PRIVACY PRESERVING PERIMETER PROTECTION PROJECT

GRANT 312784

D2.2
Privacy and Ethics Implementation

ABSTRACT

The objective of WP2 is to integrate the privacy dimension (based on legal and social issues) as design criteria for the P5 technology. The present deliverable focuses on how the rights to privacy and data protection are relevant to the issue of virtual fences for the securisation of critical infrastructures and summarizes the technical system-wide solutions implemented in the P5 technology to tackle and mitigate the data protection risks raised by virtual fences.

Keywords: private life, data protection, privacy-by design, virtual fences

The research leading to these results has received funding from the European Community's Seventh Framework Programme Security Theme (10) under grant agreement number 312784. The research is a part of the efforts in the pan-European and FOI-coordinated project P5.

Author Claire Gayrel, UNamur

Co-authors Alain Loute, UNamur
Annanda Rath Thavy Mony, UNamur
Catherine Forget, UNamur

Date 17/02/2016
Deliverable D2.2
Version Final
B/W Print OK Yes
Page Count 54

P5, The Privacy Preserving Perimeter Protection Project, is a European and FP7-funded project for the protection of critical infrastructures to benefit the sustainability of society and future well-being of the European Citizens.

P5 is coordinated by The Swedish Defence Research Agency, FOI.

Contact
Coordinator of P5, FOI
Box 1165, SE-58111 Linköping
coordinator@p5.foi.se
www.p5-fp7.eu

Executive Summary

The objective of WP2 is to integrate the privacy dimension (based on legal and social issues) as design criteria for the P5 technology. The present deliverable focuses on how the rights to privacy and data protection are relevant to the issue of virtual fences for the securization of critical infrastructure and summarizes the technical system-wide solutions implemented in the P5 technology to tackle and mitigate the data protection risks raised by virtual fences.

In particular, sections 2 deals with the private life issues raised by the concept of virtual fences and the P5 technology in particular. The concept of virtual fences is discussed in this section from a human rights perspective, in particular its implications regarding the right to respect for private and family life, home and correspondence and the right to the protection of personal data as interpreted by the European Court of Human Rights. Section 3 discusses the data protection requirements applicable to the P5 technology, notably in the light of the European directive 95/46. Since the P5 technology primarily relies on video surveillance, we will focus particularly on the data protection requirements applicable to the processing of image data. This section will therefore focus on the relevant European requirements and provide an overview of some national requirements that should be taken into account for the concrete deployment of P5 in a given context. Additionally, the Privacy-by-design principles and their application to video surveillance are discussed. Section 4 summarizes how these principles have been taken into account and implemented in the P5 technology. However, since the technical dimension of privacy is transversal to the P5 project, other working packages (especially WP4 and WP5) have already contributed to a large extent how privacy requirements have been technically implemented, in particular in deliverables D4.1, D4.2 and D5.2. Therefore, section 4 of the present report constitutes a high level presentation of the core privacy solutions developed to tackle and mitigate the privacy and data protection issues identified. Finally, section 5 contains the results of task 2.5. The objective of the task 2.5 was to elaborate frequently asked questions and an ethical roadmap and to collect methods and best practices to help other projects to manage the balance between security and privacy. In that aim, a list of core legal questions that should addressed in the course of a surveillance project and Frequently-Asked-Questions about ethics and Technology Assessment are provided.

(Blank page)

Contents

(Blank page)

1 Introduction

The objective of WP2 is to integrate the privacy dimension (based on legal and social issues) as design criteria for the P5 technology. Besides the management of the Ethical and Legal Advisory Group (T2.4), the tasks included analysis of the scope of privacy issues raised by the technologies (T2.1), definition of the privacy requirements (T2.2), conducting studies regarding the social acceptability of virtual fences (T.2.2), discussion of privacy-preserving implementation possibilities (T2.3), and the preparation of FAQ and a roadmap (T2.5).

Although strongly related between each other, these tasks actually involved research and analysis tasks in three major disciplines, human sciences (in particular, philosophy, political sciences and sociology), legal sciences and technical sciences. All these tasks are transversal and UNamur has contributed on these three dimensions as reflected in the whole tasks.

Deliverable D2.1, dedicated to "social acceptability studies" presented the results of the survey of the social acceptance of virtual fences and discussed the ethical issues raised by virtual fences. Deliverable D2.2 "Privacy and ethics implementation" instead rather focuses on how the rights to privacy and data protection are relevant to the issue of virtual fences for the securization of critical infrastructure and summarizes the technical system-wide solutions implemented in the P5 technology to tackle these issues and mitigate the privacy risks raised by virtual fences.

In particular, sections 2 deals with the private life issues raised by the concept of virtual fences and the P5 technology in particular. The concept of virtual fences is discussed in this section from a human rights perspective, in particular its implications regarding the right to respect for private and family life, home and correspondence and the right to the protection of personal data as interpreted by the European Court of Human Rights. Section 3 discusses the data protection requirements applicable to the P5 technology, notably in the light of the European directive 95/46. Since the P5 technology primarily relies on video surveillance, we will focus particularly on the data protection requirements applicable to the processing of image data. This section will therefore focus on the relevant European requirements and provide an overview of some national requirements that should be taken into account for the concrete deployment of P5 in a given context. Additionally, the Privacy-by-design principles and their application to video surveillance are discussed. Section 4 summarizes how these principles have been taken into account and implemented in the P5 technology. However, since the technical dimension of privacy is transversal to the P5 project, other working packages (especially WP4 and WP5) have already contributed to a large extent how privacy requirements have been technically implemented, in particular in deliverables D4.1, D4.2 and D5.2. Therefore, section 4 of the present report constitutes a high level presenta-

tion of the core privacy solutions developed to tackle and mitigate the privacy and data protection issues identified. Finally, section 5 contains the results of task 2.5. The objective of the task 2.5 was to elaborate frequently asked questions and an ethical roadmap and to collect methods and best practices to help other projects to manage the balance between security and privacy. In that aim, a list of core legal questions that should addressed in the course of a surveillance project and Frequently-Asked-Questions about ethics and Technology Assessment are provided.

2 Virtual fences and the right to respect for private life

Virtual fences intends to deploy surveillance system in surrounding areas of critical infrastructures in view to pre-emptively identify immediate threats and *a posteriori* provide evidence material in the course of an investigation. The solution developed in the course of the P5 project relies on a combination of technologies, associating radars, cameras and thermal sensors. As a case study, the technology is developed for the protection of a nuclear plant installed in Sweden, but the purposes of the present section is to discuss the privacy issues raised by the P5 technology and the concept of virtual fences in a broader perspective. In particular, we would like to discuss here some of the main legal issues that are raised from a human rights perspective, in particular under the article 8 of the European Convention of Human Rights relating to the right to respect for private and family life, home and correspondence. Because the very purpose of virtual fences as conceptualized in the P5 project is the monitoring of nearby areas surrounding a critical infrastructure as a way to strengthen and assist the securization of the premises, such an extension of a surveillance perimeter beyond the premises of the CI may involve public areas, where individuals may be entitled to move freely, and/or private zones and habitations. Of course, much depends on the context where the CI is located, whether in a urban area, sub-urban area or rural area. We would like to address here the extent to which the extension of a surveillance perimeter beyond CI premises involve interferences into privacy rights protected under article 8 of the ECHR and the conditions under which such virtual fences may be admissible. For the record, article 8 paragraph 1 of the ECHR provides that, quote,

> §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*.

End quote. The first part 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.[1] 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[2]. 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. The securization of CI, whether these are under public or private control (depending on national status and legislation) can be qualified as an action of public authorities that is subject to the ECHR.

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.[3] We will rather focus our attention on some important developments of the ECHR caselaw that are of particular interest to the issue of virtual fences deployed for the securization of critical infrastructures. In this aim, we need to address both situations where the surveillance perimeter is extended as to include private spaces/habitations and situations where the perimeter is extended to public areas surrounding the CI. We will start by recalling briefly 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 (2.1). We will then examine the conditions for legitimate interferences into private life under Art. 8§2, namely the legality, legitimacy and necessity requirements which are relevant to the issue of virtual fences (2.2). Finally, we will apply our findings to the case of virtual fences (2.3).

2.1 The right to respect for private life: scope of protection

2.1.1 The right to private life

Originally, the right to privacy was conceptualized in a negative way. It referred to the "*right to be let alone*", which primarily focused on interferences by States in one's private sphere, conceiving the right to privacy as conferring a right to "opacity".[4] As the Court enjoys recalling, the Convention is a "*living instrument*"[5] 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 autono-

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

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

[3] 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)

[4] 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

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

my.[6] The Court has filled the notion of private life gradually so that 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. [7] On this ground the Court expressly stated that "*the notion of 'private life' is a broad one, which is not susceptible to exhaustive definition*"[8]. 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.

2.1.2 The protection of home

The notion of "home" within the meaning of article 8 of the ECHR is an autonomous concept which is not affected by the domestic laws of Members States. The Court makes an interpretation *in concreto,* taking into account: *"the factual circumstances, namely, the existence of sufficient and continuous links with a specific place."*[9]

A home occupied without title or legal right might also be protected by article 8 of the Convention. As an example, an occupied ground is considered by the European Court of Human Rights as a home. The Court takes into account the sufficiently close and continuous connections that someone maintains regardless of the legality of that occupation under domestic law[10].

The area around the home is also protected by article 8 of the Convention. The European Court of Human Rights considers that "*The individual has a right to respect for his home, meaning not just the right to the actual physical area, but also to the quiet enjoyment of that area within reasonable limits. Breaches of the right to respect of the home are not confined to concrete breaches, such as unauthorised entry into a person's home, but may also include those that are diffuse, such as noise, emissions, smells or other similar forms of interference. A serious breach may result in the breach of a person's right to respect for his home if it prevents him from enjoying the amenities of his home. "* [11].

In addition, Members States have a positive obligation to protect the home of individuals against illegal and arbitrary interferences by the State or by any natural or artificial persons[12].

---

[6] 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

[7] An overview of the notion of private life (although not exhaustive) was given by the Court in ECHR, *Pretty v. The United-Kingdom*, 29 April 2002, 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.* [7]" The Court has then officially recognized the right to self-determination in the *Evans v. The United Kingdom*, 7 March 2006

[8] 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*."

[9] ECHR, *Winterstein and others v. France*, 17 October 2013, §141.

