first one concerns the integration in the SALT framework of **an extended conceptualisation of privacy** that takes into account its socio-political, ethical, legal and technical dimensions, the concept of accountability and its implications. An extended version of privacy implies **to go beyond the sole legal and technical compliance for reaching pro-active proposals regards to orphan dimensions**. One singularity of the PARIS project lies in its aim to **broaden the scope of privacy concerns** taken into account, while integrating supplementary dimensions to the usual legal and technical ones, going beyond the technical security requirements and the legal compliance. Privacy is more than data protection and more than privacy as informational confidentiality.

(2) A second one concerns the precision needed in the characterisation of the **surveillance technologies** that will serve as case studies during the next steps of this research. Starting from a generic definition of surveillance allows and make necessary to characterize, among different technologies of surveillance, one the one hand, the ones which are chosen as case studies and, on the other hand, the other ones for which the SALT framework is also relevant but may make necessary further development of the SALT framework in order to respond to their specificity. Several provisional

characterizations were identified: the type of surveillance's practices (watching, listening, following, etc.); the type of surveillants (public authorities, private actors, etc.); the target – direct and indirect - of the surveillance (people or objects, particular individuals, groups or social categories of persons, etc.); the technology used (video surveillance, imaging scanners, fingerprint recognition, etc.); the purpose of the surveillance (crime control, marketing, etc.); the locations and perimeters kind of surveillance (transport facilities, public space, communication facilities, etc.); the publicity/visibility of the surveillance (do the surveilled know precisely when, where, why and how they are under surveillance?); etc.

(3) A third and very important challenge concerns **privacy-by-design** philosophy or, more precisely the possible translation of the general principles of privacy-by-design into the effective design of systems of surveillance. Rather than considering the criticisms addressed to privacy-by-design as describing the reality of what is a privacy-by-design process and what are its outputs, those criticisms may be seen as showing some risks any privacy-by-design process runs. In that sense, the privacy-by-design concept may gain robustness in demonstrating how it avoids these risks. This is surely a challenge for the PARIS' project. While leaving the sole point of view of rhetoric, the critics exposed above not only identify risks any Privacy-by-Design process runs, they also identify the gap between the spirit of the Privacy-by-Design and the incorporation of Privacy-by-Design into a system-to-be. The Paris project offers the opportunity to put these difficult challenges to the test. In that sense, it is **a real scale experiment of what may be the actualisation of high privacy-by-design expectations**. The first step of this real scale experiment lies in the building of the SALT framework which is characterized by its multilateral perspectives: different knowledge and practices – be they come from academic or private sectors.

(4) A fourth and also important challenge regards **engaging a public** into the design of a surveillance system-to-be and the ways the SALT framework may participate or not to such a difficult task. The task is complicated by a very large definition of what is a stakeholder: added to the traditional stakeholders taken into account regards to surveillance technologies, that those who are involved in developing, implementing and operating surveillance systems, as well as the technological, economic, political and social drivers associated with this implementation – government and public authorities, industry, academia, policy makers, NGOs, the media – there is also civil societies and citizens or groups of citizens who are targets of surveillance technologies or who simply are or may be supporting the effects of those technologies. The issue related to this necessity of engaging a public is not just on which regards justice. Rather, it is also an issue which regards methodological requirement. Indeed, more we are around a system-to-be, more we are likely to identify from our respective perspective what the privacy issues at hand are. A relating remark was made about the important **distinction between end-user and surveilled people.** In this line, the asymmetrical stakeholder participation in different decision-making processes or Privacy Impact Assessment exercises regards to surveillance technologies must be taken into account. The largest

possible engagement of a public into the design of surveillance system is one of the responses to it.

(5) A fifth challenge, related to the third and the fourth ones, is **the success of the multidisciplinary approach** of PARIS' project. The first step in gathering the largest viewpoints on privacy begins there. Some methodological precautionary were provided in this introduction.

(6) A last challenge was outlined under the name of "zones of undecidability" and still need to be worked out. Indeed, starting from a multi-perspectivism approach does not solve the problem of how to articulate the different conceptions of privacy. This problem of articulation induces more precise questions, like: **WHAT**: what is holding the articulation (e.g. what technical system? A decision-making process? A practice of judging?)? **WHO**: who is in charge of articulating these different conceptions (e.g. a legislator? A judge? A computer scientist?)? And for which purposes (e.g. a decision-making process? An impact assessment? A judging practice?) **HOW**: What are the **procedures, the constraints, the criteria** adequate to reach this articulation with regard to the specific practice of the person (or people) who are in charge with this articulation? **SCOPE**: What are the scopes of the articulation and what are the zones which should not be articulated, regards to the responses to the previous questions? Those zones are the **zones of undecidability.** Those zones of undecidability are also of interests for the SALT Framework. There are several reasons for this. (1) In order to avoid for the system (the SALT Framework management tool) to take the place of decision-making processes that it is devoted to help finalizing and that is in charge of possible redefinition of the borders between zones which has to articulated and those which has to remain undecidable. (2) In order to be able to adapt e.g. to the emergence of new surveillance technologies, new negative impacts on privacy, new public claims regards to their privacy, new rules regards to privacy.

Several risks and precautionary were also stated.

(1) A first precautionary was expressed regards to **the relationships between surveillance and privacy**. A general classification of the kind of relationships between surveillance and privacy was offered as guidance tool for such thinking.

(2) Several methodological risks were identified regards to **the uses which are made of social sciences** in what is designated as the social acceptability paradigm.

Chapter II (Privacy from Socio-Political and Ethical Perspectives) is composed of three main sections.

The section 2.2 (Privacy from a Psychosocial Perspective) is dedicated to several issues. Psychology is an applied and academic field that studies the human mind and behaviour. Research in psychology seeks to understand and explain how we think, act and feel. Applied psychology focuses on the use of different psychosocial principles to solve real world problems. So it is important to take into account the psychology perspective when developing the SALT framework. It must consider its definition, its dimensions, its functions and the effect the lack of

privacy can cause on the population. People expect to have a balance between the privacy they desire and the one they obtain. We have to keep in mind that one of the objectives of PARIS is to help in developing privacy-enhanced surveillance systems. The study of privacy-security relationship from the point of view of social psychology must:

- Analyze the balance between desired privacy and achieved privacy in different types of spaces.
- Evaluate the optimal degree of surveillance in different spaces (public, semi-private and private).
- Analyze the acceptance of security systems implementation.
- 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.
- Evaluate the conflict among privacy, security and surveillance systems in the population.
- Analyze the social and psychological consequences of the invasion (lack) of privacy.

The section 2.3 (Privacy from a Socio-Political Perspective) contains two main inputs. (1) The claim of privacy as a social value is the keystone of the socio-political perspective on privacy. That is defending privacy as a social value, while challenging the sole addressing a challenge both to the conception of privacy as an individual right and/or value and to the one of its consequential turn of mind, that is the balancing relationships between privacy – conceived as an individual interest and/or value and/or right – and other social values such as (national) security. (2) The general claim in favour of privacy as a social value must be sustained by a conceptualization of privacy. Regards to the kind of conceptualization proposed, the effects are very different. In fact, the way privacy is conceptualised allows identifying very different kind of harms or concerns. This is worth emphasizing for the construction of the SALT framework which may be very different regards to the kind of taxonomy or conceptualization of privacy retained for its construction. Indeed, as a short term research aim, the reading of different existent taxonomies of privacy reveals that, while planning the construction of the taxonomy which will be relevant for the SALT Framework, it is necessary to be transparent in the methodological design of the taxonomy and reasons for choosing certain criteria rather than others.

Therefore a full subsection is dedicated to the identification – their outline and their interests for the SALT framework - different taxonomies of privacy which are of interest for the construction of the SALT Framework. In the next deliverable (D 2.2), a detailed analysis of their content still must be done regards to different details such as, for example: (1) The types of categories retains in the taxonomies. For example, a taxonomy which takes into account as a relevant criteria the intellectual property rights regime over information is very different than one which takes into account the social context of intersubjectivity; (2)Ttheir purpose. Indeed, the purpose of the taxonomy is not trivial. Helping Law enforcement or helping the design of a system-to-be which integrates Privacy-By-Design principles are two very different purposes. Regards to the kind of purpose, some common criteria to the analyzed taxonomy may be relevant (or not) for the SALT Framework; (3) the sources used. For example, legal sources or theoretical rationales built on the study and analyze of new and emerging technologies provide very different perspective on privacy; (4) The consequences and the types of consequence of the breaking of the criteria used in those different taxonomies. For example, the consequence may be law pursuit or a psychological effect on individuals. (5) Criticisms that have been addresses to those different taxonomies.

The several existent taxonomies which are worth being analyzed in the next deliverable are the following ones. (1) Finn, Wright and Friedewald: seven types of privacy (2) Steeves: privacy in intersubjective and social interactions (2) Solove: A taxonomy of privacy problems (3) Nissenbaum: contexts of privacy (4) Extended version of Privacy Impact Assessment.

The **section 2.4 (Privacy from an Ethical Perspective)**, proceeds to a review of the state-of-the art of the ethical perspective on privacy. Regards to the aim of this text of indentifying relevant criteria for the design of an ethical-based approach within the SALT framework, the focus is placed on (1) several ethical approaches that may be of interest for extracting ethical issues relating to surveillance technologies and (2) on several existent ethical frameworks. Different key sources are identified along this section and listed at this end with the recommendation to analyze them in details during the next step of this research. The next deliverable (D 2.2) will build on the findings of this section to provide a definitive list of requirements, adapted to the context of surveillance.

One specific remark is worth mentioning. **Surveillance technologies are a challenge for ethics.** If generally speaking, what is an "ethical issue" is in itself an issue, the question remains largely open regards to surveillance technologies. This is true for different reasons. A first reason is related to surveillance technologies itself. The argument is also true for ICT's technology at large. Indeed, "**the development of new ICTs and other security technologies are generally complicating the definition of the role of ethics**, as well as the identification of its theoretical approaches and operational instruments needed to address ICTs-related issues."[624] One explanation is that intentional actions are at the heart of traditional ethics of science and technology which thinks from the duo of the lonely scientific Frankenstein who intentionally creates his creature. However, scientific and technological developments "have the potential to bring **unintentional or highly unpredictable consequences that are usually the result of collective decisions**".[625] According to René von Schomberg, we do not have ethical theory at our disposal which would be an *Ethics of Knowledge Policy and Knowledge Assessment*[626] that is an ethics which addresses "both the aspect of **unintentional side consequences** (rather than intentional actions) and the **aspect of collective decisions** (rather than individual decisions)."[627] A second reason is that it is not sure that a specific field of research such as *surveillance ethics* exist. If **Gary T. Marx** was one of the first scholars who identified ethical issues and coined ethical tools in order to help in identifying them regards to surveillance technologies[628], most of the inspirations for offering ethical perspective on surveillance technologies come from ICTs ethics, computer ethics, ethics of technology, technology ethics, philosophy of technology,

[624] Ibid., 61.

[625] Ibid.

[626] René von Schomberg, "From the ethics of technology towards an Ethics of knowledge Policy abd Knwoledge Assessment," in *A working document for the European Commission services* (EU: European Commission's Directorate General for Research, 2007).

[627] Silvia Venier and Emilio Mordini, "Deliverable 4. FInal Report - A Privacy and Ethical Impact Assessment Framework for Emerging Sciences and Technologies," in *PRESCIENTproject. Privacy and emerging fields of scienbce and technoolgy: Towards a common framework for privacy and ethical assessmenttechnologies: Five case studies* (EC: Seventh Framework Programme (FP7), 2012), 62.

[628] G.T. Marx, "Ethics for the new surveillance", *The Information Society*, 14 (1998): 171-85.

professional ethics or applied ethics.[629] Few researches have been devoted to ethical issues relating specifically to surveillance technologies. **A lot of research still has to be done.**

Several sources were identified for further investigating towards ethical issues and criteria that may be relevant for their integration into the SALT framework. (1) The Lisbon treaty and its reformed version signed in 2007. (2) The Charter of Fundamental Rights. (3) The European Group on Ethics in Science and New Technologies (EGE) and specially its current work on an Opinion on the Ethics of Security and Surveillance Technologies which is to be finalised by the beginning of 2014, Opinion that will be the first one regards to those issues. A first public Round table is organised on 18 September 2013 in Brussels, involving experts from inside and outside academia, the Chairs of the National Ethics Councils (NECs) or equivalent bodies within the EU and beyond, representatives of the European and international institutions, civil society organizations and other stakeholders and members of the public. (4) Commission's Framework Programme(FP7) Seventh of research. Regards to researches funded under the Commission's Framework Programmes Seventh (FP7) of research and technological development, a set of ethical questions are asked to whom make proposals in order to help candidates in identifying ethical dilemmas and issues that may rise in their research[630]. The questions-based approach is particularly interesting. The specific *Data protection and privacy ethical guidelines*[631] is of interest and may be a start to identify ethical issues that may be taken into account in the SALT Framework. Nevertheless, other ethical issues listed for example under the heading *Informed Consent* must also be considered in more details.

Among different ethical approaches, we favoured an ethical approach that consider **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) Seventh 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 ethical perspective 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 stable responses.

Two existent **privacy frameworks regards to ethical issues** were presented. Other ones may still be identified during the next step of this research. Those two ones are of interest for the design of the SALT Framework and should be analysed in more details during the second step of this project and more specifically regards the two specific surveillance technologies that are at the core of the PARIS project: CCTV and biometric surveillance technologies. (1) **Beatrice von Silva-Tarouca Larsen: Ethics and CCTV surveillance.** Her book is especially interesting because it deals specifically CCTV surveillance technologies. (2) **David Wright: an ethical framework to assess the impact of ICTs**. This author makes very important proposals which are of interest for identifying relevant criteria for the SALT framework. He identifies different ethical values/principles/issue, explains them and offers a question-based approach with concrete

[629] For the distinction between those different fields of research, see: Silvia Venier and Emilio Mordini, "Deliverable 4. FInal Report - A Privacy and Ethical Impact Assessment Framework for Emerging Sciences and Technologies," in *PRESCIENTproject. Privacy and emerging fields of scienbce and technoolgy: Towards a common framework for privacy and ethical assessmenttechnologies: Five case studies* (EC: Seventh Framework Programme (FP7), 2012), 63.