[10] *Idem*

[11] ECHR, *Deés v. Hungary,* 9 November 2010 §21

[12] ECHR, *Fernadez Martinez c. Espagne*, 12 June 2014.

2.1.3 The protection 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"."[13]

2.1.4 The right to the protection of personal data

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 information relating to an individual's private life amounts to an interference within the meaning of Article 8.[14] The subsequent use of the stored information has no bearing on that finding.[15] 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*."[16] 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.[17]

Nevertheless, it cannot be considered that the ECHR has brought a general recognition of data protection rights under Article 8 of the ECHR.[18] 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*."[19] It is precisely in cases involving 'public surveillance systems' that the Court has been led to carry out such evaluation. These cases are indeed 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 extent of the protection afforded by article 8 when surveillance systems monitor public spaces/areas.

As explained below, 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

[13] ECHR, *P.G. and J.H. v. United Kingdom*, 25 September 2001, §56
[14] ECHR, *Leander v. Sweden,* 26 March 1987, §48
[15] ECHR, *Amann v. Switzerland*, 16 February 2000
[16] ECHR, *Rotaru v. Romania,* 4 May 2000
[17] ECHR, *Gaskin v. United Kingdom,* 7 July 1989
[18] Paul De Hert, "Balancing security and liberty within the European human rights framework…", *op. cit.*
[19] ECHR, *S. and Marper v. United Kingdom*, 4 December 2008, § 69

cumulative conditions, but enlighten factors helping the Court in its evaluation as to whether certain surveillance measures, although occurring in public spaces or public context, may constitute interference into one's private life.

2.1.5 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.[20] Although not explicitly foreseen in the European Convention of Human Rights, the Court introduced the criterion of "reasonable expectation of privacy"[21], 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*."[22] 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 much 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.[23] 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*."[24] The Court's approach in this ruling is problematic from a data protection perspective[25], since the definition of "processing" does not distinguish whether data is recorded or not.[26]

---

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

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

[22] *P.G. and J.H.*, *op.cit*., §57

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

[24] *Ibidem*

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

[26] 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

Whether 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*."[27]

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*."[28] 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*."[29] 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*."[30] 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.[31]

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 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 ex-*

---

part by automated means: storage of data, carrying out of logical and/or arithmetical operations on those data, their alteration, erasure, retrieval or dissemination" does not expressly refer to the sole 'collection' as an automatic processing.

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

[28] *P.G. and J.H.*, *op.cit*., §54

[29] *Ibidem*, §59-60

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

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

ceeded 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."[32]

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.[33]

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*"[34], 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*".[35]

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*."[36] 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[37], 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).[38]

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.

2.2 Legitimate and proportionate interferences into the right to private life

Once an interference into individual's right is identified, we need to assess whether this interference may be justified under §2 of article 8. For the record, the interference must first be "*in accordance with the law*" (the legal requirement), pursue one of the legitimate goals listed (legitimacy requirement) and be "*necessary in a democratic society*" (proportionality principle).

[32] ECHR, *Peck v. United Kingdom*, 28 January 2003, §62
[33] ECHR, *S. and Marper v. the United Kingdom*, 4 December 2008
[34] According to the argument of the Government of the United Kingdom, §84
[35] *Ibidem*, §85
[36] *Ibidem*, §71
[37] *Ibidem*, §73
[38] *Ibidem*, §75

2.2.1 The legal requirement and legitimacy requirement

First, 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. 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*."[39] 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.[40] 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".[41]

Second, interferences must be justified by one of the goal listed in article 8§2, namely "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.

2.2.2 The necessity requirement: the proportionality principle

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'."[42] 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."[43] 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.

The proportionality test or balancing test has raised considerable discussion among scholars. 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*".[44] 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

---

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

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

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

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

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

[44] 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; 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.[45] The proportionality principle, as a balancing method, is said to allow 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.[46] Nevertheless, the application by the ECHR of the proportionality principle reveals a case by case approach that also raise concerns regarding legal certainty[47], in particular in relation to the application of the proportionality test in the framework of Article 8§2 of the Convention.

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.[48]

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.*[49] 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 social need served by the interference.[50] 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. 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. 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*."[51] Special attention will be paid to the existence of adequate and effective guarantees against abuse and arbitrariness, also in relation to the legal requirement.

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

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

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

[47] 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

[48] 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)

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

[50] 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)

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

dedicated research. Neither this section intends to provide a global overview of ECHR caselaw in relation to new technologies.[52] Instead, we will now apply the interference assessment test and the necessity test to our case study of virtual fences in view of the securization of CI.

2.3 Application to virtual fences

2.3.1 Virtual fences as interferences into individual's rights

Virtual fences, such as P5 technology, deployed around CI involve private life concerns that can qualify as interferences into individual's rights. The combination of different technologies and the deployment of these technologies in different areas imply a harsher degree of interference.

A combination of technologies, associating radars, cameras and thermal sensors

Virtual fences, such as P5 technology, implies a combination of technologies, associating radars, cameras and thermal sensors. Images will be recorded, in particular, for the purpose of providing evidence material in the course of an investigation.

According to ECHR case law, systematic storage of personal implies an interference into privacy[53] independently of the secret nature of the surveillance[54] and independently of the subsequent use of the data[55].

Moreover, P5 technology uses thermal sensors. Thermal sensors could potentially allow to distinguish the facial features, the morphology of persons or to have an overview of their movements. Thermal sensors could detect a group of people and record its movements. As a consequence, in our view, thermal sensors may possibly involve, according to the circumstances, an interference into individuals' rights in particular their right to freedom of movement and their right of freedom of association. This point of view is however debatable. For example, in Belgium, The Court of Cassation considers that: ""*a thermal camera only measures differences of temperature without producing detailed and concrete images of the behavior and presence of persons in the premises*"[56].

Besides, it must be underlined that the virtual fences being developed can potentially generate more data and collect more information than a human eye or even a classical camera. As a consequence, the impact on privacy has to be considered as more serious than the one of "traditional" surveillance camera and therefore, the proportionality test of such a technology has to be assessed in a stricter way (see *infra*).

The deployment of virtual fences in different areas

The seriousness of the privacy interference may depend on the type of place where the surveillance will occur and thus where the CI is located. Whether the perimeter to be

[52] 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)

[53] ECHR, *Leander v. Sweden,* 26 March 1987.

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

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

[56] Cass, 29 october 2013, P. 13. 1270. N/1.

protected includes private sphere, such as home and nearby, or is limited to the public sphere will be determinant in qualifying the seriousness of the interference.

Public sphere

Private life is not limited to the private sphere. As explained earlier, the European Court of Human Rights in the case *P.G. & J.H. v. UK* 2001 ruled that « *there is a zone of interaction of a person with others, **even in a public context**, which may fall within the scope of "private life* ».[57] Consequently, the Court seems to consider that the criteria to determine whether a public area is protected or not by the right to privacy depends on the existence of interactions between people in those areas. P5 technology may observe public areas, for example, a park, a wood or a street where individuals could be entitled to move freely and interact with others. Following the ECHR caselaw, although these places are public, individuals are not entirely deprived of a protection of their private life under article 8.

Professional places

Besides, a surveillance perimeter including offices and workplaces, whether public or private, does not deprive workers from their right to privacy. Workers, even in their professional environment, still enjoy a reasonable expectation of privacy. As has already been stressed, the European Court of Human Rights has observed that "« *it would be too restrictive to limit the notion [of private life] to an "inner circle"* "t*here appears 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*. »[58]

Private places (the monitoring of home and nearby)

The extension of the surveillance perimeter of virtual fences so as to include private homes, private spaces and nearby must also be considered. The monitoring of individual's activities in their private homes indisputably qualifies as a serious interference. The private home is protected by Article 8 of the Convention and may extend, for example, to a professional person's office[59]. The nearby areas of the home are also protected by Article 8 of the Convention "*within reasonable limits*" and according to the ECHR: "*Breaches of the right to respect of the home are not confined to concrete breaches, such as unauthorised entry into a person's home, but may also include those that are diffuse, such as noise, emissions, smells or other similar forms of interference. A serious breach may result in the breach of a person's right to respect for his home if it prevents him from enjoying the amenities of his home*"[60].

2.3.2 The legitimacy of virtual fences

First, interferences must be justified by one of the goals listed in article 8§2 of the ECHR, namely "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."

Virtual fences, such as P5 technology, deployed around CI may pursue a legitimate aim since it could be intended to safeguard "national security", "public safety" or to "prevent disorder or crime" by pre-emptively identifying immediate threats and, *a posteriori*, providing evidence material in the course of an investigation.

---

[57] ECHR, *P.G. and J.H. v. United Kingdom*, 25 September 2001, §56.
[58] ECHR, *Niemietz v. Germany*, 16 December 1992, § 29.
[59] *Idem*
[60] ECHR, *Deés v. Hungary,* 9 November 2010.

Second, interferences into one's private family life, home and correspondence must be in "accordance with the law". In conformity with European Directive 2008/114/EC, all Members States have to ensure an adequate level of protection of IC described in a security plan. The details of such adequate protection measures and the content of the security plans are to be found in national laws implementing the Directive. In Belgium for example, the law of 1st July 2011 determines a mandatory procedure, which must be followed in order to provide an adequate level of internal and external security of the IC. Virtual fences could be included, as a mandatory obligation, in such security plans. Such a modification of the law could satisfy the legality requirement under the ECHR.

In addition, several States have adopted specific legislation for the use of CCTV. These domestic laws should of course be complied with when using systems in such countries. A brief (but non-exhaustive) review of such laws is provided in a section 3.

2.3.3 Virtual fences and proportionality

As explained earlier, article 8§2 then requires to assess whether the interference can be considered as "*necessary in a democratic society*", which implies in practice the application of the proportionality test.

As explained earlier, if State Parties enjoy a margin of appreciation to make the initial assessment of proportionality of an interference, such margin vary according to various factors, such as the nature and seriousness of the interests to be protected from interference, the nature of the interference and the pressing social need served by the interference.[61] The standard of review of the Court then vary according to the margin of appreciation left to States. In general, the more serious is the interference into individuals 'rights, the stricter is the standard of review of the Court.

Basically, in order to carry out such proportionality test, each context where virtual fences may be used and installed thus requires a case-by-case analysis that will, at a minimum, take into the pressing social need to be protected, the seriousness of the interference and the eventual safeguards in place to mitigate the impacts of such interferences.

The pressing social need to be protected

In this case, it implies for instance to consider the level of criticality of the CI, the level of concrete threat demonstrated by the State with respect the specific CI to be protected, and the level of impacts on the society in case of breaches of the security.

There are both European and national classification of CI. Directive 2008/114/EC distinguished for instance national "*critical infrastructures*" as those "*essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions* », from « *european critical infrastructures »,* which are those located in Member States but the disruption or destruction of which would have a significant impact on at least two Member States. The Directive establishes an obligation of identification and securization of CI, which may nevertheless result in diverging approaches across Member States. While a nuclear plant indisputably qualifies as a European infrastructure, the disruption or destruction of which would have extremely serious and long term impacts in several Member States on the health and social well-being of people, an hospital or a prison may be considered as a national CI under national law, but certainly does not imply equivalent risks to the collectivity and society in case of disruption. The level of

[61] ECHR, *Z v. Finland*, 25 February 1997.

criticality thus appear to us essential for the evaluation of the pressing social need to be protected. The qualification of CI alone may not be sufficient. The concrete threats and risks for the society should be assessed on a case by case basis.

The seriousness of the interference into individual's rights

In our view, the seriousness of the interference can be assessed taking into account the scope of the surveillance perimeter (from several meters to several kilometres surrounding the CI?) the types of places monitored within this perimeter (exclusively public spaces? Offices? Private spaces? Homes? Nearby of homes?).

In order to be admissible, the scope of the surveillance perimeter shall be reasonable so as to allow preventive action in case of detection of a threat, but shall not be extended so as to substitute human presence. A very large scope of surveillance allows remote surveillance, but security operators should be able to act as quickly as possible, so as to avoid an infinite extension of the surveillance perimeter compensating an unjustifiable response time of police and security operators. Of course the larger is the scope of surveillance, the more serious may be the interference.

With regard to the types of places included within the surveillance perimeter, we believe that it may be a determinant criterion in the Court's assessment.

If the surveillance perimeter of the virtual fences includes private areas and areas surrounding "homes" (in the meaning of the ECHR), the interference may be considered as particularly serious by the Court. Indeed, monitoring individual's activities in their private homes generally qualifies as a serious interference.

Virtual fences deployed in an urban context for instance, where there are homes, gardens, workplaces, involves a serious interference that could be considered as disproportionate by the European Court of Human Rights. Indeed, in Belgium for example, it is not allowed to place a camera in the direction of a home except in the context of a specific criminal investigation[62] . The interference is considered as particularly serious, thus a camera cannot be installed permanently except by the police and under a specific procedure[63]. Even if image data are blurred, the radars and thermal sensors could allow the collection of data in private homes that may qualify as an interference. Since these sensors allows the detection of humans, they may well reveal the presence (or not) of people in those private places and the kind of activities they are conducting. A strict exclusion of private spaces, premises, buildings and offices should be applied.

In contrast, if the surveillance perimeter of virtual fences includes public spaces only, the interference could be considered as less serious by the Court, and may be considered admissible if the system is subject to adequate safeguards. In this case, it is necessary to provide sufficient guarantees, for example, the storage period should be limited to a fixed period, the zooming capabilities of the cameras should be limited, or resolution of the cameras covering should be limited.

The existence of safeguards to mitigate the impacts of the interferences

Even if virtual fences may be considered legitimate following the pressing security need at stake and the types of places monitored, it remains absolutely necessary that virtual fences be accompanied by sufficient safeguards to ensure an adequate level of privacy protection according to the objective pursued and the other means available. The Court may take due attention of all the safeguards in place to assess the proportionality or not of the surveillance system in a specific given context.

It implies to verify whether individuals are adequately informed about the system (transparency), but also whether appropriate retention duration, conditions for ac-

[62] Art. 46 sexies Code of Criminal Procedure.
[63] Art. 46 sexies Code of Criminal Procedure.

cess/disclosure and supervision by independent supervisory authority of the system have been provided.

As will be explained in section 4 of the present report, P5 technology provides guarantees, for example, a Privacy-aware filter responsible for hiding all privacy-related information that can be used to identify physical person directly or indirectly, a PACM (Privacy-aware access control) responsible for controlling access to raw data, a TTP (Trusted Third Party) responsible for securing the processing of personal data in the protected facility. Taken altogether, these safeguards definitely contribute to make virtual fences compatible with the requirements of article 8 of the ECHR.

Besides, some authors have suggested specific solutions potentially applicable to smart cameras, where “Only suspicious behavior will be reported to the operator or will lead to recording the video. Thereby the human observer can only see the video in case of unusual or noteworthy events. All the other data is deleted immediately. Hence only the privacy of "suspicious" people will be intruded, as they are the only ones becoming identifiable. Yet, no such system will perform without error.”[64] The problem is that “Setting the system to a higher sensitivity could reduce such false negatives but on the other hand this would lead to a higher number of false positives and thus to a higher degree of privacy intrusion: In such a blinkered scenario being tagged as suspicious means data becoming available to humans.”[65] Such a system may be of interest in certain case and limit to the minimum necessary the retention of the data collected but may not be adapted to all contexts of uses.

[64] Koch H., Matzner T. & Krumm, J., "Privacy Enhancing of Smart CCTV and its Ethical and Legal Problems", *op.cit.*
[65] *Idem*.

3 Virtual fences and the right to data protection

If article 8 affords protection to one's private life and if the Court has become familiar with the notion of "personal data", we have seen that the Court's 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. The purpose of this section is to address the application of data protection requirements to virtual fences, in particular the P5 technology.

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. Both rights are therefore protected under an equal value. In this 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[66], 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*."[67]

Article 8 of the Charter of Fundamental Rights provides that "*everyone has the right to the protection of personal data concerning him or her*." Paragraph 2 provides that "*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*", and paragraph 3 that "*compliance with these rules shall be subject to control by an independent authority*."

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

[66] 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

[67] *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

adopted a rather comprehensive approach[68], 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.[69]

The first and fundamental instrument regulating the processing of personal data in the EU is the Directive 95/46 of 25 October 1995.[70] 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[71] or the OECD Guidelines[72]. 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.[73] 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 assessing the data protection requirements applicable to virtual fences, it is therefore essential to understand the importance of EU legal requirements, but also of Member States legal requirements, which will frame in practice the implementation of any surveillance measure such as virtual fences. If the Directive has contributed to a closer approximation of national laws, many divergences of interpretation on several aspects of the law remain.[74]

Besides that, except in relation to electronic communications, European Union law in the field of data protection does not specifically address one or another processing

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

[69] 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

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

[71] Council of Europe Convention 108, *op. cit.*

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

[73] Article 3§1 of Directive 95/46

[74] 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%2Dprotection/document/studies/index_en.htm

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.[75]

This section does not intend to provide an exhaustive analysis of the Directive and national law of implementation. Since the P5 technology primarily relies on video surveillance, it is particularly important to look at the data protection requirements applicable to the processing of image data. This section will therefore focus on the relevant European requirements (3.1) and provide an overview of some national requirements (3.2) that should be taken into account for the concrete deployment of P5 in a given context. Finally, we will comment the Privacy-by-design principles, and their application to video surveillance, which have been the major source of requirements for the design of the P5 technology (3.3).

3.1 European data protection requirements for the use of video surveillance

There is no specific legal instrument regulating video surveillance at EU level. The main applicable instrument is therefore the Directive 95/46. 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 video surveillance. 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.[76] Because of important divergences between Member States regarding the implementation of data protection principles and obligations in relation to video surveillance (see *Infra*), the Working Party issued a first Opinion in 2002[77] and a subsequent opinion in 2004[78] with the aim to contribute to uniform application of national measures.

3.1.1 Scope of application of Directive 95/46 to video surveillance activities

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, most of 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.[79]

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

[76] 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.

[77] Article 29 Data Protection Working Party, *Working Document on the Processing of Personal Data by means of Video Surveillance*, 25 November 2002, WP67

[78] Article 29 Data Protection Working Party, *Opinion 4/2004 on the Processing of Personal Data by means of Video Surveillance*, 11 February 2004, WP89

[79] WP89, p. 13

3.1.2 The notions of personal data and data subjects applied to video surveillance

The concepts of "personal data" and "data subject" are central to the application of the Directive and the national laws of implementation. In Directive 95/46/EC, the two concepts are closely linked, and defined in the same paragraph, Article 2(a), as follows:

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

The Article 29 Working Party[80] has issued a very important opinion[81] on the concept of personal data. According to that document the concept of personal data refers to:

"any information": Directive 95/46/EC is a human rights instrument, thus the concept of "personal data" must be widely interpreted. Hence, it is not limited to information touching the individual's private and family life "*stricto sensu*", or to information of a particularly intrusive, private nature. Mundane, trivial, even publicly-available information, is all included (though, by the way, such information may be subject to relatively lax rules).

The concept of personal data moreover includes not just factual and objective records (name, date of birth, address, occupation, bank account number, face on a videotape, etc.) but also subjective opinions, intentions and predictions, either correct or incorrect, about individuals, regardless of their position of capacity (as consumer, patient, employee, customer, etc.), and regardless of the format or medium on which that information is contained (numerical, graphical, photographical, acoustic,…).

"that relates, even indirectly, to individuals": According to the Article 29 Working Party, there are several ways in which data can be said to "relate" to an individual: "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."

The "content" element is present in those cases where - corresponding to the most obvious and common understanding in a society of the word "relate" - information is given about a particular person, regardless of any purpose on the side of the data controller or of a third party, or the impact of that information on the data subject. Information "relates" to a person when it is "about" that person, and this has to be assessed in the light of all circumstances. For example, video surveillance images on which people can be identified "relate" to those people.

According to the Working Party, a "purpose" element can be responsible for the fact that information "relates" to a certain person as well. That "purpose" element can be considered to exist when the data are used or are likely to be used, taking into account all the circumstances surrounding the precise case, with the purpose to evaluate, treat in a certain way or influence the status or behaviour of an individual. Thus, when a company extracts patterns of video-images with a view to identifying passengers having an "abnormal behaviour" in order to prevent a terrorist threat, those video-images

[80] The Article 29 Data Protection Working Party was set up under the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. It has advisory status and acts independently.

[81] Article 29 Working Party, Opinion Nº 4/2007 on the concept of personal data, WP136, 20.06.2007

ipso facto contain personal data, even if not all passengers are instantaneously identified.