[630] CORDIS: Community research and Developement Information Service, "Getting Through Ethics Review," in *Sventh Framework Programme (FP7)* (EU: European Commission). Available at: http://cordis.europa.eu/fp7/ethics_en.html#ethics-cl

[631] Expert Working Group on data protection and privacy, "Data Protection and privacy ethical guidelines," in *Ethical Review in FP7* (EU: European Commission, 2009). Avalaible at: ftp://ftp.cordis.europa.eu/pub/fp7/docs/privacy.doc

questions that may be addressed regards to all of those ethical issues. Here are those ethical values/principles and related ethical issues retained by Wright. Further analysis of those ethical values/principles and related ethical issues is needed and must imply a particularly focus on the questions formulated by Wright regards to each of them.

(2) Respect of autonomy (right to liberty)
   xii. Dignity
   xiii. Informed consent
   xiv. Nonmaleficience (avoiding harm)
   xv. Safety
   xvi. Social solidarity, inclusion and exclusion
   xvii. Isolation and substitution of human contact
   xviii. Discrimination and social sorting

(7) Beneficence
   i. Universal service
   ii. Accessibility
   iii. Value sensitive design
   iv. Sustainability

(8) Justice
   i. Equality and fairness (social justice)

(9) Privacy and data protection
   i. Collection limitation (data minimisation) and retention
   ii. Data quality
   iii. Purpose specification
   iv. Use limitation
   v. Confidentiality, security and protection of data
   vi. Transparency (openness)
   vii. Individual participation and access to data
   viii. Anonymity
   ix. Privacy of personal communications: monitoring and location tracking
   x. Privacy of the person
   xi. Privacy of personal behaviour

Beside the list of ethical values/principles and related issues, several points received a particularly strong attention because they are real **challenges for the design of the SALT framework**

(1) The need to involve stakeholders in the process, in the sense that stakeholders are defined as **all the people who are or may be interested in or are or may be affected by the outcome.** It will be **a challenge for the SALT framework** to be able to translate such a necessity to involve different stakeholders who are not solely the experts who prepare the SALT framework. It is evident that **the involvement of stakeholders** – more than experts and less than a general public – is out of the scope of a SALT framework. The

same can be said about the integration of the ethical tools above mentioned, **ethical tools** which may facilitate the involvement of stakeholders. However, I suggest investigating about the possible integration of several questions about the involvement of stakeholder into the SALT framework: Were stakeholders consulted or are going to be consulted? Who are those stakeholders? Is there one or several ethical tool which are used in order to help the involvement of those stakeholders and which ones?

(2) Another challenge for the SALT framework will 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).

(3) A remark is worth to be mentioned here, regards to the SALT framework. The specific people or person or group of people who use the SALT framework should be **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 different stakeholders.

Chapter 3 (Privacy from a Legal Perspective - European Legal Framework for Privacy and Data Protection) dedicated to the state of the art regarding privacy and data protection requirements within the EU allowed us to seeing that the objective to achieve a correct balance is actually a concern shared at various levels, legislative and operational, and a challenge for the European Union and its Member States. 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 identifying pending issues regarding the very perimeter of the SALT framework.

Preliminary criteria and perimeter: integration of privacy *and* data protection requirements

As far as the identification of privacy interests are at stake, we have suggested that the SALT framework establish as a principle that any envisaged surveillance technology involve potential concerns according to Article 8§1 of the ECHR. In our view, this could be established as a precautionary principle. We have then claimed that the SALT framework should instead focus its attention on the way to integrate the elements of the ECHR caselaw in relation to legal and legitimate interferences. We propose to build on the permissible limitation test proposed by P. De Hert, who has identified seven core elements: the technology should be used in accordance with and as provided by the law; the technology or processing should serve a legitimate aim; the technology should not violate the core aspects of the privacy rights; the technology should be necessary in a democratic society; the technology should nor have or give unfettered discretion; the technology should be appropriate, least intrusive and proportionate; the technology should be consistent with other human rights.[632] The next deliverable will therefore focus on the possibilities to operationalize the principle of proportionality in the SALT framework.

[632] Paul De Hert, "A Human Rights Perspective on Privacy and Data Protection Impact Assessment"s, *op. cit.*, p. 33-76

Besides, the fundamental principles of data protection, as expressed in Directive 95/46 also provide the essential elements that any surveillance technology shall integrate. We have seen that the protection of personal data is not limited to data security requirements and that other elements (definition of purpose(s), principle of minimisation, restriction to onward transfers, contractual relationships between controllers and processors, limited retention duration et cetera) are all relevant requirements that should be taken into account by the SALT framework. For this task, the privacy and data protection impact assessment framework regarding RFID applications[633] published by the European Commission constitutes a good starting point.

Challenge: operationalizing proportionality into a process

One of the essential task of the future work during the next phases of the PARIS project 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 et cetera) 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.

Pending issue: extent of integration of national requirements

One of the main issues 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. In other words, it also questions the extent to which the SALT framework intends to integrate the national state of law. According to the Member State and/or the surveillance technology, such integration may be more or less complex. For example, in the case of France and biometric technologies, the CNIL has developed extensive 'jurisprudence' in the framework of its power of authorization. An in-depth analysis of CNIL's deliberations may allow identifying the underlying policy of the CNIL in this respect. The fundamental criteria of such 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. On the contrary, in the case of Belgium where there is almost no guidance available from the Privacy Commission, the SALT framework in relation to biometrics may well be limited to an overall impact assessment. It will be difficult to integrate more criteria than those generally defined under the Privacy Act and the proportionality principle. The added value that the SALT framework could bring should nevertheless not be underestimated. A lots of work still have to be done to familiarize data

[633] European Commission, Privacy and Data Protection Impact Assessment Framework for RFID Applications, 12 Januray 2011, available at : http://cordis.europa.eu/fp7/ict/enet/documents/rfid-pia-framework-final.pdf

controllers, processors and system designers with the fundamental principles of privacy and data protection.

Besides, the integration of national state of law into the SALT framework also raise issues in relation to its compatibility with European privacy and data protection established standards. In the ideal of the world, the hierarchy of norms commands that each Member States national laws and regulations (and Data Protection Authority's interpretative work) complied with higher European (EU-ECHR) established standards and norms. However, in the real world, the implementation and application at national level of those standards may be more or less consistent with higher ranked European norms. The conciliation into the SALT framework of the fundamental principle of proportionality and European data protection standards may reveal contradictions. For instance, although the case of the United Kingdom has not been examined in the present report, current caselaw across the Channel raise concerns, not to say contradictions, with European interpretations of the right to privacy and data protection. A judgement of 2003 has developed a narrow interpretation of the notion of personal data[634] that has the consequence to leave out many users of basic CCTV systems out of the scope of the Data Protection Act, although this is explicitly contrary to the objective of Directive 95/46.[635] Applying the SALT framework to videosurveillance in the United Kingdom for instance may reveal specific difficulties, if the SALT framework has the double and contradictory aim to integrate both European and UK state of the law. This raises the issue of the extent to which the SALT framework should be 'nationally rule-based ' (based on national positive law) or should be limited to a 'European standard-based' (based on European recognized fundamental principles of privacy and data protection known as 'standards'). If both approaches should ideally be fully consistent and compatible, there may be difficulties to reconcile them in some cases.

The chapter 4 (Accountability: A Way to Ensure Transparency and Trust) proceeds to a review of the state-of-the-art on the principle of accountability in view of extracting preliminary criteria for the design of an accountability-based approach for personal data governance practices within the SALT framework. The different initiatives reviewed do however not address the specifics of surveillance practices, which means that further work is required to tailor these preliminary criteria to the context of surveillance. The next deliverable (D.2.2.) will build on the findings of this Chapter to provide a definitive list of requirements, adapted to the context of surveillance.

Accountability is a concept 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

[634] *Durant v. The Financial Services Authrority*, Court of Appeal, 8 December 2003. See the explanations of Douwe Korff, in *United Kingdom Country Study*, 4-11. This study was carried out in the framework of a European Commission research services contract destined to provide a Comparative study on different approaches to new privacy challenges, June 2010, available here : http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_country_report_A6_united_kingdom.pdf

[635] See the analysis of the consequences of the Durant case to CCTV by Lilian Edwards, "Switching off the Surveillance society? Legal Regulation of CCTV in the United Knigdom", in *Reasonable Expectations of Privacy? Eleven Country Reports on Camera Surveillance and Workplace Privacy*, ed. Sjaak Nouwt et al. (The Hague: Cambridge University Press, 2005), 96-102

passive sense, as “mechanism of control” [2]. Both approaches are of interest for the SALT Framework:

3) 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.
4) Accountability understood in its narrow or passive sense, i.e. as a coercitive means to increase legal compliance, as a way to exercise constrain 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.

Within the SALT framework, the first meaning of accountability will be more fitted to address the need to increase the legitimacy of decisions which involve a balancing exercise between privacy and surveillance interests. Accountability mechanisms relying on the first meaning could address the needs of decision-makers when considering the implementation of surveillance systems. Accountability mechanisms understood as compliance instruments will operate at a lower level and will rather tend on providing trust in the design and further use of surveillance systems. They will rather be directed to system developers and operators during the life-cycle of the surveillance system.

As elaborated in section 2 both concepts of accountability share common features. In short, accountability relationships involve a third party external to the accountable agent and in which the latter is asked to answer the requests of the former, which may result in corrective actions taken by the agent. The main difference between the broad and narrow sense of accountability relies on whether the third party to whom the account is given owns rights of authority over the agent and thus whether the accountability process can end up in the imposition of sanctions or the agent been required to integrate corrections to its actions or decisions. When accountability is understood in its broad sense the impact of the whole process is largely defined by the agent itself, while in the second case the process might end up in a decision of the third party which should mandatorily be enforced by the agent.

The graph below shows, in a simplified way and with the only purpose of illustrating the different notions used in this Chapter, how accountability relationships in surveillance systems could arise and intertwine. The different actors part to these relationships appears either on the first line, if they act as accountors (Who gives the account), or in the second line if they act as accountees (To whom is the account given). The third line indicates what can be the object of the account. Finally the fourth line indicates whether this relationship is likely to be framed as an accountability relationship understood in its broad or narrow sense (respectively, as “answerability” or “compliance”).

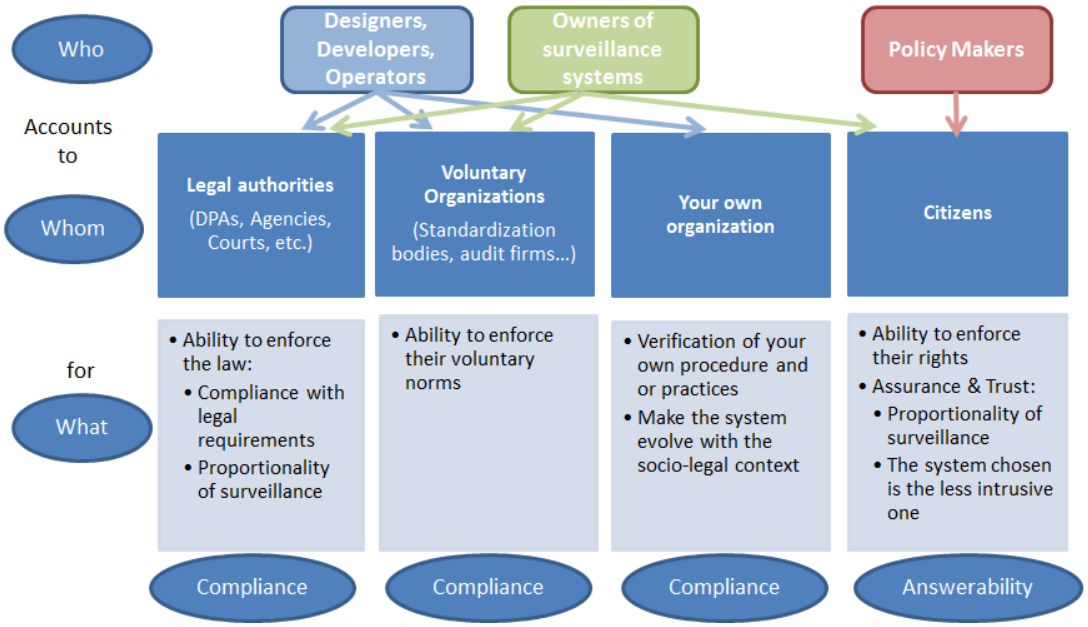

Figure 8: Accountability Relationships

The review of the different initiatives in view of the introduction of an accountability-based approach within the data protection framework in section 3 shows that they approach accountability as implementation and enforcement mechanism of the existing framework (compliance). However, none of the policy instruments reviewed provides for a definition of the principle of accountability. In PARIS, we will, as first step, rely on the definition proposed by the Accountability Projects who gathered experts from privacy authorities, the private sector, NGOs and Academia. Accountability is defined as "*a demonstrable acknowledgement and assumption of responsibility for having in place appropriate policies and procedures, and promotion of good practices that include correction and remediation for failures and misconduct.*" In that context, accountability is understood as the obligation and/or willingness to demonstrate and take responsibility for performance in light of agreed-upon expectations.

Accountability relationships will differ depending on the parties to the relationship, its content and motivation. Four elements will thus determine the shapes and meaning of an accountability relationship: who is accountable to whom, why and what for. These four elements should be clearly identified and made explicit before accountability mechanisms are incorporate into general policies or to organisations' policies.

The design of accountability processes should thus start by defining the following elements:

1. **Identify the stakeholders**, i.e. whom the organization is answering to. Different stakeholders will have different expectations, generating different types of relationships.
2. Make explicit the **motivation** underlying the accountability relationship, i.e. why the organization decides to engage into such procedure. An organization can engage into the implementation of accountability mechanisms to ensure

compliance but also to give added-value to its products or greater legitimacy to its decisions.