Finally, a third kind of "relating" to specific persons arises when a "result" element is present. According to the Working Party, despite the absence of a "content" or "purpose" element, data can be considered to "relate" to an individual because their use is likely to have an impact on a certain person's rights and interests, taking into account all the circumstances surrounding the precise case. It is worth noting that a major impact is not strictly required: the possibility that the individual is treated differently from other persons as a result of the processing of such data represents a consequence which must be taken into account.

"identifiable": The Working Party Opinion is quite detailed on the various aspects of this element, but its basic approach can be relatively simply summarized: the main point about identification of a person is not whether one knows his/her name, but, on the contrary, whether the person can be distinguished from other members of the group he/she is part of (e.g., a database or other data collection means). Or, we may add, whether one can link information on an otherwise unknown person to information held elsewhere, as when one can determine that a person in one CCTV image is the same person as is captured in another image (or in a database of, say, suspected persons).

As an example, in the London Underground, pictures from CCTV cameras are automatically analysed, by a computer that can detect behavioural patterns that may indicate the intent of a particular person to commit suicide. On the one hand, the system collects information on everyone (and presumably retains this for a limited time), but it singles out only a very few for individualized attention (a security person is sent to the platform in case of an alert). On the basis of the Working Party's approach, one must conclude that the person causing the alert is "identified" - not by name, but by being distinguished from the ordinary, non-suicidal travellers.

Directive 95/46/EC applies whenever an individual is identified or identifiable "*directly or indirectly*"; and the latter includes circumstances in which someone or some (public or private) body, who may or may not be the data controller, is capable of achieving this. As regards "indirectly" identified or identifiable persons, this category typically relates to the phenomenon of "unique combinations". In cases where *prima facie* the extent of the identifiers available does not allow anyone to single out a particular person, that person might still be "identifiable" because that information combined with other pieces of information (whether the latter is retained by the data controller or not) will allow the individual to be distinguished from others. The mere hypothetical possibility to single out the individual is not enough to consider the person as "identifiable".

3.1.3 The notion of processing

This concept is defined in Article 2(b) of Directive 95/46/EC as follows:

> "*processing of personal data" ("processing") shall mean 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*".

The term "processing" here is clearly defined so to include not just "technical" processing but also the collection, recording, consultation, and destruction of personal data. Importantly, it also includes the processes of pseudonymisation and anonymisation

of data: as a result, pseudonymising or (supposedly) anonymising the data is not sufficient, as information controllers must comply with the relevant legal requirements for lawful processing. Thus they may, for instance, need to inform the data subject, or indeed obtain their consent for this processing.

The broad understanding of the concepts of "personal data" and "processing" has the consequence that the principles that will be detailed below apply to a very large scope of sensors such as video surveillance cameras.

3.1.4 Lawfulness of the processing

The principle that a processing should be "lawful" is of particular interest in the framework of video surveillance. Indeed, any processing shall be in accordance with the law, and not only data protection legislation. This is particularly relevant in the case of video surveillance, 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.

3.1.5 Purpose limitation principle

Article 6(1)(b) of Directive 95/46/EC lists the purpose limitation principle among the key data protection principles. It provides that personal data must *be "collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes"*.

Purpose specification is an essential condition to processing personal data and a prerequisite for applying other data quality requirements. Purpose specification and the concept of compatible use contribute to transparency, legal certainty and predictability; they aim to protect the data subject by setting limits on how controllers are able to use their data and reinforce the fairness of the processing. The limitation should, for example, prevent the use of individuals' personal data in a way (or for further purposes) that they might find unexpected, inappropriate or otherwise objectionable.

Hence, the purpose limitation principle imposes that:

First, any purpose must be specified, that is, sufficiently defined to enable the implementation of any necessary data protection safeguards, and to delimit the scope of the processing operation;

Second, to be explicit, the purpose must be sufficiently unambiguous and clearly expressed. Comparing the notion of 'explicit purpose' with the notion of 'hidden purpose' may help to understand the scope of this requirement;

Third, purposes must also be legitimate. This notion goes beyond the requirement to have a legal ground for the processing under Article 7 of the Directive and also extends to other areas of law;

And, **finally**, the prohibition of incompatible use sets a limitation on further use. It requires that a distinction be made between further use that is 'compatible', and further use that is 'incompatible' and therefore prohibited. To assess whether a further use is compatible, an important criteria is the context in which the data have been collected and the reasonable expectations of the data subjects as to their further use.

3.1.6 Legitimate grounds for processing

The Working Party 29 provides examples in relation to each legitimate ground for processing. Except some cases where the video surveillance may possibly (although it is

very questionable) rely on consent[82] and cases where the video surveillance may be necessary to protect the vital interest of the data subject[83], there are mainly two legitimate grounds that may justify video surveillance in the cases of P5, namely the securization of critical infrastructures.

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.[84] Again in Belgium, it is compulsory for certain categories of casinos and gambling establishments to install a video surveillance system.[85] It is possible that certain Member States explicitly provide for the securization, by means of video surveillance, of critical infrastructures.

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 video surveillance should always be grounded on express legal provisions if they are carried out by public bodies.[86] The securization of CI with the P5 technology, whether by a public or private body, may well be considered as carried out in the public interest or in the exercise of official authority vested in the controller.

3.1.7 Principle of subsidiarity of video surveillance

Video surveillance 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 video surveillance, in particular considering the increasingly use of cameras near public buildings and offices.

3.1.8 Principle of proportionality

Video surveillance systems should only be installed for purposes that actually justify recourse to such systems. Basically, "whilst a proportionate video surveillance and alert-

[82] For example, concerning premises where a person's private life is led, such as in the case of installation of cameras in co-ownership

[83] The Working Party refers to the distance monitoring of patients in resuscitation units

[84] 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

[85] 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

[86] WP89, p. 18

ing 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."[87] 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".

3.1.9 Data quality principle

The data quality principle derives from Article 6.1(b) and (c) of Directive 95/46/EC, which provide that personal data must be "*collected for specified, explicit and legitimate purposes" and must be "adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed*."

This principle requires a careful assessment of the filming arrangements, which may be defined following the principle of privacy-by design (see *infra*).

The Directive also limits the nature and amount of data that can be collected. The adequacy, accuracy, up-to-date, relevance or excessiveness of personal data is also to be assessed with reference to the specified purpose or purposes. According to this principle, only the data needed to achieve the specified purpose may be collected. As an example, the Article 29 Working Party recommends that data processed by video surveillance in public transportation should be limited: *"Video surveillance in public transportation systems should be designed in a way that the faces of traced individuals are not recognizable or other measures are taken to minimize the risk for the data subject. Of course, an exception must be made for exceptional circumstances such as if the person is suspected of having committed a criminal offence"*.[88]

Furthermore, as the Directive puts it in Art. 6(1)(d), "*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". Data that are "adequate" or sufficiently accurate or "complete*" for one purpose may therefore well be inadequate and insufficiently accurate or complete for other purposes. And finally, data may only be held as long as necessary for the purpose(s) for which they were collected or used. The data retention period is, therefore, also linked to the specified purpose: in other words, data held for one purpose may be kept for longer (or less long) periods than data kept for other purposes.

Note that in some Member States, the retention period for video surveillance data is specifically regulated. As an example, in Belgium, video surveillance data may not be kept longer than one month if the data does not serve as evidence in court (see *Infra*).

3.1.10 Transparency principle

The European Data Protection Directive 95/46/EC contains general provisions to ensure that data subjects are informed of their rights to data protection. These requirements are contained in the following articles:

- Article 6(1)(a), which requires that personal data be processed "fairly and lawfully";
- Article 10, which contains minimum information that must be provided to the data subject in cases when the data are collected directly from him.

[87] WP 89, p. 19

[88] Article 29 Working Party, WP 168, "The Future of Privacy" Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data, Adopted on 01 December 2009, p. 14.

- Article 11, which contains minimum information that must be provided to the data subject in cases when data about him are collected from a third party.
- Article 14, which contains a requirement to inform the data subject before personal data are disclosed to third parties.

Besides, the Directive distinguishes between two types of information:

- Essential information, namely– the identity of the controller and of his representative, if any, as well as the purpose of the data processing except where the data subject already has this information; and;
- Possible "further information", including the recipient of the data, the response obligation and the existence of access and rectification rights, as far as such further information is necessary having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject.

Note that the laws in the Member States considerably vary with regard to the kinds of information that must be provided, the form in which it must be provided, and the time at which it must be provided. They also differ as to the kinds of additional information that may need to be provided to ensure a fair processing. Some Member States repeat the examples given in the Directive, others give somewhat different examples, and some give no examples at all.

In order to facilitate the respect of the transparency requirement, the Article 29 Working Party provided guidelines[89], and examples of information notices[90]. Also note that some national law regulating video surveillance imposes standard information notices. This is for example the case in Belgium. A brief review of some domestic laws is provided in section 3.2 below.

3.1.11 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 video surveillance 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.[91]

3.2 National requirements applicable to video surveillance

Given the increasing development of video surveillance technologies, several States have adopted specific legislation in the area for the deployment/use of CCTV. These domestic laws should of course be complied with when deploying/using systems in such countries. A brief (but non-exhaustive) review of such laws is provided in this section. We will see that the implementation (both in law and in practice) in Member States of

[89] Article 29 Working Party, Opinion 10/2004 on More Harmonised Information Provisions, WP100, 25/11/2004

[90] An example of such an information notice is available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp100a_en.pdf

[91] WP89, p. 24

the general requirements of the Directive 95/46 to video surveillance 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, Italy or Poland however, there is no specific legislation applicable. Certain legal frameworks distinguish different categories of spaces, providing specific rules for the monitoring of each category of places. This is highly relevant for the issue of virtual fences in order to determine the conditions applicable to the monitoring of each category of places.

3.2.1 France

The regulation of video surveillance in France mainly follows from two laws. The Act on Information Technologies and Civil Liberties ('Loi Informatique et Libertés')[92] 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'[93] (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.[94] 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.

"Videoprotection" of publicly accessible spaces/premises

Video surveillance 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 "video surveillance" into "videoprotection". It is important to notice that the scope of application of the LOPSI Act covers all video surveillance 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 ter-

[92] 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

[93] 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

[94] See CNIL Press Release of June 2012 on best practices in relation to videoprotection and video surveillance, at https://www.cnil.fr/fr/videosurveillance%2Dvideoprotection%2Dles%2Dbonnes%2Dpratiques%2Dpour%2Ddes%2Dsystemes%2Dplus%2Drespectueux%2Dde%2Dla%2Dvie (equivalent to https://www.cnil.fr/fr/videosurveillance-videoprotection-les-bonnes-pratiques-pour-des-systemes-plus-respectueux-de-la-vie)

rorist acts; 7) prevention of natural or technological disasters; 8) emergency assistance to individuals and fire protection; 9) safety of installations in amusement parks.[95]

Regarding publicly accessible premises (whether public or private premises), video surveillance 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*."[96]

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.[97] 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.[98]

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).

"Video surveillance" of non publicly accessible spaces/premises

Video surveillance 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 cetera…) and obligations (information, declaration et cetera…) enshrined in the law.

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 "video surveillance system" in non-publicly accessible premises (30% of the controls)
- Lack of declaration to the CNIL in cases of video surveillance 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%)
- nsufficient security measure (20%)[99]

[95] Unofficial translation by the author, see article 10 II. of the LOPSI Act

[96] 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 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.* »

[97] Article 10 III. of the LOPSI Act

[98] 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

[99] See CNIL Press Release of June 2012 on best practices in relation to videoprotection and video surveillance, *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 video surveillance in public spaces, at work, in schools, shops, living buildings, and home.[100]

3.2.2 Belgium

The legal framework applicable to video surveillance in Belgium is rather complex since it follows from a series of general and sectoral legislations, the articulation of which has raised many questions and issues.[101] Belgium provides for a specific legislation in relation to video surveillance adopted in 2007[102], and further amended in 2009[103]. Besides this specific legislation, the Privacy Act of 1992[104], 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.[105] 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 video surveillance law, because of its relevance as a specific legislation.

Scope of application of the video surveillance law

The Video surveillance 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.[106] 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 not apply to "simulated" cameras.[107] It also applies

[100] All these information notices are downloadable at http://www.cnil.fr/les%2Dthemes/videosurveillance/

[101] 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

[102] 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 "video surveillance law"

[103] Loi visant à modifier la loi réglant l'installation et l'utilisation de cameras de surveillance du 12 novembre 2009, *MB,* 18/12/2009

[104] 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

[105] 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 Video surveillance Law of 2012 ».

[106] Unofficial translation of article 2, 4° of the Law on video surveillance : « *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* »

[107] Frequently Asked Questions, Privacy Commission Recommendations regarding the Video surveillance Law of 2012, p. 4

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.[108] This has led to a series of questions regarding the articulation of the video surveillance law with other specific legislations.

Furthermore, it is provided that the general Privacy legislation remains applicable, except where it is explicitly contrary to the video surveillance 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 video surveillance 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 video surveillance 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.

Video surveillance in publicly accessible open spaces ("lieu ouvert"[109])

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.[110] They are considered to include all "public spaces" in general, such as public roads ("voie publique"), market place, streets, squares, public gardens and parks.[111] 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.[112]

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 the Chief Police Zone.[113] 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.[114] This means that when a camera monitoring a street will include in its visual angle the entrance of a pri-

---

[108] Article 3 of the Law on video surveillance

[109] Defined as "*tout lieu non délimité par une enceinte et accessible librement au public*"

[110] 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* »

[111] Privacy Commission Note relative à la loi réglant l'installation et l'utilisation de caméras de surveillance, 20/01/2010, p. 5,

[112] 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 »

[113] Article 5§2 of the Law on video surveillance

[114] Article 5§3 last alinea of the Law on video surveillance : « *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*. »

vate 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.[115] The video surveillance system should be announced via a standard pictogram as provided by Royal Decree.[116]

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.[117] 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.

Video surveillance in closed spaces, publicly accessible ("lieu fermé accessible au public"[118]) or non-publicly accessible ("lieu fermé non accessible au public[119])

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.[120] 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.

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.[121]

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.[122] The cameras should be oriented so as to limit to the

[115] Ministerial Circular of 2009, point 1.4 "proportionality of images"

[116] Arrêté Royal du 10 février 2008 définissant la manière de signaler l'existence d'une surveillance par caméra, *MB*, 21/02/2008

[117] Article 5§4 of the Law on video surveillance: "*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* »

[118] Defined as "*tout bâtiment ou lieu fermé destine à l'usage du public, où des services peuvent lui être fournis*"

[119] Defined as "*tout bâtiment ou lieu fermé destine uniquement à l'usage des utilisateurs habituels*"

[120] Ministerial Circular of 2009, point 1.5.2. "Difference between closed premises publicly accessible and non publicly accessible"

[121] Article 6§2 and 7§2 of the Law on video surveillance

[122] Ministerial Circular of 2009, point 1.4 "proportionality of images"

maximum extent the filming of the open space.[123] The video surveillance system should be announced via a standard pictogram as provided by Royal Decree.[124]

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.[125] 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.[126] The controller can nevertheless transmit the images to police services.[127] The police services can request the access to images from cameras installed in "closed spaces" whether publicly accessible or not.[128] 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.[129]

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 video surveillance, except under specific legal circumstances: during the 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.[130]

3.2.3 Italy

There is no specific CCTV law in Italy. A decision from April 8th 2010[131] refers for CCTV to the "Data protection Code"[132] implemented by the Italian Data Protection Agency. The decision on April 8th 2010 underlines the same general principles as the Data protection Code on personal data treatment: a measure must be proportional, necessary and in conformation with the Italian law and the Data protection Code.[133] Specifically for the private sector, Italy adopted a "*Code of conduct and professional practice apply-*

[123] Article 7§2 of the law on video surveillance

[124] Arrêté Royal du 10 février 2008 définissant la manière de signaler l'existence d'une surveillance par caméra, *MB*, 21/02/2008

[125] Article 5§4 of the Law on video surveillance: "*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* »

[126] Article 9 of the Law on video surveillance

[127] Article 9 1° of the law on video surveillance

[128] Article 9§2 of the Law on video surveillance

[129] *Ibidem*

[130] Privacy Commission Recommendations regarding the Video surveillance Law of 2012, p. 9

[131] Italian Data Protection Authority, 'Video Surveillance Guidelines', Rome, *Garante per la Protezione dei dati personali* (8 April 2010). Available at: http://www.garanteprivacy.it/web/guest/home/docweb/%2D/docweb%2Ddisplay/docweb/1767009

[132] Legislative Decree 196/2003 bearing the adoption of the *Codice in material di protezione dei dati personali.*
Available at
http://194.242.234.211/documents/10160/2012405/DataProtectionCode%2D2003.pdf

[133] Italian Data Protection Authority, 'Video Surveillance Guidelines', *op. cit.*

ing to information systems managed by private entities with regard to consumer credit, reliability, and timeliness of payments".[134]
In publicly accessible places, people must be informed of the camera installation. A sign must appear with a camera symbol, the name of the person in charge for the installation and the reasons for monitoring, for example, guarantee urban safety in public space, protection of property, collecting evidence.[135]

Some data protection code dispositions, for example the obligation of information, must not be respected if the cameras are installed under the competence of the Data Processing Centre at the Public Security Department or by the police. For example when data must be transferred by public bodies with the aim "of protecting public order and security, the prevention, detection or suppression of offences as expressly provided for by laws that specifically refer to such processing."[136]
The images from cameras installed for public order can been retained for a maximum of 24 hours.[137] The national Police can keep the images for 7 days for investigation of crimes. In case of terrorism they can keep the images up to thirty days.[138]

The involved persons have a right to know if there are personal data about them and may ask for erasure[139]. Under article 7, clause 2 of the Data protection Code, the right to information gives access to:

a) *the origin of his/her data;*
b) *the aim and modality of data retention;*
c) *the criterion according to which the data are stored in an electronic system;*
d) *the identification of the data controller and processor;*
e) *the subjects and related categories of subjects the personal data could be transmitted to, as representatives of the State or persons responsible for the data retention and management*

In some cases, the involved person may request deletion of personal data. By virtue of to Article 7, clause 3 of the Data Protection Code:

a) *the update, the modification and, when necessary, the integration of his/her personal data*
b) *the deletion, the conversion into an anonym form or the block of data retained infringing the law, included those data for which is not necessary to gather in light of the aims according to which they have been collected or afterwards retained;*
c) *the guarantee that any of the operations described in a) and b) above would be communicated to the data subject by the person to whom the data have been transmitted and diffused. The exception is the case when this communication is objectively impossible because it is disproportional compared to the protected right"*

[134] Published in the Official Journal no. 300 dated 23 December 2004 and subsequently amended by the notice published in the Official Journal no. 56 dated 9March 2005
Available at:
http://www.garanteprivacy.it/web/guest/home/docweb/%2D/docweb%2Ddisplay/docweb/1079077
[135] Italian Data Protection Authority, 'Video Surveillance Guidelines', *op.cit.*
[136] Section 53 Data protection Code.
[137] Italian Data Protection Authority, 'Video Surveillance Guidelines', *op.cit.*
[138] Garante per la protezione dei dati pernali, Prescrizioni per la videosorveglianza presso i siti di interesse culturale maggiormente esposti alla minaccia terroristica (12 March 2009).
Available at:
http://www.garanteprivacy.it/web/guest/home/docweb/%2D/docweb%2Ddisplay/docweb/1002987
[139] Article 7 Data protection Code.

Under article 7, clause 4 of the Data protection Code, the involved person can make an opposition:

a) *for legitimate motives concerning the data retention, also related to the aim of the data gathering;*
b) *against the data retention aimed at publicity or for direct sales or marketing research or commercial communications"*

The delay to answer to the request is 15 days[140]. The Code defines some exceptions for the delays for example in cases of complexity. In practice, it is difficult for citizens to exercise their rights[141]. The Italian Data protection Authority[142] sets up to protect the privacy and fundamental rights and freedoms, takes recommendations and processes the complaints.