3. Identify the **nature of the account** that should be given, i.e. what should be the content and extent of the accountability procedure. This comes to defining which kind of responsibility or power has been entrusted to the agent and thus what this agent should be answerable for.

As shown by the Accountability projects, within the data protection framework, three stakeholders can be identified, all of them having different expectations, namely:

- **Businesses** are concerned about what might be expected of them in an accountability system, how their effort to meet these expectations would be measured and how the rules related to accountability would be defined and enforced
- **Privacy enforcement agencies** are concerned about how accountability might work under local law, how do enforcement agencies measure an organisation's willingness and capacity to protect information when it is no longer in the privacy protection agency's jurisdiction, how does the agency work with and trust agencies in other jurisdictions
- **Consumers advocates**, representing **citizens**, worry that accountability would lessen the individual's ability to make his own determination about appropriate use of information pertaining to him.

Once the basic characteristic features of the accountability relationship at stake has been defined and identified, the methodology proposed by the Global Accountability Framework to set up accountability mechanisms can then be used as general guideline. The work carried out by the Accountability projects and the Canadian Privacy Commissioners, as well as several policy instruments such as Madrid Declaration of the European Commission proposals of the Data Protection Reform, help specifying such general guidelines to the specific context of data protection.

For the organization which wants to implement accountability mechanisms for its data governance practices, this means to set up:

- An **Accountability strategy** which identifies the stakeholders to the process, their expectations, the mission statement of the organization for this process (motivation/intentions) and the mechanisms put in place.
    - Adoption of internal, biding and enforceable privacy policies consistent with external criteria (law, biding codes of conducts, international standards).
    - Organisation commitment to accountability: support of top management, allocation of sufficient resources and adequately trained staff.
    - Appointment of a person responsible for the overview of the policies set forth such as a Data Protection Officer.
    - The implementation of the principles of privacy-by-design and privacy-by-default within the organization for the monitoring of products and services design.

  - **Transparency mechanisms** which gives visibility for the stakeholders of the actions taken in view of the obligation to give an account such as privacy notices, icons, videos.
  - **Participation mechanisms** which allow stakeholders to involve into a dialogue with the organization, obtain the information required, ask further explanation, and contest the narrative given by the agent. Organizations can be for instance obliged to provide information on their accountability mechanisms to supervisory authorities and/or other stakeholders (such as data subjects) on request.

- **Evaluation mechanisms** which allows the agent to obtain feedback over their own accountability mechanisms in view of further improvements. This requirement refers to systems for internal, ongoing oversight and assurance reviews and external verification.

- **Complaint and response mechanisms**, which allows an interaction with their stakeholders, so they can provide feedback on the accountability process. This might involve the implementation of complaint procedure and means for remediation.

Finally, as framed by the Accountability projects, it is worth reminding that when introducing an accountability scheme within the legal framework, such scheme can be modulated into several stages, depending on the organisation's level of commitment/rights of authority given to the accountee. The first two stages could be approached as accountability relationships in their broad sense, in that the accountor (who should be identified but is likely to be incardinated into citizens and consumers) does not have any right of authority over the accountor, in the sense of imposing sanctions. The last two stages reflect accountability relationships understood in their narrow sense, where the accountor should abide by the decisions made by the accountee.

1. First stage.- The organization takes appropriate measures to establish processes and procedures that implement its privacy policies.
2. Second stage.- The organization self-certified that it meets the requirements of accountability.
3. Third stage.- The supervisory authority or recognized accountability agent reviews such filings and provide some form of acceptance of the certification.
4. Fourth stage.- The organization submits to enforcement by the supervisory authority or recognized accountability agent.

There are also **pending issues** that might be taken into account in further steps of this research. As far as accountability is concerned, the position taken in PARIS is that it can significantly enhance privacy protection in the context of surveillance provided that sufficient guarantees are provided.

Accountability is a critical feature of surveillance systems: Accountability is especially needed for surveillance systems because it is impossible to rely entirely on *ex ante* protection tools such as consent, obfuscation or anonymisation tools. Whatever privacy enhancing technologies are used, personal data will be collected (and very often even potentially sensitive data) and the only protection for individuals will be the guarantee that those data will be used properly (by the right people for the right purpose).

But accountability in the context of surveillance rises challenging issues. Among these issues, let us mention:

- Actors: multiple actors pay a role in surveillance systems (owner, operators, processors, designers, auditors, subjects, etc.) and their interests may be conflicting.
- Data: multiple modalities (types of data) can be used by surveillance systems, with different levels of precision.
- Processing: specific operations (blurring, matching, etc.) have to be taken into account. In addition, knowledge inference (aggregation, data mining) raises further issues (traceability, status of the inferred knowledge, etc.).

In order for accountability to bring the required level of guarantee to individuals, an accountability framework should[636]:

- Cover not only accountability of policies and procedures, but also accountability of practices (following Colin Benett's terminology).
- Cover the whole data life cycle (collection, inference, copy, transfer, sharing, access, use by the controller, correction by the subject, deletion, etc.).
- Be supported by definitions of policies and procedures which are defined precisely enough for auditors to establish the compliance of data controllers (and hence to increase the trustworthiness of the whole process and the confidence of the subjects).

One of the goals of PARIS with respect to accountability is to provide a framework and guidelines for such an accountability framework.

In **chapter 5 (Privacy from a Computer Engineering Perspective),** the focus of the SALT framework is on system engineering, i.e., methods and technologies to design and build surveillance systems that are privacy friendly and preserving. Therefore, in this deliverable, we investigate several fundamentals related to system engineering at a conceptual level. As described in Chapter 5, privacy principles, concepts, and enhancement technologies are closely related basics for electronic privacy. The overarching privacy principles provide guidelines. Privacy concepts extend these guidelines to specific technological domains. Privacy-enhanced technologies implement the concepts and thus are the technical measures to achieve privacy.

Note that neither legal nor technical means alone can achieve privacy in surveillance systems. Laws can be bypassed or violations can be undetected if there are no technical measures in place. Technical measures would suffer from deterrent powers if legal requirements and accountability are not defined. As a result, we regard system engineering as a technical enforcement of the SALT framework that complements the other pillars.

[636] Butin, Denis, Marcos Chicote and Daniel Le Métayer, Strong Accountability: Beyond Vague Promises in Serge Gutwirth, Ronald Leenes & Paul De Hert (eds.), *Reloading data protection*, Springer, Dordrecht, 2014, forthcoming.

Video surveillance system is basically different from other information and communication systems. Hence the methods and technologies are domain-specific. Nevertheless, we foresee that many concepts and technical measures developed in other domains are applicable to surveillance systems with slight modifications. We also foresee that those measures currently used for information security from risk assessment to access control are highly relevant to privacy in surveillance systems. These topics will be further developed to be integrated into the SALT framework in the next round of our work.

It is also worth to notice that little by little, the user's privacy is being increasingly threatened by the amazing improvement of technologies. For example, hardware improvements have led to an increase of the speed at which information can be analyzed, and of the storage capacity of such information. In addition, the rising connectedness over networks has made possible to share and process large amounts of information. Finally, software advances have greatly improved the algorithms for extracting information stored both, locally and remotely on the network.

All these improvements have led to the appearance of new surveillance technologies, which depending on their use could damage individual's privacy. As we show in this document, according to their technology, surveillance systems can be classified into: visual surveillance, biometrics, dataveillance, communications surveillance, sensors, and location technologies. New surveillance is less visible and more continuous in time and space, it provides fewer opportunities for targets to object to or prevent the surveillance, it is greater in analytical power, it produces more enduring data, it is faster and more widely diffused, and it is less expensive.

Such progress and technologies generate more data on an individual. Therefore, it is necessary to take into account from the visualization and design of the product or application, all privacy related aspects in order to minimize the impact on the user.

7 References

7.1 General literature

Agrawal, Rakesh, Jerry Kiernan, Ramakrishnan Srikant, and Yirong Xu. "Hippocartic database." *VLDB '02:Proceeding of the 28th international conference on Very Large Data Bases*, 2002: 143-154.

Alhadeff, Joseph, Van Alsenoy, Brendan and Dumortier, Jos. “The Accountability Principle in Data Protection Regulation: Origin, Development and Future Directions”, in *Managing Privacy through Accountability,* edited by Daniel Guagnin, Leon Hempel, Carla Ilten, Inga Kroener, Daniel Neyland and Hector Postigo, 49-82. Palgrave Macmillan, 2012.

Altman, Irwin. “Privacy regulation: culturally universal or culturally specific.” *Journal of Social Issues*, 38 (1977): 66-84.

Altman, Irwin. *The environment and social behavior: Privacy, personal space, territoriality and crowding*. Monterey (Ca.): Books/Cole, 1975.

Amicelle, Anthony, et al. "D1.1. Report on Theoretical Frameworks and Previous Empirical Research." In *PACT. Public perception of security and privacy. Assessing knowledge Collecting evidence, Translating research into action*. EC: Seventh Framework Programme, 2012.

Amoore, L., and M. De Goede (ed.). *Risk and the War on Terror.* London: Routledge, 2008.

Arai-Tahahashi, Yutaka. *The margin of appreciation doctrine and the principle of proportionality in the jurisprudence of the ECHR.* Antwerpen: Intersentia, 2002.

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

Arthur, Charles “Google ‘to be told by EU to unravel privacy policy’”, *The Guardian*, 15 October 2012. Available at: http://www.guardian.co.uk/technology/2012/oct/15/google-privacy-policy?newsfeed=true

Barben, Daniel. "Analyszing acceptance politics: Towards an epistemological shift in the public understanding of science and technology." *Public Undesrtanding of Science* 19(3), no. 3 (2010): 274-292.

Barefoot, John C., Howard Hoople, and David McClay. “Avoidance of an act which would violate personal space.” *Psychonomic Science*, 28 (1972): 205-206.

Barth, Adam, Anupam Datta, John C. Mitchell, and Helen Nissenbaum. "Privacy and Contextual Integrity: Framework and Applications." *SP '06: Proceedings of the 2006 IEEE Symposium on Security and Privacy*, May, 2006: 184-198.

Baum, Andrew and Carl I. Greenberg. “Waiting for a crowd: The behavioral and perceptual effects of anticipating crowding.” *Journal of Personality and Social Psychology*, 32 (1975): 671–679.

Beauchamp, Tom L., and Childress, James F., 2008, « *Principles of Biomedical Ethics* », 6th edition, New York:Oxford University Press.

Beck, Ulrich. *Risk Society: Towards a New Modernity.* London: Sage, 1992.

Beekman, V. and F. W. A. Brom, "Ethical tools to support systematic public deliberations about the ethical aspects of agricultural biotechnologies", *Journal of Agricultural and Environmental Ethics*, 20(1) (2007): 3-12.

Beekman, V. et al., "Ethical Bio-Technology Assessment Tools for Agriculture and Food Production. Final Report Ethical Bio-TA Tools," in *Ethical Bio-TA Tools* (EC: Fifth Framework Programme, February 2006).

Bennett, Colin. “International privacy standards: can accountability be adequate?”, *Privacy Laws and Business International* 106 (August 2010): 21-23

Bennett, Colin. "In the defense of privacy. The concept and the regime." *Surveillance & Society* 8 (4) (2011): 485-496.

Bennett, Colin. "The Accountability Approach to Privacy and Data Protection: Assumptions and Caveat", in *Managing Privacy through Accountability*, edited by Daniel Guagnin, Leon Hempel, Carla Ilten, Inga Kroener, Daniel Neyland and Hector Postigo, 33-48. Palgrave Macmillan, 2012.

Bennett, Colin, and Charles Raab. *The Governance of Privacy. Policy instruments in Global Perspective*. Cambridge (MA): MIT Press, 2006.

Bennett, Colin, and Charles Raab. "The privacy paradigm." In *The Governance of Privacy. Policy instruments in Global Perspective*, edited by Colin Bennett and Charles Raab, 3-28. Cambridge (MA): MIT Press, 2006.

Bernier, Chantal. « Intégrer le droit à la vie privée aux mesures de sécurité publique du 21ème siècle : une expérience canadienne », in *Circulation Internationale de l'Information et Sécurité*, edited by Karim Benyekhlef and Esther Mitjans 139-152, Montréal: Thémis, 2013.

Bigo, Didier, and Anastassia Tsoukala (ed.). *Terror, Insecurity and Liberty: lliberal Practices of Liberal Regimes after 9/11.* London: Routledge, 2008.

Blagescu, Monica, De Las Casas, Lucy and Lloyd, Robert. "Pathways to accountability, A short guide to the GAP framework", edited by One World Trust (2005), available at: http://www.who.int/management/partnerships/accountability/PathwaysAccountabilityGAPFramework.pdf

Boehm, Franzisca. *Information Sharing and Data Protection in the Area of Freedom, Security and Justice*. Springer, 2012.

Bovens, Mark**.** "Two Concepts of Accountability: Accountability as a Virtue and as a Mechanism", *West European Politics* 33 (2010): 946 — 967 http://dx.doi.org/10.1080/01402382.2010.486119**.**

Buttarelli, Giovanni. *Protection of personal data with regard to surveillance and Guiding principles for the protection of individuals with regard to the collection and processing of data by means of video surveillance*. Report for the European Commission. 2000. Available at: http://www.coe.int/t/dghl/standardsetting/dataprotection/Reports/Report_Buttarelli_2000.pdf

Butin, Denis, Marcos Chicote and Daniel Le Métayer, Strong Accountability: Beyond Vague Promises in Serge Gutwirth, Ronald Leenes & Paul De Hert (eds.), *Reloading data protection*, Springer, Dordrecht, 2014, forthcoming.

Butler, J. (2005), « Giving An Account of Oneself », Fordham University Press; 4 edition. We read the following french traduction, and we refer to it in this paper : Butler, J (2007) « Le récit de soi », PUF, Pratiques théoriques, 2007 (2005).

Cavallaro, Andrea. "Privacy in Video Surveillance." *IEEE Signal Processing Magazine*, 2007: 168-169.

Cavoukian, Ann. *Privacy by Design ... Take the Chalenge.* Ontario (Canada): Information and Privacy Commissioner of Ontario, 2009.

—. *Privacy by Design: The 7 Foundational Principles Implementation and Mapping of Fair Information Practices.* Ontario (Canada): Information & Privacy Commisionner of Ontario, Originally published: May 2010, Revised January: 2011.

Cavoukian, Ann, Abrams, Martin E. and Taylor, Scott. "Privacy by Design: essential for organizational accountability and strong business practices", in *Identity in the Information*

Society Vol. 3 Issue 2 (2010): 405-413, available at: http://link.springer.com/article/10.1007%2Fs12394-010-0053-z

Clarke, Roger. "Introduction to Dataveillance and Information Privacy, and Definitions of Terms", *Xamas Consultancy*, 1997: Available at: http://www.rogerclarke.com/DV/Intro.html.

Clarke, Roger. "An evaluation of privacy impact assessment guidance documents", *International Data Privacy Law*, Vol.1 N°2 2011, 111-120. Available at: http://rogerclarke.com/DV/PIAG-Eva.html

Cockfield, Arthur J. "Protecting the Social Value of Privacy in the Context of Dtate INverstigations Using New Technologies", *U.B.C. Law Review*, 40 (1) (2007): 41-68.

Costa, Luiz and Poullet, Yves. "Privacy and the Regulation of 2012", *Computer Law & Security Review* 28 (2012): 254-262

Couts, Andrew. *State of the Web: Who killed privacy? You did.* http://www.digitaltrends.com/opinion/state-of-the-web-who-killed-privacy/ (accessed June 11, 2013).

Davis, Darren W., and Brian D. Silver. "Civil Liberties vs. Security: Public Opinion in the Context of the Terrorist Attacks on America." *American Journal of Political Science* 48 (1) (2004): 28-46.

DeCew, Judith. "Privacy." In *The Standfordf Encyclopedia of Philosophy*, edited by Edward N. Zalta. Standford: The Metaphysics Research Lab, 2012). Available at http://plato.stanford.edu/entries/privacy/.

De Hert, Paul. "Balancing security and liberty within the European human rights framework. A critical reading of the Court's case law in the light of surveillance and criminal law enforcement strategies after 9/11", *Utrecht Law Review* Vol. 1 issue 1 (2005)

De Hert, Paul. "A Human Rights Perspective on Privacy and Data Protection Impact Assessments", in *Privacy Impact Assessment,* edited by David Wright and Paul de Hert, 33-76. London, Brussels: Springer, 2012.

De Hert, Paul. "Accountability and system responsibility: New Concepts in Data Protection Law and Human Rights Law", in *Managing Privacy through Accountability,* edited by Daniel Guagnin, Leon Hempel, Carla Ilten, Inga Kroener, Daniel Neyland and Hector Postigo, 193-232, Palgrave Macmillan, 2012.

De Hert, Paul and Gutwirth, Serge. "Interoperability of police databases within the EU: an accountable political choice?", *TILT Law & Technology Working Paper series* (2006) available at http://ssrn.com/abstract=971855

De Hert, Paul and Gutwirth, Serge. "Privacy, data protection and law enforcement. Opacity of the individual and transparency of power", in *Privacy and the criminal law*, edited by E. Claes et al., 61-104. Antwerpen/Oxford: Intersensia, 2006.

Paul De Hert, Dariusz Kloza and David Wright, "Deliverable D3: Recommandations of a privacy impact assessment framework for the European Union," in *PIAF: Privacy Impact Assessment Framework* (Brussels-London: European Commission - Directorate Generale Justice, 2012).

De Schutter, Olivier, *Fonction de juger et droits fondamentaux. Transformation du contrôle juridictionnel dans les ordres juridiques américain et européens*. Bruxelles: Bruylant, 1999.

Dewey, J., *Démocratie et éducation*, Armand Collin, Paris, 1975.

Dewey, John. *The public and its problems.* Ohio: Swallow Press, Ohio University Press, 1991.

Dewey, J., 1998, The Essential Dewey, L. Hickman and T.M. Alexander (ed.), Bloomington: Indiana University Press.

Dignan, Larry. *Privacy is dead: So what if you friended the NSA?* http://www.zdnet.com/privacy-is-dead-so-what-if-you-friended-the-nsa-7000016507/ (accessed June 9, 2013).

Dourish, Paul, and Genevieve Bell. *Divining a digital future.* Cambridge, Massachusetts: MIT Press, 2011.

Dourish, Paul, and Ken Anderson. "Collective Information Practice: Exploring Privacy and Security and Culture Phenomena." *Human-Computer Interaction* 21(3) (2006): 319-342.

Dumortier, Franck, Gayrel, Claire, Jouret, Joelle, Moreau, Damien and Poullet, Yves. « La protection des données dans l'Espace européen de Liberté, de Sécurité et de Justice », *Journal de Droit Européen* 166 (2010) : 33-46

Dumortier, Franck. « Caméras de surveillance: la cohabitation légale reste houleuse…A propos du champ d'application de la loi du 21 mars 2007 et de sa coexistence avec d'autres normes réglant les caméras de surveillance », in *La vidéosurveillance. Entre usages politiques et pratiques policières*, under the direction of Marie-Sophie Devresse and Jean Pieret, Bruxelles: Politeia, 2010.

Edwards, Lilian. "Switching off the Surveillance society? Legal Regulation of CCTV in the United Knigdom", in *Reasonable Expectations of Privacy? Eleven Country Reports on Camera Surveillance and Workplace Privacy*, edited by Sjaak Nouwt , Berend R. de Vries and Corien Prins, 91-114. The Hague: Cambridge University Press, 2005.

Efran, Michael G. and J. Allan Cheyn. "Affective concomitants of the invasion of shared space: Behavioral, physiological, and verbal indicators." *Journal of Personality and Social Psychology*, 29 (1974): 219- 226.

Finn, Rachel L., David Wright, and Michael Friedewald. "Seven Types of Privacy." In *European Data Protection: Coming of Age*, edited by Serge Gutwirth, 3-32. Dordrecht: Springer, 2013.

Fisher, Jeffrey D., Paul A. Bell and Andrew Baum. *Environmental Psychology*, 2nd Edition. New York: Holt, Rinehart and Winston, 1984.

Foucault, Michel. *Discipline and Punish:The birth of the prison.* New York: Random House, 1975.

Fried, Matthew L. and Victor J. DeFazio. "Territoriality and boundary conflicts in the subway." *Psychiatry*, 37 (1974): 47–59.

Frieddewald, Michael, and Rocco Bellanova. "Deliverable 1.1: Smart Surveillance - State of the Art." In *SAPIENT. Supporting fundamental Al rights, Privacy and Ethics in surveillance Technologies*. EC: Seven Frameworks Programme, January 2012.

Friedewald, Michael. "Deliverable 2: Engaging stakeholders and civil society in the assessment of surveillance practices." In *SAPIENT: Supporting fundamentAl rights, PrIvacy and Ethics in surveillaNce Technologies*. EU: Seven Framework Programme for Research and technological development, 2012.

Fung, Benjamin C. M., Ke Wang, Rui Chen, and Philip S. Yu. "Privacy-Preserving data publishing: a survey of recent developments." *ACM Computing Surveys*, 42(4), June 2010.

García, Alberto Crespo, et al. "D1.3. Report on Technology Taxonomy and Mapping." *PACCT: Public perception of security and privacy: Assessing knowledge, Collecting evidence, Translating research into action*, June 2012.

Gayrel, Claire and Poullet, Yves. “Methodology Balancing Privacy v. Security, the Increasing Role of Impact Assessment in the EU. Benefits and Risks”, in *Circulation Internationale de l’Information et Sécurité*, edited by Karim Benyekhlef et Esther Mitjans, 153-180, Montréal: Thémis, 2013.

Gellman, Barton, and Laura Poitras. "U.S., British intelligence mining data from nine U.S. INternet companies in broad secret program." *The Washington Post*, June 2013, June 6.

Giddens, Anthony. *The Constitution of Society. Outline of the Theory of Structuration.* Cambridge: Polity, 1984.

Gifford, Robert. *Environmental Psychology: Principles and Practice,* 4th edition. Canada: Optimal Books, 2007.

Gonzáles Fuster, Gloria. “Security and the future of personal data protection in the European Union”, *Security and Human Rights* 28 (2012): 331-342

Goujon, Philippe and Catherine Flick, "Givernance approaches. A critical appraisal of theory and practice. Deliverable 4.1 ," in *ETICA: Ethical Issues of Emerging ICT Applications* (EC: Seventh Framework Programme, 2011).

Gürses, Seda. *Multilateral Privacy Requirements Analysis in Online Social Network Service. PhD thesis.* Leuven: HMDB, Department of Computer Science, K.U.L., 2010.

Gürses, Seda, and Bettina Berendt. "PETs in the Surveillance Society. A critical review of the potentials and limitations of the privacy as confidentiality paradigm." In *Data protection in a profiled world*, edited by Serge Gutwirth, Yves Poullet and Paul De Hert. Dordrecht Heidelberg London New York: Springler, 2010.

Gutwirth, Serge. *Privacy and the Information Age.* Lanham/Boulder/New York/Oxford: Rowman 1 Littlefield Publishers, 2002.

Gutwirth, Serge, et al. "Deliverable D1: Legal, social, economic and ethical conceptualisations of privacy and data protection." In *PRESCIENT. Privacy and emerging fields of science and technology: Towards a common framework for privacy and ethical assessment*. EC: Seventh Framework Programme, March 2011.

Hammer Michael and Whitty, Brendan. *Accountability principles for policy oriented research organisations. A guide to the framework and online database*, One World Trust: 2011.

Hammer, Michael. IBRD Accountability Assessment, Briefing, 20 July 2012, One World Trust, 2012, http://oneworldtrust.org/climategovernance/sites/default/files/publications/Michael%20Hammer/PEAGCCG%20IBRD%20Acc%20Assess%20summary%20briefing%20July%202012%20v3.pdf

Donna Haraway, "Situated Knowledges: The Science Question in Feminism and the Privilege of Partial Perspective", *Feminists Studies*, 14 (3) (1988): 575-99.

Harper, Jim, and Solveig M. Singleton. *With A Grain of Salt: What Consumer Privacy Surveys Don't Tell Us.* . Available at SSRN: http://ssrn.com/abstract=299930 or http://dx.doi.org/10.2139/ssrn.299930.

Havas Worldwide. *This Digital Life*. *Prosumer Report,* vol. 13 (2012): 10-21.

Herveg, Jean and Gayrel, Claire. “Chronique de Jurisprudence de la Cour européenne des Droits de l’Homme 2002-2008 », *Revue du Droit des Technologies de l’Information* 37 (2009) : 104-115.

Herveg, Jean. « Chronique de Jurisprudence de la Cour européenne des Droits de l'Homme 2009-2011 » *, Revue du Droit des Technologies de l'Information* 48-49 (2012) : 99_116.

Hofkirchner, Wolfgang. *Twenty questions about a Unified Theory of Information. A Short Exploration into Information from a Complex System View.* Litchfield Park (AZ): Emergent Publications, 2010.

Horlick-Jones, Tom. *The GM debate: risk, politics and public engagement.* London: Routledge, 2007.

http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf.

http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf.

http://oneworldtrust.org/climategovernance/sites/default/files/publications/testmanager/OWT%20128%20-%20The%20Global%20Accountability%20Framework%202011.pdf

Johnson, Bobbie. "Privacy no longer a social norm, says Facebook founder." *The Guardian*, Jan 11 Jan 2010.

Krämer, Beatrice. "Classification of generic places: explorations with implications for evaluation." *Journal of Environmental Psychology*, 15 (1995): 3-22.

Kupritz, Virginia W. "Privacy management at work: A conceptual model." *Journal of Architectural and Planning Research*, 17 (2000): 47–63.

Kurath, Monica, and Priska Gisler. "Informing, involving and engaging: Science communication in the ages of atom, bio- and nanotechnology." *Public Understanding of Science* 18 (5) (2009): 559-573.

Ladrière, J., L'éthique dans l'univers de la rationalité, Artel/fides, Namur, 1997.

Latour, Bruno. *Reassembling the Social: An Introduction to Actor-Network Theory.* Oxford, UK: Oxford University Pess, 2005.

Levidow, L., and Cl Marris. "Science and Governance in Europe: lessons from the case of agricultural biotechnology." *Science and public policy*, 2001: 345-360.

Liu, Nancy Yue. *Bio-Privacy, Privacy Regulations and the Challenge of Biometrics*. New York: Routledge, 2012.

LLP, Trilateral Research and Consulting. "Deliverable D1.1: Surveillance, fighting crime and violence." In *IRISS: INcreasing Resilience in Surveillance Societies*. EC: Seventh Framework Programme, 2012.

Lyon, David. "Editorial. Surveillance Studies. Understanding visibility, mobility and the phenetic fix." *Surveillance and Society* 1 (1) (2002).

Margulis, Stephen T. "Privacy as a Social Issue and Behavioral Concept", *Journal of Social Issues*, 59 (2) (2003): 243-61.

Martens, Paul. "L'irrésistible ascension du principe de proportionnalité", in *Présence du droit public et des droits de l'Homme. Mélanges offerts à J.Velu*. t. 1. Bruxelles : Bruylant, 1992.

Marx, G.T. "Ethics for the new surveillance", *The Information Society*, 14 (1998): 171-85.

Massey, A. K., and A. Antòn. "A requirements-based comparison of privacy taxonomies." *Requirements Engineering and Law*, 2008.

Moor, J. H. What is computer ethics? In T.B. Bynum (ed.) Computer & Ethics (Oxford: Blackwell, 1985), 266-275.