3.2.4 United Kingdom

United Kingdom is notorious for an incredible amount of cameras in the streets. Private companies involved estimate that there are more than 5.9 millions cameras.[143] The Data Protection Act (DPA) of 1998 concerns most privacy-related issues.[144]

Regarding the lack of specific video surveillance legislation, United Kingdom adopted a CCTV code of practice under the Protection of Freedoms Act[145] and developed by the Information Commissioner's Office.[146] The aim of this code "*will be to ensure that individuals and wider communities have confidence that surveillance cameras are deployed to protect and support them, rather than spy on them".*[147] This code is a non-statutory instrument with 12 extremely vague guidelines:

1. always be for a specified purpose which is in pursuit of a legitimate aim and necessary to meet an identified pressing need;
2. take into account its effect on individuals and their privacy;
3. have as much transparency as possible, including a published contact point for access to information and complaints;
4. have clear responsibility and accountability for all surveillance activities including images and information collected, held and used;
5. have clear rules, policies and procedures in place and these must be communicated to all who need to comply with them;
6. have no more images and information stored than that which is strictly required;
7. restrict access to retained images and information with clear rules on who can gain access;
8. consider any approved operational, technical and competency standards relevant to a system and its purpose and work to meet and maintain those standards;

[140] Article 146, clause 2 Data Protection Code.

[141] There are a lot of cases law, see on Italy Country Reports, *Increasing reslience in surveillance societies (IRISS)*, April 2014, http://irissproject.eu/wp%2Dcontent/uploads/2014/06/Italy%2DComposite%2DReports%2DFinal.pdf For examples of how video surveillance is applied in some Italian cities, see Vv.Aa. European Forum for Urban Security, 'Citizens, Cities and Video Surveillance. Towards a Democratic and Responsible Use of Cctv', Montreuil, European Forum for Urban Security (2010).

[142] Section 154 (1) c of the Data Protection Code, see on http://www.garanteprivacy.it/

[143] David Barrett, D.: One surveillance camera for every 11 people in Britain, says c-ctv survey. http://www.telegraph.co.uk/technology/10172298/One-surveillance-camera-for-every-11-people-in-Britain-says-CCTV-survey.html

[144] Data Protection Act 1998, available online at: http://www.legislation.gov.uk/ukpga/1998/29/contents

[145] Section 32(1) of Protection of Freedoms Act.

[146] Home Office (2013) '*Surveillance Camera Code of Practice'*, available online at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/204775/Surveillance_Camera_Code_of_Practice_WEB.pdf

[147] Home Office (2013) 'Surveillance Camera Code of Practice', *Ibidem* p. 5

9. be subject to appropriate security measures to safeguard against unauthorised access and use;
10. have effective review and audit mechanisms to ensure legal requirements, policies and standards are complied with;
11. be used in the most effective way to support public safety and law enforcement with the aim of processing images and information of evidential value, when used in pursuit of a legitimate aim;
12. be accurate and kept up to date when any information is used to support a surveillance camera system which compares against a reference database for matching purposes.

A Surveillance Camera Commissioner control the guidelines application.[148] He is also in charge of "encouraging compliance with the code, reviewing the operation of the code, providing advice about the code (including changes to it or breaches of it)".[149] An authorisation is not necessary for a camera installation except if the operations involved people specifically targeted for investigations. The request must specify witch activity will be filmed and the responders examine the consequences for the privacy of the people who are not concerned by the investigation.[150] The right to personal data access is regulated by section 7 of DPA.[151] The controller has 40 days to answer.[152] In some cases the access can be denied, for example for national security, crime detection and the assessment or collection of tax...[153]

3.2.5 Poland

There is no specific legal regulation for CCTV in Poland. A camera installation and the image treatment are subject to the general provisions of data processing act.[154] The absence of specific legislation causes difficulties for video monitoring activities. Many NGOs and Humans Rights associations recommend that Polish institutions adopt video surveillance laws as many cameras are installed without legal basis[155] and the Polish government has a project to finance more cameras.[156]

The Ministry of Internal Affairs adopted on July 10th 2014 new guidelines for the respect of privacy and fundamental liberties[157]. The project make the difference between open spaces (streets, parks, squares) and closed spaces (schools, bank, shops, offices). In the public space, for large public events, the installation of cameras is subject to a specific legislation.[158] The installation requires an authorisation from the municipal council and a public consultation.

---

[148] Code of practice is also applied to the Automatic Number Plate Recognition (ANPR). See on https://www.gov.uk/government/publications/circular%2D0112013

[149] Section 34 of Protection of Freedoms Act.

[150] Information Commissioner's Office (2013b) 'Register of data controllers'

[151] Note that the interpretation of the concept of "personal data" and the right to access to such data is the subject of case law. See on http://irissproject.eu/wp%2Dcontent/uploads/2014/06/UK%2DComposite%2DReports%2DFinal.pdf

[152] Information Commissioner's Office (2013a) 'Find out how to access your personal information' available online at https://ico.org.uk/for%2Dthe%2Dpublic/personal%2Dinformation/

[153] Sections 28 to 34 Data Protection Act.

[154] The Act of 29 august 1997 on the protection of personal data, See on http://www.giodo.gov.pl/

[155] Opinion no. 28 of the European group on ethics in science and new technologies, p.40 see on http://www.statewatch.org/news/2014/jun/eu%2Dcom%2Dopinion%2Dethics%2Dsecurity%2Dsurveillance%2Dtechnologies.pdf

[156] Poland: *New project on public institutions' surveillance practices*, see on https://edri.org/poland%2Dnew%2Dproject%2Dpublic%2Dinstitutions%2Dsurveillance%2Dpractices/

[157] M. KOGUT, *Poland is developing video monitoring law,* see on http://globalcompliancenews.com/author/magdalenakogut/

[158] Act of 20 March 2009, Law Gazette 2013 Art. 6114

In closed places, the installation can be made by private companies if in charge of the area. Citizens have a right to be informed about the surveillance by a signalisation. The image can be retained for maximum 90 days. In case of automatic recognition, the installation must respect additional obligations[159].

3.3 Privacy-by-Design requirements

The concept of "*privacy by design*" refers to the idea that privacy and data protection should be integrated into the design of Information and Communication Technologies. The application of such principle would emphasize the need to implement privacy enhancing technologies. This principle of "*Privacy by Design*" applies to data controllers, but also to technology designers and producers. "*Privacy by design*" means that ICT should not only maintain security but also should be designed and constructed in a way to avoid or minimize the amount of personal data processed. These principles have been taken into account as a method to take into privacy and data protection requirements.

3.3.1 Privacy by design principles

The concept of **privacy-by-design** is coined by Ann Cavoukian, the Ontario's Information and Privacy Commissioner, 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 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."[160]

In practice, the implementation of the privacy by design principle will require the evaluation of several, concrete aspects or objectives of the user requirements and system specifications. In particular, when making decisions about the design, acquisition and running of a processing system, the following general aspects / objectives should be respected:

- **Data Minimization**: data processing systems are to be designed and selected in accordance with the aim of collecting, processing or using no personal data at all or as few personal data as possible.
- **Controllability**: an IT system should provide the data subjects with effective means of control concerning their personal data. The possibilities regarding consent and objection should be supported by technological means.
- **Transparency**: both developers and operators of IT systems have to ensure that the data subjects are sufficiently informed about the means of operation of the systems. Electronic access / information should be enabled.
- **User Friendly Systems**: privacy related functions and facilities should be user friendly, i.e. they should provide sufficient help and simple interfaces to be used also by less experienced users.
- **Data Confidentiality**: it is necessary to design and secure IT systems in a way that only authorised entities have access to personal data.
- **Data Quality**: data controllers have to support data quality by technical means. Relevant data should be accessible if needed for lawful purposes.
- **Use Limitation**: IT systems which can be used for different purposes or are run in a multi-user environment (i.e. virtually connected systems, such as data warehouses, cloud computing, digital identifiers) have to guarantee that data and processes serving different tasks or purposes can be segregated from each other in a secure way.

In order to ensure that the design of CCTV systems does not adversely impact on privacy, these "privacy by design" principles should be applied.

3.3.2 Privacy-by-design applied to CCTV

Subsidiarity of video surveillance

The principle that data must be adequate and proportionate to the sought purposes means, in the first place, that CCTV and similar surveillance equipment may only be deployed on a subsidiary basis. According to the Article 29 Working Party *"that is to say that it should be avoided, for instance, that a company installs video surveillance equipment in connection with minor offences. In other words, it is necessary to apply, on a case by case basis, the principle of adequacy in respect of the purposes sought, which entails a sort of data minimisation duty on the controller's part"*[161].

According to the Working Party, "*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 – as described to a data protection authority -, or else at identifying citizens liable for minor administrative offences such as the fact of leaving waste disposal bags outside litter bins and/or*

[160] 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

[161] Article 29, WP 67, *op.cit.*

in areas where no litter is to be left about. Proportionality should be assessed on the basis of even stricter criteria as regards non-publicly accessible premises."[162]

If the video surveillance is carried out for security purposes, the data controller should carefully evaluate risks, and not merely state that the purpose is to "*observe any anomalies inside the security perimeter*", or "*to deal with security incidents*". Indeed, the data controller should not only have a general idea of what they wish to use their system for, but should also detail the types of security incidents that are expected to occur in the area under surveillance and that they wish to deter, prevent, investigate or prosecute using the cameras.

In our case, this evaluation has been thoroughly done in the deliverable D3.1 on user requirements.

Proportionality of the filming arrangements

As an example, concerning video surveillance, the Article 29 Working Party recommends the following:

> *"The filming arrangements will have to be taken into account in the first place, by having regard, in particular, to the following issues:*
> - *the visual angle as related to the purposes sought. E.g., if the surveillance is performed in a public place, the angle should be such as not to allow visualising details and/or somatic traits that are irrelevant to the purposes sought, or else the areas inside private places located nearby, especially if zooming functions are implemented,*
> - *the type of equipment used for filming, i.e. whether fixed or mobile,*
> - *actual installation arrangements, i.e. location of cameras, use of fixed view and/or movable cameras, etc.,*
> - *possibility of magnifying and/or zooming in images either at the time the latter are filmed or thereafter, i.e. as regards stored images,*
> - *image-freezing functions,*
> - *connection with a "centre" to send sound and/or visual alerts,*
> - *the steps taken as a result of video surveillance, i.e. shutting down of entrances, calling up surveillance staff, etc. .*
>
> *[…] The above safeguards are meant to implement, also operationally, the principle referred to in the domestic laws of a few countries as the principle of moderation in the use of personal data – which is aimed at preventing or reducing, to the greatest possible degree, the processing of personal data. This principle should be implemented in all sectors by also having regard to the fact that many purposes can be actually achieved without making recourse to personal data, or by using really anonymous data, even though they may initially seem to require the use of personal information."*[163]

A possible solution has been proposed by A Senior et al.[164]: protection of privacy is based on a layered access model enforced by a multi-level access control system architecture. The access model defines the access right based on the following questions: 1) what data is present, 2) has the subject given consent, 3) what form does the data take, 4) who sees the data, 5) how long is data kept, and 6) how raw is the data. The answers to these questions lead to a layered access model. Raw video stream is further processed, and information is extracted to generate versions of different image details. For

[162] *Ibidem*

[163] *Ibidem*

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

example, the access model can include three layers for three types of users: ordinary users can only access statistical information, privileged users can access limited individual information, and law enforcement agencies can access raw video information. Figure 3 illustrates the concept.