Moor, J. H. "Why we need better ethics for emerging technologies?", in *Ethics and Information Technology*, 7(3) (2005): 111-9.

Mulgan, Richard. "Accountability': An Ever-Expanding Concept?", *Public Administration* 78 Issue 3 (2000): 555–573

Network, Surveillance Society. *A Report on the Surveillance Society. For the UK Information Commissioner.* U.K.: Information Commissioner's Office, 2006.

Newell, Patricia B. "A Systems Model of Privacy." *Journal of Environmental Psychology*, 14 (1994): 65-78.

Niemietz vs. Germany and Pretty vs. UK, Judgement of 16 December 1992.

Nissenbaum, Helen. "Privacy as contextual integrity", *Washington Law Review*, 79(1) (2004).

Nissenbaum, Helen. *Privacy in Context. Technology, Policy and the Integrity of Socail Life.* Standford: Standford University Press, 2010.

Nussbaum, M., C. and Sen, A. (1993), « Quality of Life », Clarendon Press, Oxford. Nussbaum, M., C. (1999), « Sex and Social Justice », Oxford University Press, Oxford.

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (Part 2). Annex to the Recommendation of the Council of 23rd September 1980. www.oecd.org.

Orlikowski W.J. and C. S. Iacono, "Reasearch commentary: Desperately seeking the "IT" in IT research-a call to theorizing the IT artifact", *Information Systems Research*, 12(2) (2001): 121-34.

Orlikowski, W. J. "Sociomaterial practices: Exploring technology at work." *Organization Studies* 28 (2007).

Pedersen, Darhl M. "Model for types of privacy by privacy functions." *Journal of Environmental Psychology,* 19 (1999): 397-405.

Pedersen, Darhl M. "Psychological Functions of Privacy." *Journal of Environmental Psychology*, 17 (1997): 147-156.

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

Pfitzmann, Andreas, en Hansen Marit. "A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management." Tech. Report, v0.34, Aug. 2010. Available at: http://dud.inf.tu-dresden.de/literatur/Anon_Terminology_v0.34.pdf.

Prosser, William L. "Privacy", *California Law Review*, 48 (1960): 383.

Pytlikzillig, Lisa M., and Alan J. Tomkins. "Public engagement for informing science and technology policy: What do we know, what do we need to know, how do we get there?" *Review of Policy Research* 28 (2) (2011): 197-217.

Raab, Charles. "The Meaning of 'Accountability' in the Information Privacy Context", in *Managing Privacy through Accountability,* edited by Daniel Guagnin, Leon Hempel, Carla Ilten, Inga Kroener, Daniel Neyland and Hector Postigo, 15-32. Palgrave Macmillan, 2012.

Regan, Priscilla M. *Legislating Privacy: Technology, Social Values, and Public Policy* (Chapel Hill: University of North Carolina Press, 1995).

Rouvroy, Antoinette and Poullet, Yves. "The Right to Informational Self-Determination and the Value of Self-Development", in *Reinventing Data Protection?*, edited by Serge Gutwirth, Yves Poullet, Paul De Hert, Cécile De Terwangne and Sjaak Nouwt, 45-76. Springer, 2009.

Senior, Andrew, et al. “Enabling Video Privacy through Computer Vision.” May 2005: 50-57.

Senior, Andrew. *Protecing privacy in video surveillance.* New York: Springer, 2009.

Solove, Daniel. *Understanding Privacy*. Cambridge: Harvard University Press, 2008.

Solove, Daniel J. *Nothing To Hide. The False tradeoff between privacy and security.* New Haven: Yale University Press, 2011.

Sottiaux, Stefan. *Terrorism and The Limitations of Rights, the ECHR and the US Constitution*. Oxford: Hart Publishing, 2008.

Sprenger, Polly. *Sun on Privacy: 'Get Over It'.* http://www.wired.com/politics/law/news/1999/01/17538 (accessed June 10, 2013).

Steeves, Valerie. "Reclaiming the Social Values of Privacy," in *Lessons from Identity Trail*, ed. I. Keer (Oxford: Oxford University Press, 2008).

Stone Sweet, Alec and Matthews, Jed. “Proportionality, Balancing and Global Constitutionalism”, *Columbia Journal of Transnational Law* 47 (2008): 73-165

Story, Louise. "To Aim Ads, Web is keeping Closer Eye on You." *The New York Times*, March 2008.

Stross, Randall. "Google anything, So Long as It's Not Google"." *The New York Times*, Aug 28 Aug 2005.

Sudre, Frédéric (under the dir.). *Le droit au respect de la vie privée au sens de la Convention européenne des droits de l’homme.* Bruxelles: Bruylant, 2005.

Thompson, Bill. *Networks blur the private and public divide.* news.bbc.co.uk/2/hi/technology/8570406.stm (accessed June 6, 2013).

Thoreau, François. *Embarquement immédiat pour les nanotechnologies responsables. Comment poser et re-poser la question de la réflexivité?* Liège: Université de Liège, 2013.

Travis, Alan. *Fight against terror 'spells end of privacy'.* http://www.guardian.co.uk/uk/2009/feb/25/personal-data-terrorism-surveillance (accessed June 11 2013).

Trussart, Nathalie. "Publics et expérimentations." *Multitudes* 23 (2005): 169-179.

Van Drooghenbroeck, Sebastien. *La proportionnalité dans le droit de la convention européenne des droits de l’homme, prendre l’idée simple au sérieux*. Bruxelles : Bruylant, 2001.

Van Orp, A. "Ethics in and during technological research; An addition to IT ethics and scienbce ethics," in *Evaluating new technologies*, ed. P. Sollie and M. Düwell (Dordrecht: Springer, 2009), 35-50.

Venier, Silvia and Emilio Mordini, "Deliverable 4. FInal Report - A Privacy and Ethical Impact Assessment Framework for Emerging Sciences and Technologies," in *PRESCIENTproject. Privacy and emerging fields of scienbce and technoolgy: Towards a common framework for privacy and ethical assessmenttechnologies: Five case studies* (EC: Seventh Framework Programme (FP7), 2012).

von Silva-Tarouca Larsen, Beatrice. *Setting the watch, Privacy and the Ethics of CCTV Surveillance* (Oxford: Hart Publishing, 2011).

von Schomberg, René. "From the ethics of technology towards an Ethics of knowledge Policy abd Knwoledge Assessment," in *A working document for the European Commission services* (EU: European Commission's Directorate General for Research, 2007).

Warren, Samuel D., and Brandeis, Louis D. Samuel D. “The Right to Privacy”, *Harvard Law Review* Vol. IV. No. 5 (1890)

Watson, Haley, and David (ed.) Wright. "Deliverable 7.1: Report on Existing Surveys." In *PRISMS . The PRIvacy and Security MirrorS: Towards a European framework for integrated decision making.* EC: Seventh Framework Programme, March 2013. Available at http://prismsproject.eu/wp-content/uploads/2013/03/PRISMS-D7-1-Report-on-existing-surveys.pdf

Weitzner, Daniel J. et al, Information accountability, *Communications of the ACM* Vol.51, N°6 (2008): 84-87

Westin, Alan. *Privacy and Freedom*. New York: Atheneum, 1967.

Westin, Alan. "Social and Political dimensions of Privacy", *Journal of Social Issues*, 59(2) (2003): 431-53.

Wilsdon, James, and Rebecca Willis. *See through science: Why public engagement needs to move upstream.* London: Demos, 2004.

Winner, Langdon. "Do artifacts have politics?" *Daedalus* 109 (1) (1980).

Winner, Langdon. "How technology reweave the fabric of society." *The chronicle of higher education* 39 (48) (1993).

Winseck, Dwayne. "Netscapes of power. Convergence, network design, walled gardens, and other strategies of control in the information age." In *Surveillance as social sorting*, edited by David Lyon, 176-198. New York: Routledge, 2003.

Withman, James Q. “The Two Western Cultures of Privacy: Dignity Versus Liberty”, *The Yale Law Journal* 113 (2004): 1151-1221

Worchel, Stephen and Steven M. Yohai. “The role of attribution in the experience of crowding.” *Journal of Experimental Social Psychology*, 15 (1979): 91–104.

Wright, David ."A framework for the ethical impact assessment of information technology", *Ethics and Information Technology*, 3 (13) (2011

Wright, David and Paul De Hert (eds.), *Privacy impact assessment* (New York: Springer, 2012).

Wright, David and Emilio Mordini, "Privacy and ethical impact assessment," in *Privacy impact assessment* (New York: Springer, 2012), 397-418.

Zahran, Mounir. Accountability Frameworks in the United Nations System, doc. JIU/REP/2011/52011, Geneva, 2011, available at: https://www.unjiu.org/en/reports-notes/JIU%20Products/JIU_REP_2011_5.pdf

Zimring, Craig. “The built environment as a source of psychological stress: Impacts of buildings and cities on satisfaction and behavior.” In *Environmental Stress,* edited by Gary W. Evans. New York: Cambridge University Press, 1982.

Zureilk, Elia, and Lynda Hardling Stalker. "The Cross-Cultural Study of Privacy: Probelms and Proepcts." In *Surveillance, Privacy and the Globalization of Personal data: International Comparisons*, edited by Elia Zureik, Lynda Hardling Stalker, Emily Smith, David Lyon and Yolande E. Chan, 8-30. Montreal & Kingston: McGill-Queen's University Press, 2010.

7.2 Studies

APEC Data Privacy Pathfinder Projects Implementation Work Plan – Revised, Submitted by Australia, 2009/SOM1/ECSG/SEM/027, First Technical Assistance Seminar on the Implementation of the APEC Data Privacy Pathfinder, Singapore, 2009, http://www.apec.org/About-Us/About-APEC/Fact-Sheets/APEC-Privacy-Framework.aspx

British Institute of International & Comparative Law published a *Report on the Implementation of Directive 95/46/EC to the Processing of Sound and Image Data*, 2002

Douwe Korff, Comparative Study on different approaches to new Privacy Challenges, in particular in the light of technological developments, Working Paper No. 2: Data Protection in the EU: the difficulties in meeting the challenges posed by global social and technical developments, 20 January 2010.

Douwe Korff, Comparative Study on different approaches to new Privacy Challenges, in particular in the light of technological developments, Working Paper No. 1: The challenges to European data protection laws and principles, 20 January 2010

Douwe Korff, Comparative Summary of National laws, University of Essex/European Commission, 2002) and on five Country Reports regarding Denmark, France, Germany, the UK and the Czech Republic all submitted in 2010 and available at: http://ec.europa.eu/justice/data-protection/document/studies/index_en.htm

The Centre for Information Policy Leadership (acting as secretariat to the Galway project), "Data Protection Accountability: The Essential Elements", October 2009, available at: http://www.huntonfiles.com/files/webupload/CIPL_Galway_Accountability_Paper.pdf

The Centre for Information Policy Leadership (acting as secretariat to the Paris project), Demonstrating and Measuring Accountability, Accountability Phase II – The Paris Project, October 2010, available at: http://www.huntonfiles.com/files/webupload/CIPL_Accountability_Phase_II_Paris_Project.PDF

The Centre for Information Policy Leadership , "Accountability: data governance for the evolving digital marketplace", 2011, available at: http://www.huntonfiles.com/files/webupload/CIPL_Centre_Accountability_Data_Governance_Paper_2011.pdf

7.3 Documents from Data Protection Authorities

European Data Protection Supervisor (EDPS), Opinion on the data protection reform package, 7 March 2012, available at: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2012/12-03-07_EDPS_Reform_package_EN.pdf

Article 29 Data Protection Working Party, *Opinion 03/2013 on purpose limitation*, 2 April 2013, WP203

Article 29 Data Protection Working Party, *Opinion 03/2012 on developments in biometric technologies*, 27 April 2012, WP193

Article 29 Data protection Working Party, *Opinion 01/2012 on the data protection reform proposals*, 23 March 2012, WP191

Article 29 Data Protection Working Party, *Opinion 15/2011 on the definition of consent*, 13 July 2011, WP187

Article 29 Data Protection Working Party, Opinion 3/2010 on the principle of accountability, 13 July 2010, WP173

Article 29 Data Protection Working Party, *Opinion 01/2010 on the concepts of 'controller' and 'processor'*, 16 February 2010, WP169,

Article 29 Data Protection Working Party, *Opinion 04/2007 on the concept of Personal data*, 20 June 2007, WP136

Article 29 Data Protection Working Party, *Opinion 4/2004 on the Processing of Personal Data by means of Video Surveillance*, 11 February 2004, WP89

Article 29 Data Protection Working Party, *Working Document on biometrics*, 1 August 2003, WP80

Article 29 Data Protection Working Party, *Working Document on the Processing of Personal Data by means of Video Surveillance*, 25 November 2002, WP67

CNIL Press Release of June 2012 on best practices in relation to videoprotection and videosurveillance, at http://www.cnil.fr/fileadmin/documents/approfondir/dossier/Videosurveillance/CNIL-DP_Video.pdf

Privacy Commission, Recommandation d'initiative n°04/2012 du 29 février 2012 sur les diverses possibilités d'application de la surveillance par caméras, further referred to as « Privacy Commission Recommendations regarding the Videosurveillance Law of 2012 ».