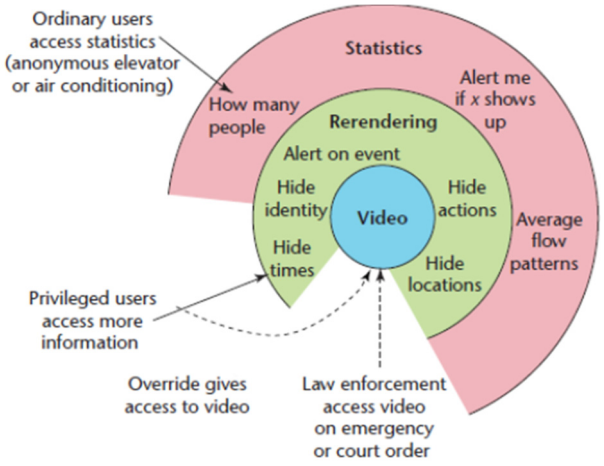


Figure 1. A layered access model to the presentation of video surveillance.

Data quality and data minimization

According to this principle, only the data needed to achieve the specified purpose may be collected. As an example, the Article 29 Working Party recommends that data processed by video surveillance in public transportation should be limited: *"Video surveillance in public transportation systems should be designed in a way that the faces of traced individuals are not recognizable or other measures are taken to minimize the risk for the data subject. Of course, an exception must be made for exceptional circumstances such as if the person is suspected of having committed a criminal offence".*[165]

In other terms, the resolution of the images should correspond to the aim of the processing: the resolution for detection in live operation should be lower than the resolution used for recorded evidence.

[165] Article 29 Working Party, WP 67, *op.cit.*

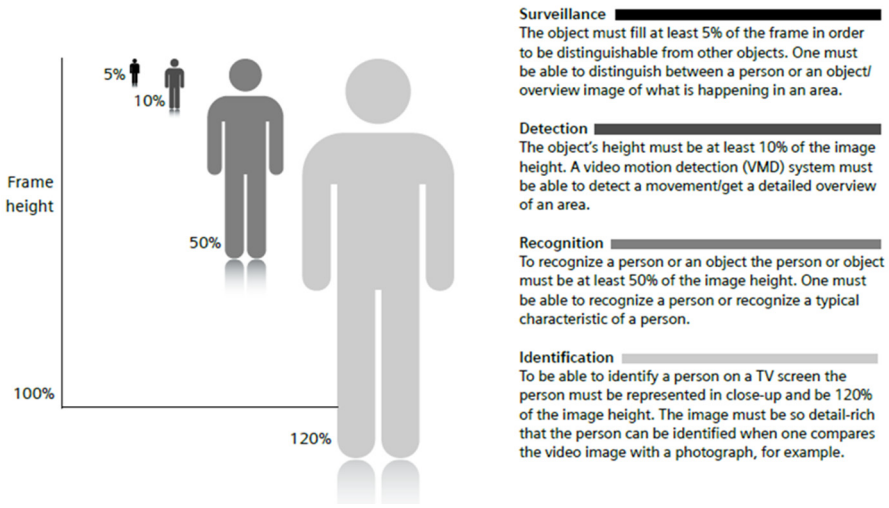


Figure 2. Video surveillance system's generic missions (extract from Video Surveillance Portfolio overview, SIEMENS 2010).

In Figure 4, it is proposed to discriminate the video surveillance systems (technical) capabilities using a video detail sorting capability, and by adding the recording and live operation dimension. This leads to the classification below:

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

Masking or scrambling images to help eliminate surveillance of areas irrelevant to the surveillance target or lowering the resolution of the images so that people could not be recognized or identified in certain areas can thus be useful. This technique is also useful to edit out images of third persons when providing access to the images of a data subject.

Storage and retention period

According to article 6 e) of Directive 95/46/EC, recordings must not be retained longer than necessary for the specific purposes for which they were made. It must also be considered whether recording is necessary in the first place and whether live monitoring without recording would be sufficient.

If a data controller opts for recording, it must specify the period of time for which the recordings will be retained. Some domestic laws specify maximum retention periods. After the lapse of this period the recordings must be erased. If possible, the process of erasure should be automated, for example by automatically and periodically overwriting the media on a first-in, first-out basis. Once the media is no longer useable (after many cycles of use) it must be safely disposed of in such a manner that the remaining data on it would be permanently and irreversibly deleted (e.g. via shredding or other equivalent means). If the purpose of the video surveillance is security and access control, and a security incident occurs and it is determined that the recordings are necessary to further investigate the incident or use the recordings as evidence, the relevant footage may be retained beyond the normal retention periods for as long as it is necessary for these purposes. Thereafter, however, they must be also erased.

A register - whenever possible, in an electronic form - should be held to keep track of any recording that is retained beyond the normal retention period, indicating:

- the date and time of the footage and camera location,
- a short description of the security incident,
- the reason why the footage needs to be retained and
- the expected date of the review of the necessity to retain the footage any longer.

In the case of P5, it is therefore important to check the applicable national requirements regarding retention. This requirement will vary from one Member State to the other. In case a Member State does not provide for any specific retention duration, it will be the responsibility of the data controller to define such retention period following the principle of “necessity”.

Data security

First and foremost, an internal analysis of the security risks must be carried out to determine what security measures are necessary to protect the video surveillance system, including the personal data it processes. In all cases, measures must be taken to ensure security with respect to:

- transmission,
- storage (such as in computer databases), and
- access (such as access to computer systems and premises).

Transmission must be routed through secure communication channels and protected against interception. Protection against interception is especially important if a wireless transmission system is used or if any footage is transferred via the Internet. In these cases the data must be encrypted while in transit or equivalent protection must be provided. Encryption or other technical means ensuring equivalent protection must also be considered in other cases, while in transit and while in storage, if the internal analysis of the security risks justifies it.

All premises where the video surveillance footage is stored and also where it is viewed must be secured. Physical access to the control room and the room storing the video surveillance footage must be protected. No third parties (e.g. cleaning or maintenance personnel) should have unsupervised access to these premises. The location of monitors must be chosen so that unauthorized personnel cannot view them. If they must be near the reception area, the monitors must be positioned so that only the security personnel can view them.

A reliable digital logging system must be in place to ensure that an audit can determine at any time who accessed the system, where and when. The logging system must be able to identify who viewed, deleted, copied or altered any video surveillance footage. In this respect, and elsewhere, particular attention must be paid to the key functions and powers of the system administrators, and the need to balance these with adequate monitoring and safeguards.

A process must also be in place to appropriately respond to any inadvertent disclosure of personal information. This should include, whenever possible, notification of the breach to those whose data are inadvertently disclosed as well as to the company’s data protection authority.

The security analysis as well as the measures taken to protect the video surveillance footage must be adequately documented.

Access to the images

Access rights must be limited to a small number of clearly identified individuals on a strictly need-to-know basis. It must also be ensured that authorized users can access only those personal data to which their access rights refer. Access control policies

should be defined following the principle of "least privilege": access right to users should be granted to only those resources which are strictly necessary to carry out their tasks.

Only the "controller", the system administrator, or other staff member/s specifically appointed by the controller for this purpose should be able to grant, alter or annul access rights of any persons. Any provision, alteration or annulment of access rights must be made in accordance with criteria established in the company's video surveillance policy. Those having access rights must at all times be clearly identifiable individuals.

The video surveillance policy must clearly specify and document who has access to the video surveillance footage and/or the technical architecture of the video surveillance system, for what purpose and what those access rights consist of. In particular, one must specify who has the right to:

- view the footage real-time,
- operate the pan-tilt-and-zoom ("PTZ") cameras,
- view the recorded footage, or
- copy,
- download,
- delete, or
- alter any footage;

Any distinction between the rights of different categories of persons must be clearly specified. For example, those

- monitoring the images live,
- responsible for the technical maintenance of the system, or
- investigating security incidents

Each of them has different tasks and should therefore have different access rights to the system. In-house personnel and outside contractors will also have different tasks and should therefore also have different access rights. Access rights should be technically built into the system. For example, the user profile of one individual may allow copying recorded footage, while the profile of another only allows viewing rights. In addition, the access policy must also clearly describe the conditions under which access rights may be exercised. For example, in which cases a person whose profile allows copying or deletion is actually authorized to copy or delete any footage.

When the video surveillance is carried out for purposes of security and access control, no access rights should be given to anyone other than in-house and outsourced security personnel and those responsible for the technical maintenance of the system. All personnel with access rights, including outsourced personnel carrying out the day-to-day CCTV operations or the maintenance of the system, should be given data protection training and should be familiar with the provisions of Directive 95/46/EC insofar as these are relevant to their tasks. The training should pay special attention to the need to prevent the disclosure of video surveillance footage to anyone other than authorized individuals.

In P5, the implementation of access control mechanisms has been one of the main concern. We will now briefly see how these requirements have been implemented in the P5 technology.

4 Privacy solutions implemented

Ensuring the implementation of privacy and data protection requirements under European law has been one of the main task in P5. The legal requirements in particular are analysed based on the EU Directive 95/46/EC as reported in deliverable D3.1, D2.2 and D5.2. As explained in the previous sections, EU Directive 95/46/EC specifies rules for handling personal data. The directive defines objectives for the legislation of the member states of the European Union and it is binding on the member states as to the result to be achieved but leaves them the choice of the form and method they adopt to realize the community objectives within the framework of their internal legal order.

In summary, there are three main legal requirements when processing personal data: (1) prevent excessive usage of personal data. This means that the personal data must be processed in accordance with its intended purpose. None can use or reuse personal data without data owner's consent or beyond its intended purpose. (2) Prevent unauthorised access and usage of personal data. We need to ensure that only authorised user can get access to personal data of individual. (3) Ensure accountability of personal data usage. This means that the data processor must be able to ensure that data owner must have all the information concerning the processing of his data and the information must be available when needed. Data owner must have enough information about who have accessed and processed his data.