Privacy Commission Note relative à la loi réglant l'installation et l'utilisation de caméras de surveillance, 20/01/2010

Office of the Privacy Commissioner of Canada, "A matter of Trust: Integrating Privacy and Public Safety in the 21st Century. A reference Document From the Office of the Privacy Commissioner of Canada", November 2010, online at http://www.priv.gc.ca/information/pub/gd_sec_201011_e.asp

Office of the Information and Privacy Commissioner of Alberta, Office of the Privacy Commissioner of Canada, Office of the Information and Privacy Commissioner for British Columbia, Guidelines: Getting Accountability right with a Privacy Management Program, 2012, available at: http://www.priv.gc.ca/information/guide/2012/gl_acc_201204_e.asp#e

Consultative Committee on the Convention for the protection of Individuals with regard to the automatic processing of personal data **(T-PD),** Progress Report on the application of the principle of Convention 108 to the collection and processing of biometric data (2005)

7.4 Documentation from the European Institutions

European Commission

European Commission, Privacy and Data Protection Impact Assessment Framework for RFID Applications, 12 Januray 2011, available at : http://cordis.europa.eu/fp7/ict/enet/documents/rfid-pia-framework-final.pdf

European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, COM(2012)11 final, Brussels, 25 Januray 2012

European Commission, Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, COM(2012)10 final, Brussels, 25 January 2012

Commission Staff Working Paper, *Operational Guidance on taking account of Fundamental Rights in Commission Impact Assessments*, SEC(2011)567 final, 6 May 2011

Communication from the Commission to the European Parliament, the Council, the Economic And Social Committee and the Committee Of The Regions, *A comprehensive approach on personal data protection in the European Union*, COM(2010) 609 final, Brussels, 4 November 2010

Communication from the Commission, *Strategy for the effective implementation of the Charter of Fundamental Rights by the European Union*, COM(2010)573/4, 19 October 2010

Communication from the Commission to the European Parliament and the Council on *Promoting Data Protection by Privacy Enhancing Technology (PETs*), COM(2007) 228 final, 2 May 2007

Communication from the Commission to the Council and the European Parliament on *improved effectiveness, enhanced interoperability and synergies among European databases in the area of justice and home affairs*, COM(2005)0597 final, 24 November 2005

CORDIS: Community research and Developement Information Service, "Getting Through Ethics Review," in *Sventh Framework Programme (FP7)* (EU: European Commission). Available at: http://cordis.europa.eu/fp7/ethics_en.html#ethics-cl

European Group on Ethics in Science and New Technologies to the European Commission, "The Protection of fundamental ethical principles in international research and innovation programmes," in *Report on the third meeting of the European Commission's international Dialogies on Bioethics*, ed. bepa: Bureau of European Policy Advisers (Brussels: European Commission , 2011). Available at: http://ec.europa.eu/bepa/european-group-ethics/docs/ibd/idb_20sept.2011.pdf

Expert Working Group on data protection and privacy, "Data Protection and privacy ethical guidelines," in *Ethical Review in FP7* (EU: European Commission, 2009). Avalaible at: ftp://ftp.cordis.europa.eu/pub/fp7/docs/privacy.doc

Leaked text of Proposal for a Directive of The European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such

data ("Police and Criminal Justice Data Protection Directive") published by Statewatch at: http://www.statewatch.org/news/2011/dec/ep-dp-leas-draft-directive.pdf

European Parliament

European Parliament, Committee on Civil Liberties, Justice and Home Affairs, Draft Report on the proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)), doc num. PE501.927, 17 December 2012, available at: http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/pr/922/922387/922387en.pdf

European Parliament, Committee on Civil Liberties, Justice and Home Affairs, "Draft Report on the proposal for a directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data", doc num. PE 501.928v02-00, 20 December 2012, available at: http://www.europarl.europa.eu/sides/getDoc.do?type=COMPARL&mode=XML&language=EN&reference=PE501.928

7.5 Main Legal Sources

International

OECD Guidelines of 1980 governing the protection of privacy and transborder data flows of personal data

Council of Europe

Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, signed in Rome, 1950

Council of Europe Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data signed in Strasbourg, 1981

Council of Europe Parliamentary Assembly, Resolution 1604 (2008) on videosurveillance of public areas of 25 January 2008 (non binding)

Council of Europe Parliamentary Assembly, Resolution 1797 (2011) on the need for a global consideration of the human rights implications of biometrics of 11 March 2011 (non binding)

European Court of Human Rights Caselaw

ECHR, *Handyside v. the United Kingdom*, 7 December 1976

ECHR, *Tyrer v. United Kingdom*, 25 April 1978

ECHR, *Klass v. Germany*, 6 September 1978,

ECHR, *Malone v. United Kingdom*, 2 August 1984

ECHR, *X. & Y. v. The Netherlands*, 26 March 1985

ECHR, *Leander v. Sweden,* 26 March 1987

ECHR, *Olsson v. Sweden*, 24 March 1988

ECHR, *Gaskin v. United Kingdom,* 7 July 1989

ECHR*, Kruslin v. France* and *Huvig v. France*, 24 April 1990

ECHR, *Niemietz v. Germany*, 16 December 1992

ECHR, *Andersson v. Sweden*, 25 February 1992

ECHR, *Costello-Roberts v. The United Kingdom*, 25 March 1993

ECHR, *Frield v. Austria*, 26 January 1995

ECHR, *Z. v. Finland*, 25 February 1997

ECHR, *Halford v. United Kingdom*, 25 June 1997

ECHR, *Pierre Herbecq and the Association Ligue des droits de l'homme v. Belgium*, 14 January 1998

ECHR, *Amann v. Switzerland,* 16 February 2000

ECHR, *Rotaru v. Romania,* 4 May 2000

ECHR, *P.G. and J.H. v. United Kingdom*, 25 September 2001

ECHR, *Pretty v. The United-Kingdom*, 29 April 2002

ECHR, *Peck v. United Kingdom*, 28 January 2003

ECHR, *Perry v. United Kingdom*, 17 July 2003

ECHR, *Evans v. The United Kingdom*, 7 March 2006

ECHR, *S. and Marper v. United Kingdom*, 4 December 2008

ECHR, *Uzun v. Germany*, 2 September 2010

ECHR, *Aydogdu v. Turkey*, 11 January 2011

European Union

EU Charter of Fundamental Rights

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the automatic processing of personal data and on the free movement of such data, *OJEC* L281, 23 November 1995.

Regulation 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community Institutions and bodies and on the free movement of such data, *OJEC* L8, 12 January 2001

Directive 2002/58/EC of the European Parliament and of the Council of 17 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, *OJEU* L201, 31 July 2002.

Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks, *OJEU* L 105 of 13 April 2006

Council Framework Decision 2008/977/JAI of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, *OJEU* L350, 30 December 2008

Treaty of Lisbon amending the Treaty on European, Union and the Treaty established the European Community, signed at Lisbon, 13 December 2007. Available at: http://eur-lex.europa.eu/JOHtml.do?uri=OJ:C:2007:306:SOM:EN:HTML

European Court of Justice Caselaw

E.C.J., 9 November 2011, *Volker und Markus Schecke GbR and Harmut Eifert v. Land Hessen*, joint cases C-92/09 and C-93/09

E.C.J., 24 November 2011, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECEMD) v. Administración, del Estado*, joint cases C-468/10 et C-469-10

National Law

France

Act No. 78-17 of 6 January 1978 on Information Technology, Data Files and Civil Liberties – Loi No. 78-17 Informatique et Libertés du 6 Janvier 1978 – as amended

Act No. 95-73 of 21 january 1995 on homeland security orientation and programming - Loi n°95-73 du 21 janvier 1995 d'orientation et de programmation pour la sécurité intérieure

Décret n°96-926 du 17 octobre 1996 relatif à la vidéoprotection pris pour l'application des articles 10 et 10-1 de la loi n° 95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité

Belgium

Privacy Act of 8 December 1992 on the protection of privacy in relation to the processing of personal data – Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *MB*, 18/03/1993

Loi réglant l'installation et l'utilisation de cameras de surveillance du 21 mars 2007, *M.B.,* 31/05/2007, further referred to as the "videosurveillance law"

Loi visant à modifier la loi réglant l'installation et l'utilisation de cameras de surveillance du 12 novembre 2009, *MB,* 18/12/2009

Arrêté Royal du 2 juillet 2008 relatif aux déclarations d'installation et d'utilisation de caméras de surveillance

Arrêté Royal du 10 février 2008 définissant la manière de signaler l'existence d'une surveillance par caméra, *MB*, 21/02/2008

Circulaire ministérielle du 10 décembre 2009 relative à la loi du 21 mars 2007 réglant l'installation et l'utilisation de caméras de surveillance, telle que modifiée par la loi du 12 novembre 2009, M.B., 18/12/2009, as amended on 13 may 2011, M.B., 20/05/2011, further referred to as the « Ministerial Circular of 2009 »

Appendix 1. Taxonomy: the Main Categories in a Video Surveillance System

Zhendong Ma and Bernhard Strobl (AIT)

In this section we will define a basic taxonomy to classify the conceptualization of the video, everything related to a video surveillance system, the different existing permission to access the video, the kind of users that can access to the system and different organizations or users that can interact with the organization responsible for video surveillance equipment. Before starting to describe this classification, it is important to stare the graphical representation of that taxonomy (Figure 9).

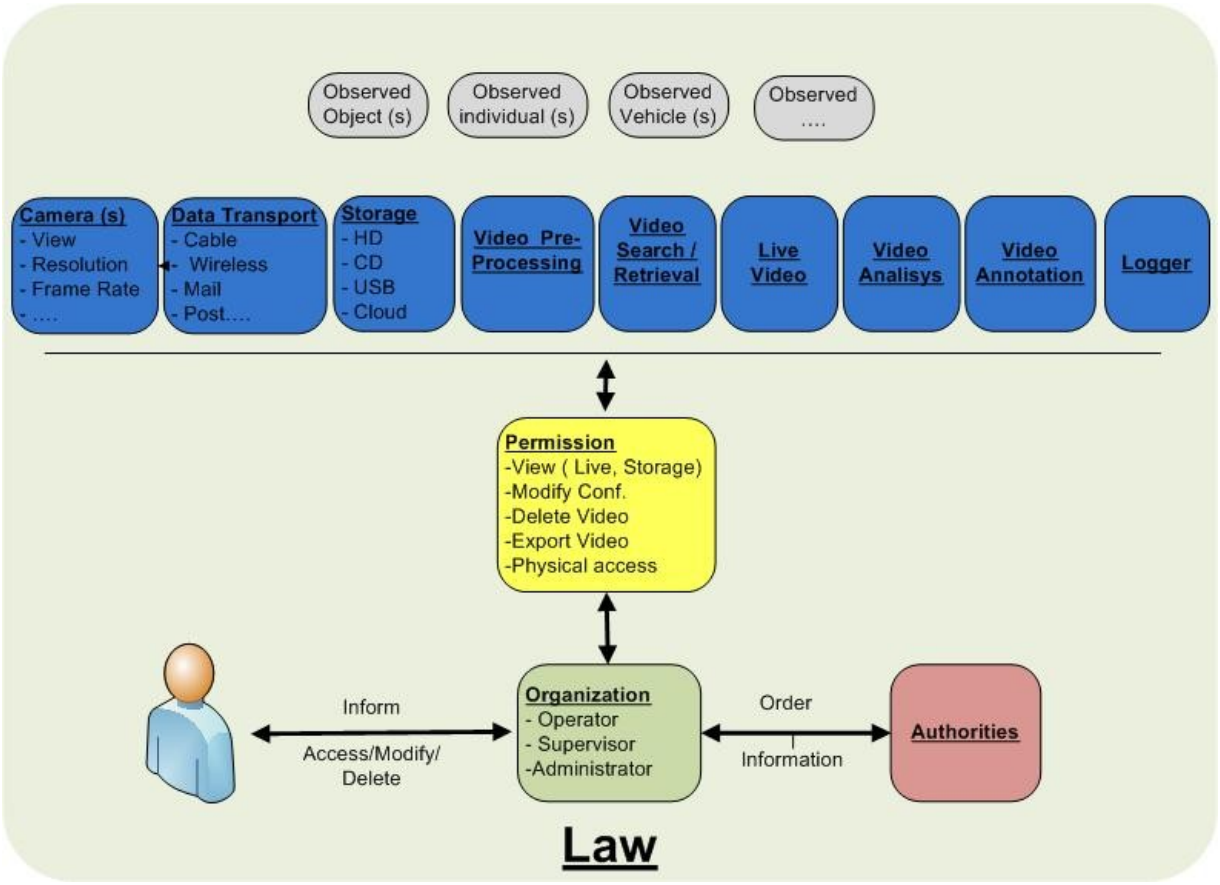

Figure 9: Taxonomy for Video Surveillance

We will start with the **first layer**, the grey group. This group represents the **video concept**, different things that can be seen through the video. For example, we can observe a vehicle, an individual, a specific alarm, or other objects. In order to make a more detailed classification in this group we are going to rely on the taxonomy of the Vidi Video Project[637]. In this project the video content is conceptualized as follows: a "concept" can describe either the context of the video (e.g., indoor, traffic surveillance, a building with a specific security), or the content which

[637] VIDI-Video Project, http://www.vidivideo.info/

can be a physical object characterizing or present in the scene (e.g., building, person, animal) or a detectable action/event occurring (e.g., falls, intrusions, movement detection, interaction between people). Figure 10 shows a graphical representation of the taxonomy of the Vidi Video Project.

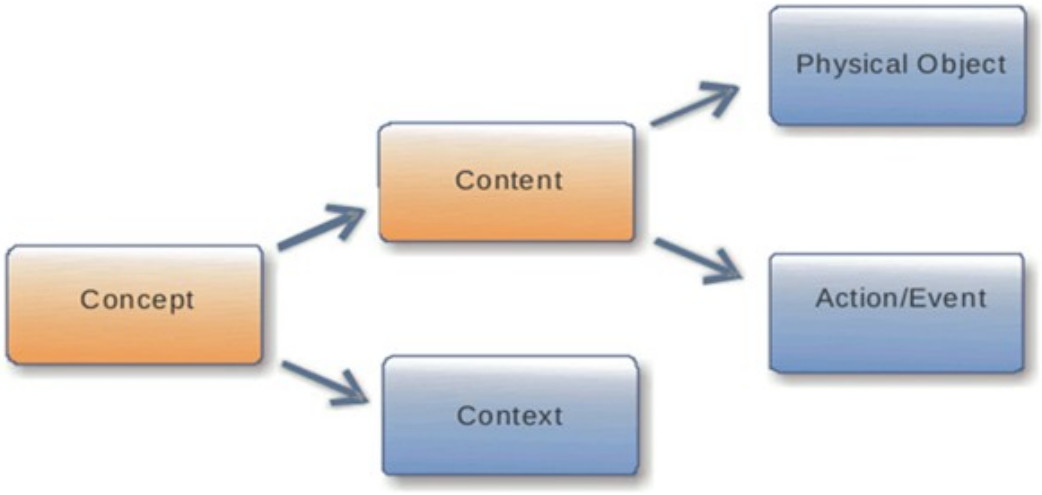

Figure 10: Video Concept Classification

After seeing the video concept classification, we are going to focus on the **second layer**. This layer is related to everything that has to do with a **video surveillance system** (storage, monitoring). Now, we are going to describe each of the blocks in this layer:

- **Camera.** It is the sensor through which the system receives video. The cameras can be statics or pan-tilt-zoom cameras. The static cameras are installed to focus on a fixed area. The pan-tilt-zoom cameras use remote control to focus on an area from alternate angels, providing a wider coverage. Some important properties about the cameras are: resolution, frame rate, kind of compression.
- **Data transportation.** It is the medium through which the video is transported. For example, the organization responsible for the system can deliver the video through network (e.gl, cable, wireless) or the mail to the police if necessary.
- **Storage.** It is the medium where the video is stored. The most common is stored the video in the internal hard disk of the video surveillance equipment. The video could also be stored in different places through the cloud, as well as in a USB or CD.
- **Video Pre-processing.** This module is in charge of making the necessary operations in order to prepare the video for subsequent use. For example if we want to store the images with a different size or kind of compression, this module will do the resize of the images or compress/decompress the images in the appropriate format.
- **Video Search/Retrieval.** Through this module we can get some specific video sequences based on date or the content of the video if we use a mechanism to make annotations over the video. Once, we have found the specific sequences we can visualize the sequence or export the video in order to obtain this sequence for a specific purpose (e.g., deliver to the police).
- **Live video.** Through this module we can watch in real time what is happening in the area covered by the camera. For example, this module allows operators to check an alarm in order to verify whether it is a false alarm or not.

- **Video analysis.** Thanks to this module, if we have the proper algorithms, we can classify the different objects in an automatic mode or detect a specific event as an intrusion or an alarm generated by motion detection.
- **Video annotation.** Sometimes, there are systems which include video annotation functionality through which we can provide extra information. Here we can classify the kind of annotations in Automatic or User annotations. Through the automatic annotations the system can add some information as the size of the video. Through the user Annotations, the user can write down some comments to the video (i.e., the operator can indicate that in this part of the video exist a possible suspects).
- **Logger.** From the privacy perspective, this module is very important. Since, it is in charge of recording all the actions that the different users carry out. For example, when some operator deletes some sequences, this module is going to record that this operator has deleted this particular sequence corresponding to a specific time and data.

To finish with this group, it is important to emphasize that the first two layer are linked through the vide analysis and video annotation module. Thanks to these two modules we can conceptualize the video based on the schema provided by the Vidi video project.

Thirdly, we are going to explain the **third layer.** On this layer, we will focus on establishing the different **permissions** that the user has to view, handle, modify or delete anything related to the system. You can see the different permissions below.

- **Modify the configuration.** We must establish who is responsible for change the different computers settings as the network, camera, event and profile parameters.
- **View Video**. We must define what are the user how can monitor the live video or the video storage.
- **Delete Video.** We must assign who are the users with the proper permissions to delete video sequences.
- **Export Video.** In the same way, we have to detail who are the users with the enough permission to retrieve the video.
- **Physical access.** Finally, it is important to keep this equipment in safe areas with restricted access in order to prevent theft. For this reason, we must define a responsible person who has access to that area.

The **fourth layer** is related to the **individuals** of the organization who can **access** to the digital video recorder system. Depending on the system and the organization we can have many users accessing to the video. A very basic classification could be next (different user roles described could vary greatly depending on system or organization):

- **Operator.** This user could have permissions to watch only the live video.
- **Supervisor.** This user could have permissions to watch the live video, search and watch the video storage.
- **Administrator.** This user could have all the permissions of the systems.

The **fifth layer** is related to the authorities (e.g., the police). The authorities can order some specific sequences (some day at certain time) in order to investigate a crime or something similar. As a consequence the organization will deliver the corresponding information.

Finally, we are going to present the **sixth layer.** This layer has to do with the **users** how are undergone to the system. On this occasion we can see that users can interact with the organization. In this case, this interaction can be based on the law. For example, the law can require that:

- The organization informs the users that they are being recorded.

- The user can give their consent or not
- The user can have the right to access, modify and delete their personal information.

It is important to remark that all these layers are influenced by the law. For example, in France, the only user who can delete the video sequences is the administrator.

Appendix 2. Privacy Benefits and Harms. One Perspective

Here below are two tables taken from the appendix of the PRESCIENT project, in its "Deliverable D1: Legal, social, economic and ethical conceptualisations of privacy and data protection". [638]

The first one reproduces the taxonomy of types of privacy proposed in 2013 by Rachel L. Finn, David Wright and Michael Friedwald.[639]

The second one shows the benefits and harms corresponding to each of these types of privacy.

As mentioned in the chapter II, the identification of privacy benefits and harms depends on the types of conceptualization of that is retained. That means that this one is of great interest but may be subject of modification and completion with the help of other privacy taxonomies, regards to the specificity of the SALT Framework.

[638] Serge Gutwirth et al., "Deliverable D1: Legal, social, economic and ethical conceptualisations of privacy and data protection," in *PRESCIENT. Privacy and emerging fields of science and technology: Towards a common framework for privacy and ethical assessment* (EC: Seventh Framework Programme, March 2011), 63-7.

[639] Rachel L. Finn, David Wright and Michael Friedewald, "Seven Types of Privacy," in *European Data Protection: Coming of Age*, ed. Serge Gutwirth (Dordrecht: Springer, 2013), 3-32.

Seven Types of Privacy

Types of privacy	Definition / scope	Trade-offs , limitations	Examples of threats[242]
Privacy of person	People have a right to keep private bodily functions (excreting, making love, picking their nose) and body characteristics, including their DNA (genetic code) and other biometrics.	In the interests of its safety and security, society should be able to establish a database of offenders' DNA in order to help identify and apprehend criminals. Some medical research needs access to the genetic fingerprints (DNA) of many people in order to minimise the threat of disease or illnesses that may afflict society.	Government DNA bases in the US, UK and elsewhere include the DNA of many law-abiding citizens. The ubiquitous prevalence of surveillance cameras are making incursions into the privacy of persons. Old people suffering from dementia are monitored all the time.
Privacy of thought and feelings	People have a right to not share their thoughts or feelings and to not have their thoughts or feelings revealed.	Employers need to understand whether their employees are mentally stable and will be able to perform their jobs satisfactorily. This is especially important re jobs in critical infrastructures.	Research is being conducted that would help read people's minds.[243]
Privacy of location and space	People have a right to go wherever they want without being tracked or monitored. They have a right to the privacy of their personal space, including their home, car, office. They have a right to solitude.	Some areas (such as nuclear power plants) are off-limits to most people. If a person is in a car crash, automatic position determination can help get ambulance services or police to the scene of the accident quickly. Parents feel they have a right to know where their children are.	Companies may use location information generated from the user's mobile phones or other web services to bombard the individual with "special offers" from nearby shops. Knowing that an individual is not at home may help evil-doers in knowing when to break in and burglarise the individual's home.
Privacy of data and image	People have a right to control over their personal data and image.	Governments may need some personal data for a range of purposes such as taxation, census, the provision of certain social services. Employers may want to see the academic records of prospective employees. Companies and governments can provide more personalised products and services, which should result in efficiency gains for the economy. If one is walking down a street, it is not possible to control someone who takes your photograph or from being captured by closed circuit television (CCTV).	Governments and companies may repurpose personal data, i.e., to use it for purposes beyond those for which the data was originally collected.[244] The paparazzi may pursue a celebrity relentlessly in order to profit from photos even though the person has made strenuous efforts to shield him or herself from such pursuit.
Privacy of behaviour (and action)	People have a right to behave as they please and do what they want without being monitored or having their behaviour controlled by others.	Some people's behaviour and actions may put others at risk – yobs may beat up law-abiding citizens.	Companies may try to manipulate people's behaviour so that they do what the companies want (e.g., to buy their products or services).
Privacy of communication	People have a right to keep their communication with others private and not monitored by others.	Law enforcement authorities and intelligence agencies may need to monitor some people's communication in order to apprehend evil doers.	Governments may monitor everyone's communications and engage in "fishing expeditions", i.e., to identify trouble-makers and dissidents.
Privacy of association, including group privacy	People have a right to associate with whomever they want without being monitored	Someone's association with terrorists or criminals is of legitimate societal concern.	Surveillance cameras and other technologies may be used to determine who meets with whom.

Table 3 Seven Types of Privacy

Privacy Benefits and Harms

Types of privacy	Benefits in protecting privacy		Harms arising from compromising privacy	
	To individual:	To society:	To individual:	To society:
Privacy of person	People do not need to feel inhibited if they can perform bodily function in private. Privacy of person is conducive to feelings of individual freedom.	Enabling and supporting privacy of person is conducive to a healthy, well-adjusted society.	People will feel inhibited. It leads to a Big Brother syndrome.	Society will become dysfunctional if it is populated by inhibited citizens.
Privacy of thought and feelings	People can contemplate whatever they like, which will help them grow their creativity and self-expression. People may feel accountable for many of their actions, but they can at least feel as free as a bird in their own minds.	Society benefits from the creativity of free-thinking individuals. Privacy of thought helps society avoid a Huxleyan Brave New World.	People will feel truly enslaved and repressed. They will become dysfunctional. They may lash out at society.	Society will put social order at risk if it is populated by repressed individuals. Social order through "thought control", enforced by "thought control police" is illusory.
Privacy of location and space	Being free to go wherever one wants without others knowing where contributes to the individual's overall sense of living in a democracy, of feeling free.	Freedom of movement is a feature of a trusting, well adjusted democracy.	If our movements and location are monitored all the time, we will suffer from Big Brother syndrome. We will not feel as if we are living in a democracy.	If individuals' locations are monitored all the time, people will feel they live in an exploiting, Big Brother society. There will be a chilling effect. Some people will attempt to undermine the social order. Society puts itself at risk.
Privacy of data and image	If individuals have control of their personal data, they will feel empowered. It builds self-confidence and a sense that we have real choices.	Democracy benefits from a society of individuals who believe they are in control of their own data (their own destiny).	Individuals will be relentlessly exploited by governments and companies. Personal data enables more precise targeting of individuals. Who wants to be a "target"?	The nature of society will be harmed if governments and companies are continually using personal data to exploit its citizens.
Privacy of behaviour and action	The individual feels free to do what he/she likes without interference from others.[245] People can benefit from solitude, from tranquillity arising from solitude. "Insofar as privacy… frees us from the stultifying effects of scrutiny and approbation (or disapprobation), it contributes to… the development and exercise of autonomy and freedom in thought and action."[246]	Society holds freedom as an important value. Democratic society is composed of individuals who feel free to do what they like. Democracy fosters social cohesion and solidarity.	The individual feels constrained in what he/she can do. The individual feels others watching him, judging him constantly. The individual feels oppressed, subjugated, disempowered, resentful, dysfunctional.	Society is composed of angry, oppressed citizens, who will most likely attempt to vote out, subvert or overthrow the ruling government. They will not be law-abiding because they disagree with the law.
Privacy of communication	The individual feels free to say whatever he or she likes to whomever he likes. The individual feels free to express his unvarnished views, to express his opinions freely.	Society is composed of people who do not feel inhibited in what they say or the need to be on constant guard re what they say, by phone, e-mail, the Internet, mobile or any other form of communication, including face-to-face communication. Society will benefit from free discussion of a wide range of views, opinions. There is more likely to be growth in communication services if users feel they can use them freely without being monitored. Some companies will benefit from the sale of eavesdropping or monitoring equipment and services.	The individual will need to be careful in what he or she says. There will be a chilling effect. People will feel the effect of Big Brother as well as many little brothers. The person may feel fearful, possibly subdued, possibly angry.	There will be a lack of trust in society, as individuals do not know who will be listening in on their communications and using what is said against them. People will avoid use of certain services especially social networks, which will thus have a chilling effect on the economy.
Privacy of association, including group privacy	The individual will be able to associate with anyone he or she feels like.[247]	Society will benefit by being composed of more social citizens. A wide variety of groups will spring up, some of whom will press for more democratic political or economic change.	The individual will feel more withdrawn. He / she is less likely to associate with certain people or groups.	Social vitality will be sapped as fewer groups will form. Some groups, even innocuous ones, will feel they need to go "underground".

Table 4 Privacy Benefits and Harms

Appendix 3. The SALT Framework: an Ambitious Vision for Integrating a Wide Scope of Privacy's Dimensions

Antonio Kung and Christophe Jouvray (Trialog), Antonio Maña and Francisco Jaime (UMA), Zhendong Ma and Bernhard Strobl (AIT), Víctor Manuel Hidalgo (Visual Tools) and Mathias Bossuet (Thales)

Privacy is complex, multi-facet, and evolving. Therefore, it is very difficult for those behind video surveillance systems, e.g., system designer, developer, and operator etc. to take into account of all social, anthropological, psychological, cultural, legal, and technical constraints and regulations related to privacy. Consequently, it is very challenging to ensure compliance in the design, implementation, deployment, and operation of video surveillance systems. This will require not only a broad and cross-disciplinary knowledge but also a deep understanding of many related factors. Moreover, external factors are not static, which means surveillance systems need to react and adapt to the changes (e.g., changes of legal requirements or public opinion) accordingly.

We foresee that the SALT framework will include **overarching privacy principles, privacy-by-design process and methodology, privacy assessment procedure, privacy-enhancement measures and controls, practical guidance, and supporting tools** for privacy preserving video surveillance systems. The framework should help designers and developers to understand and take into account the relevant factors. Additionally, the SALT frameworks should support operators in modifying their systems and operations according to changing political and social environment. On the practical side, we envision that the SALT framework will be modular and build upon existing advances in privacy research and best industrial practices.

Besides, we envision that there would be some kind of knowledge representation of the SALT framework, e.g., in the form of an expert system, which includes measures and tools for usability, manageability, extensibility, and adaptability of the framework.

The SALT framework will contain a set of knowledge provided by a group of experts concerning to the scope of surveillance systems. Depending on their field of expertise, these experts may focus their knowledge towards four different fields of knowledge: Social, Anthropological, Legal and Technological (hence the origin of the acronym SALT).

There are several types of actors who will interact with the SALT framework, such as the aforementioned experts, the surveillance system designer, the system operator, the subject under surveillance, or even a public authority. Each of them uses the SALT framework for different, but related, purposes. Therefore, in order to facilitate the use of the SALT framework, a management tool will be implemented. This tool will aid to the addition of new concerns (data related to surveillance systems provided by the experts) to the framework, and the extraction of filtered information according to a certain surveillance system. The SALT framework will play a key role during the design phase of a surveillance system, since it will help system designers to take design decisions.

Surveillance systems require a special consideration concerning their design process: as any other system, a surveillance system has to be designed before it is deployed, but in this case each instance is different, since the scenario characteristics where the system will be deployed have also to be taken into account. Therefore, design decisions are taken not only during design time, but also during deployment time.

With this in mind, system designers, attending to the given system specifications and the scenario characteristics, make use of the SALT framework instances corresponding to the particular context they are working with (country, public space, etc.). An instance is 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 knowledge entitles designers to take the proper design decisions to develop the desired surveillance system.

Figure 11 shows a comprehensive view of the SALT framework. It describes its relationship with all types of actors that can interact with it. As it can be seen, it distinguishes between six types of actors:

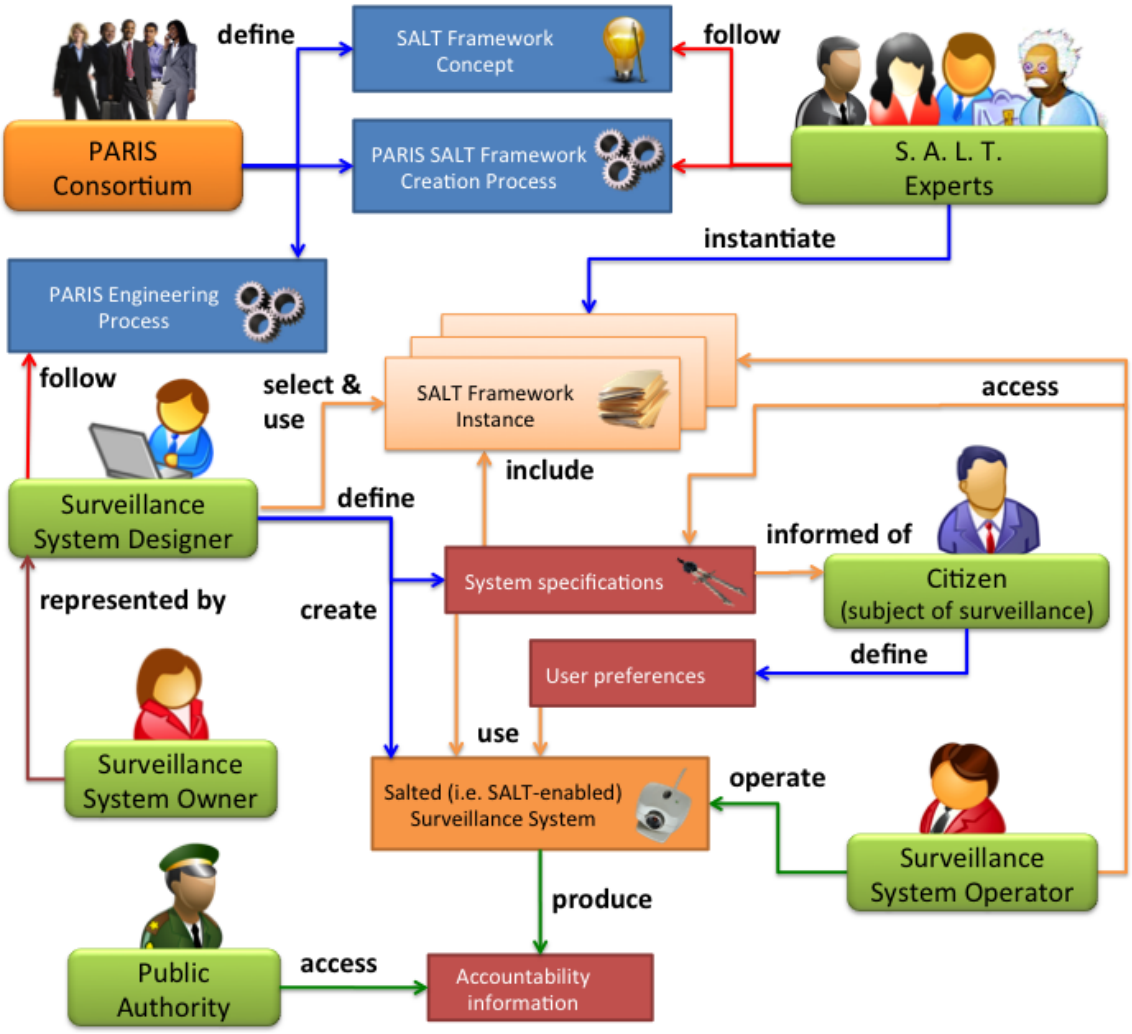

Figure 11: SALT Framework Complete Lifecycle

- **PARIS consortium:** these are the people working in PARIS project. They define the SALT framework concept, the process for a SALT framework creation, and also the final engineering process.
- **SALT experts:** these are the people who will provide the specific knowledge from the social, anthropological, legal and technological scopes. Taking into account the concept of a SALT framework and following the process of a SALT framework creation, they will be able to instantiate several SALT framework instances with their corresponding data.
- **Surveillance system designer:** these are the people who represent the owner of the surveillance system. The owner decisions influence designers' requests. System designers gather the system specifications depending on the scenario they are dealing with. Then, they select the proper SALT framework instance (probably more than one) and use it to create a SALT compliant surveillance system.
- **Surveillance system operator:** these are the people who operate a given surveillance system. In order to do so, they require access to the system specifications, and in this case, since they are working with a SALT compliant system, they also need access to the SALT framework instance(s) used for the system development.
- **Citizen:** this person is the subject of surveillance. There may be various possible ways for the system to interact with citizens: the most simple would be a warning about their entrance into a surveilled area.
- **Public authority:** represents the persons responsible for the system accountability aspects. In order to accomplish their task, they require access to the accountability information produced by the surveillance system: typically auditable logs, which may be compared against the information stored within the SALT framework.

There are many other potential possibilities for using a SALT framework (e.g., a public authority could use it to analyze citizens' behaviours, tendencies or desires regarding to surveillance in order to align laws with them). However, this kind of use is not outside of the scope of the project and will therefore not be considered in the definition the SALT process that we are developing.

At first sight, the main functionality of the SALT framework regards to the surveillance system designer. Figure 12 shows how the SALT framework helps designers to take their design decisions.

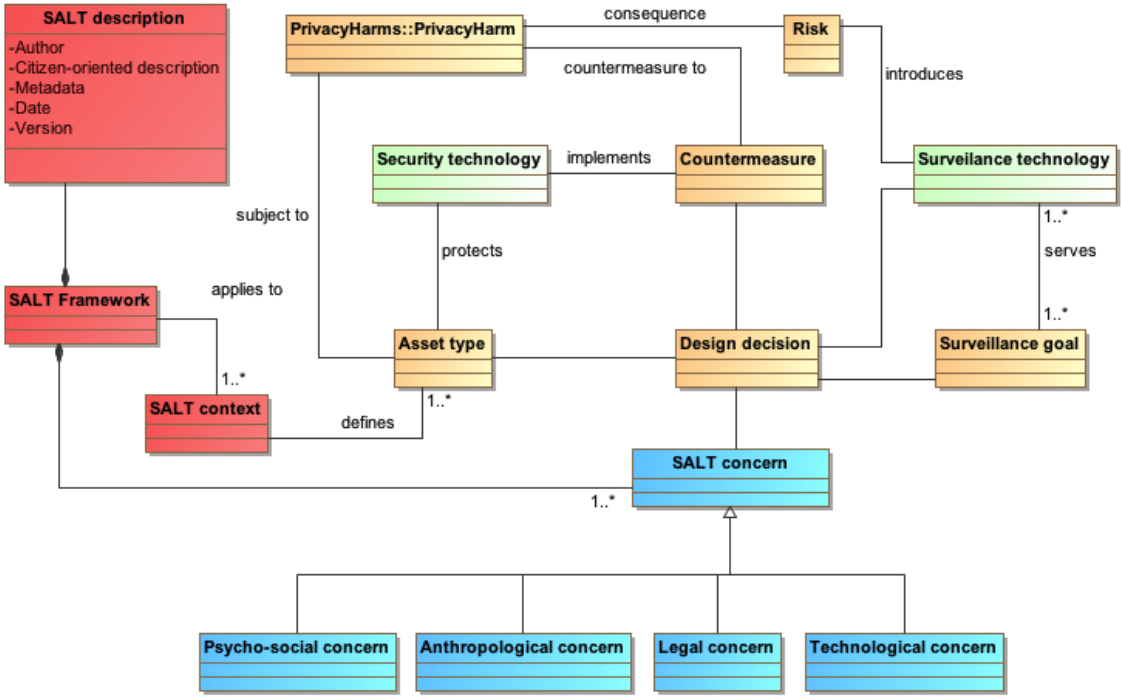

Figure 12: Excerpt of the Metamodel of the SALT Framework from a Surveillance System Development Perspective

Recall that we mentioned that it is very difficult for those behind video surveillance systems, e.g., system designer, developer, and operator etc. to take into account of all social, anthropological, psychological, cultural, legal, and technical constraints and regulations related to privacy. To aid designers to take these constraints into account while performing their task SALT Framework instances will be captured in a computer-processable and engineering-oriented format. In this way, while designing a surveillance system developers will be able to use of one or several SALT framework instances to provide the necessary information about those perspectives. Each instance contains specific information, called SALT concerns, which are divided into four different groups: psycho-social concerns, anthropological concerns, legal concerns and technological concerns.

Designers' starting point is a surveillance goal which has to be fulfilled for a given asset type. For example, a surveillance goal could be recognizing what is being recorded by a video-camera, whereas a car license plate would be an asset type. The existence of a surveillance goal and an asset type brings in the following considerations:

How the surveillance goal is addressed will depend on the surveillance technology available, for example, a wireless video-camera. The use of this technology will entail a series of risks, and as a consequence, it could occur a number of privacy harms.

Depending on the asset type, the system will use one or another security technology to protect the resources from possible privacy harms. For example, ciphering the video recorded data.

With all these elements in mind, it is mandatory to produce some kind of countermeasures in order to protect the system from possible harms. The way a countermeasure is provided will be by implementing a determined security technology (e.g., data ciphering).

Therefore, system designers will have to take a design decision taking into account the surveillance goal they have to fulfill for a given asset type, the surveillance technology that will be used for achieving such goal, and the countermeasures needed to avoid possible privacy harms. Besides, they will have to consider the SALT concerns given by the SALT framework instances that correspond to the contexts of the scenario where the surveillance system is going to be deployed.

For the sake of clarity and ease of use, privacy harms can be divided into different groups: confidentiality breach, exposure, disclosure, etc.

Before and After the SALT Framework

Let's see how the SALT framework technology influences all actors that interact with it:

- **SALT experts:**

Before: each expert works with a big amount of data concerning to his own scope of applicability. This is raw data (not normalized), usually expressed in terms of common language, which includes the slang and technical terms typical from each area of expertise. This fact limits the availability of information inter-areas and complicates the understanding of information even when a given expert gains access to data concerning to a scope different from his/her own.

After: data from different scopes is centralized within a SALT framework, thus it is easily accessible by all experts regardless their area of expertise. Moreover, the information stored within the framework follows a normalized representation, which helps to its understanding.

- **Surveillance system designer**

Before: system designers have to cope with a design/deployment process. They have to design a surveillance system for a given scenario without having specific information concerning its special characteristics, information such as social issues, legal constraints, privacy requirements, etc. Therefore, once they are up to deploy the system and face those problems, they have to go back to the design phase of the process and make all required changes before trying to deploy it again.

After: with a SALT framework at hand, all social, anthropological, legal and technological information for a given scenario is available at design time, allowing system designers to create an accurate system design before its final deployment. This fact does not prevent from an iterative process, indeed, it is possible to repeat any phase of the process and add any new required functionality. However, it allows for a faster deployment, since the first design will better meet the system specifications.

- **Surveillance system operator**

Before: they work with a surveillance system, which they know how to operate, but they may not know whether a determined action is applicable or not for a given circumstance (it may be forbidden to record a child's face, for example), therefore they may fall into an undesired behaviour.

After: they have access to the SALT framework instance(s) used within the system they work with. Therefore, apart from knowing how to operate the system, they also know the social, anthropological, legal and technological constraints corresponding to their system scenario. Because of this, they are qualified to make an optimized used of the system.

- **Citizen**

Before: they enter a space under surveillance without any knowledge regarding the surveillance system that is watching them. They may not even know they are entering a space under surveillance. This fact derives to a potential privacy threat.

After: it is not yet established how the surveillance system interacts with citizens, but at least it can warn them about their entrance into a SALT compliant area under surveillance hence they can be sure that the system fulfils certain privacy requirements.

- **Public authority**

Before: their ability to request accountability to the system is very limited, since the system does not provide information regarding this matter. Hence, their actions are restricted too.

After: the system provides them with auditable logs regarding its operators' actions. These logs can be compared against the SALT concerns used for the system design, thus the public authority can check the correctness of all actions. This fact allows them to take whatever corrective actions required.