The three requirements above are translated to technical requirements and implementation under P5 (see Figure 3). Firstly, in order to prevent the excessive usage of personal data in P5 system, we propose to integrate a module called "Privacy-aware filter" that is able to filter out all the privacy-related information of the objects (e.g. physical person or vehicles) before displaying those objects to guards in control room. This ensures that guards in control room have sufficient information for ensuring the proper security of the protected facility, but not more than necessary. Secondly, to prevent the unauthorised user from accessing personal data, we propose a privacy-aware access control system that is able to control the access to personal data in P5. This systems is not only able to say who can or cannot access to system, but it also provides the access history, which can be used later to track user's activities for ensuring usage accountability of personal data. Thirdly, to ensure the accountability of the personal data usage in P5, we also propose a module called "TTP: Trusted Third Party", TTP is a module allowing users to perform some functionalities that ensure the accountability of personal data usage. TTP module can be installed in the protected facility and managed by internal users or be managed by the external entities.

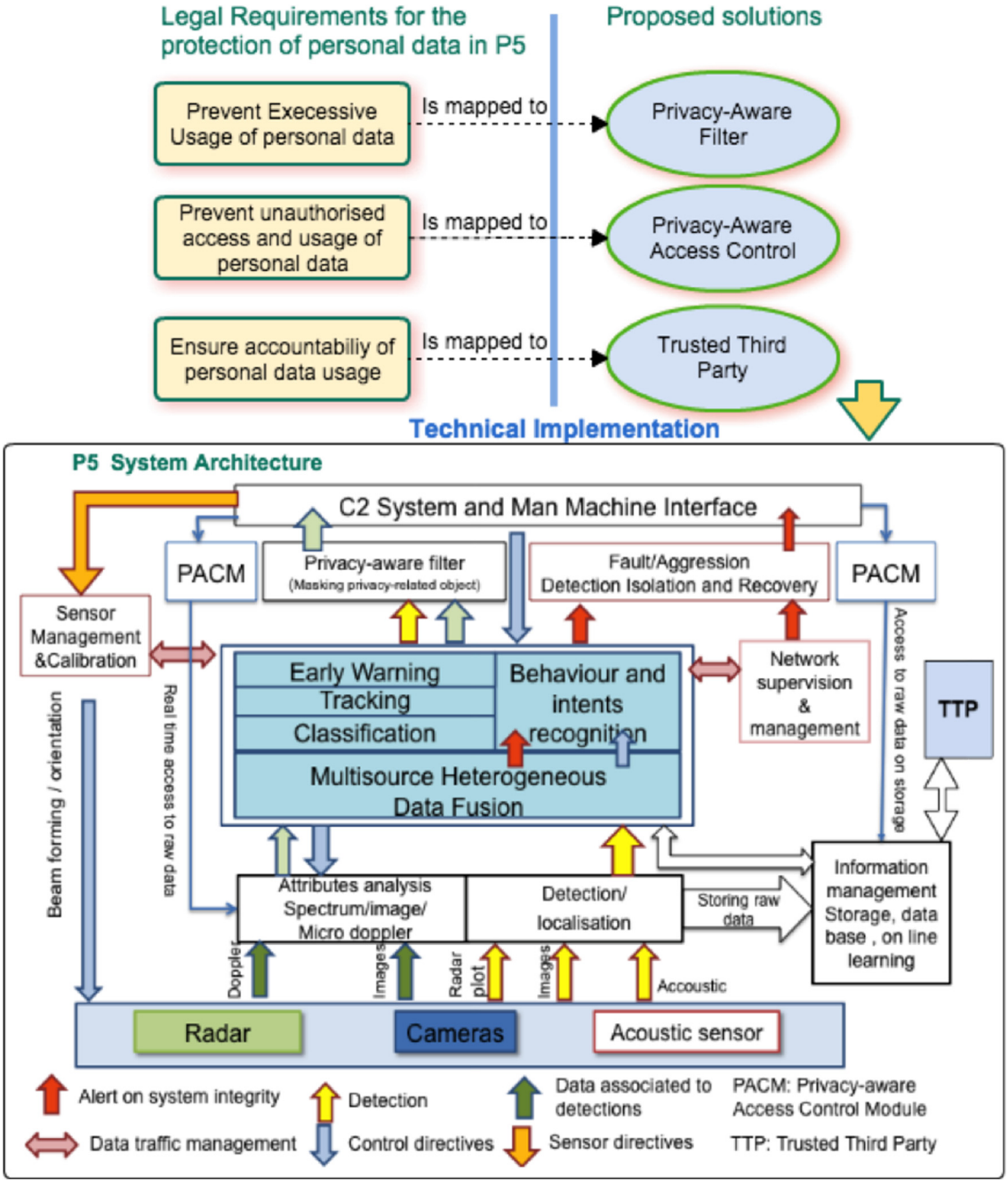


Figure 3. P5's Architecture, from Legal requirements to technical implementation.

Privacy-aware filter

Privacy-aware filter is responsible for hiding all privacy-related information that can be used to identify physical person directly or indirectly. The masking of an object is performed based on the masking policy that is defined to be in accordance with the legal requirements (EU Directive 96/45/EC). The privacy-aware filter is the intermediate interface between sensors and Human/Man Machine Interface (HMI). By default, guards in control room could see only the filtered data. In case of emergency, raw data can be viewed, but with tighter security control like auditing. Privacy-aware filter is designed to respond the legal requirements to prevent the excessive usage of personal data. As presented in Figure 4, Privacy-filter consists of the following modules. Thermal and Visual cameras provides the input data to object classification where the objects are analysed

and classified. The objects identified as vehicles and physical person are then passed further to privacy-filter module for masking. The masking policy is applied at this stage to ensure that only objects bearing personal information are masked. Finally, privacy-aware filter provides filtered data to screen (HMI module) for guards in control room.

Privacy-aware access control

PACM is responsible for controlling access to raw data. This module is responsible also for enforcing access control policies. The access control policies are generally defined by the Trusted Third Party (TTP). The idea of using TTP to define privacy-aware access control policies instead of allowing people in facility to do the job is to avoid the uncontrolled data manipulation by those people. PACM prevents the unauthorised access and also prevents the excessive usage of personal data that is generated from different sensors installed in protected facility. The main concepts of PACM are the use of user's role and purpose to control and enforce the access of personal data. With the proposed model, only an authorised group of user can access to personal data for the limited purposes. Actions performed on data are also limited; this ensures that data is used transparently with proper control. Furthermore, user, accessing data, needs to fulfil some obligations, such as notify to data owner, the obligation functionality allows data owner to keep track on his data processing status, see Figure 5.

Further details about the implementation of privacy-aware filters can be found in section 5 of deliverable D5.2.

Trusted-Third Party (TTP)

TTP is a trusted private or state entity that is responsible for securing the processing of personal data in the protected facility. This module is an important tool for ensuring the accountability of data usage.

TTP module provides to TTP administrator a way to manage access control policies, to manage and to protect the raw as well as filtered data and to audit the access to data. It is worth noting that the whole system is generally installed in the protected facility. However, TTP administrator can remotely control system through secure communication channel, see Figure 6.

Further details about the implementation of privacy-aware access control modules can be found in section 4 of deliverable D5.2.

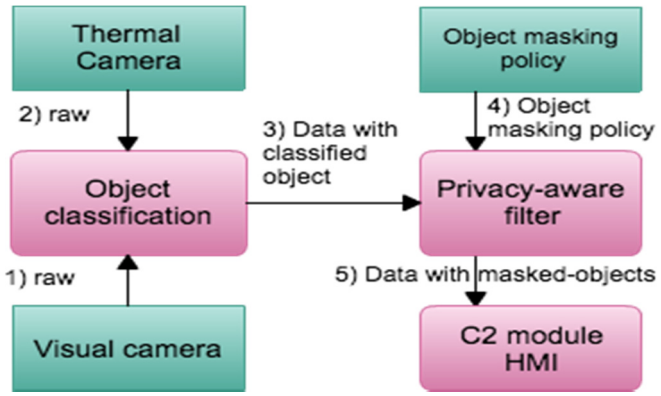


Figure 4: Privacy-aware filter

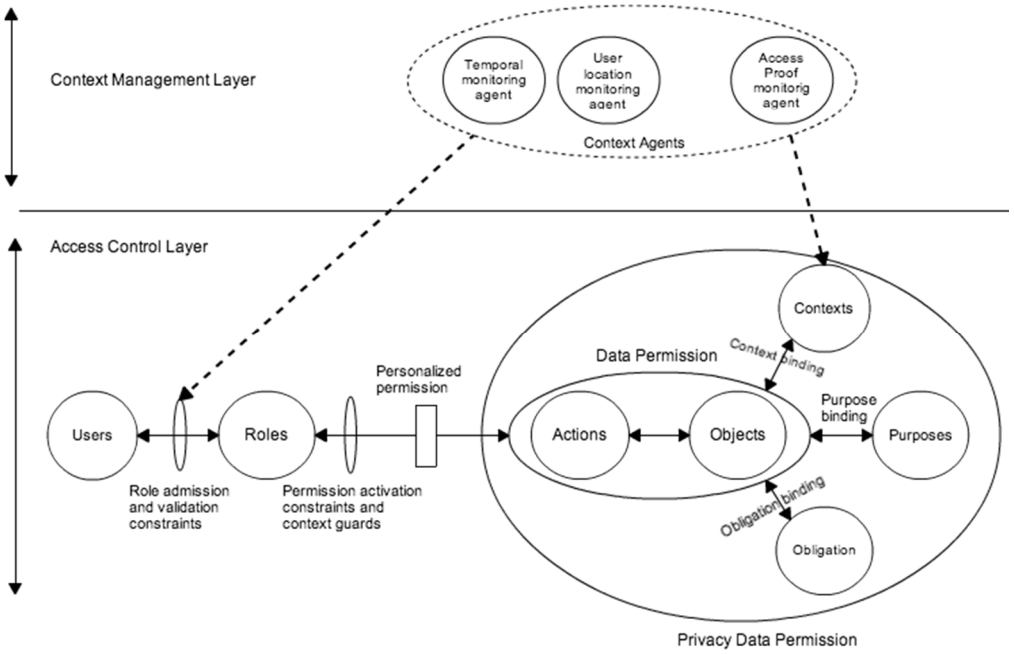
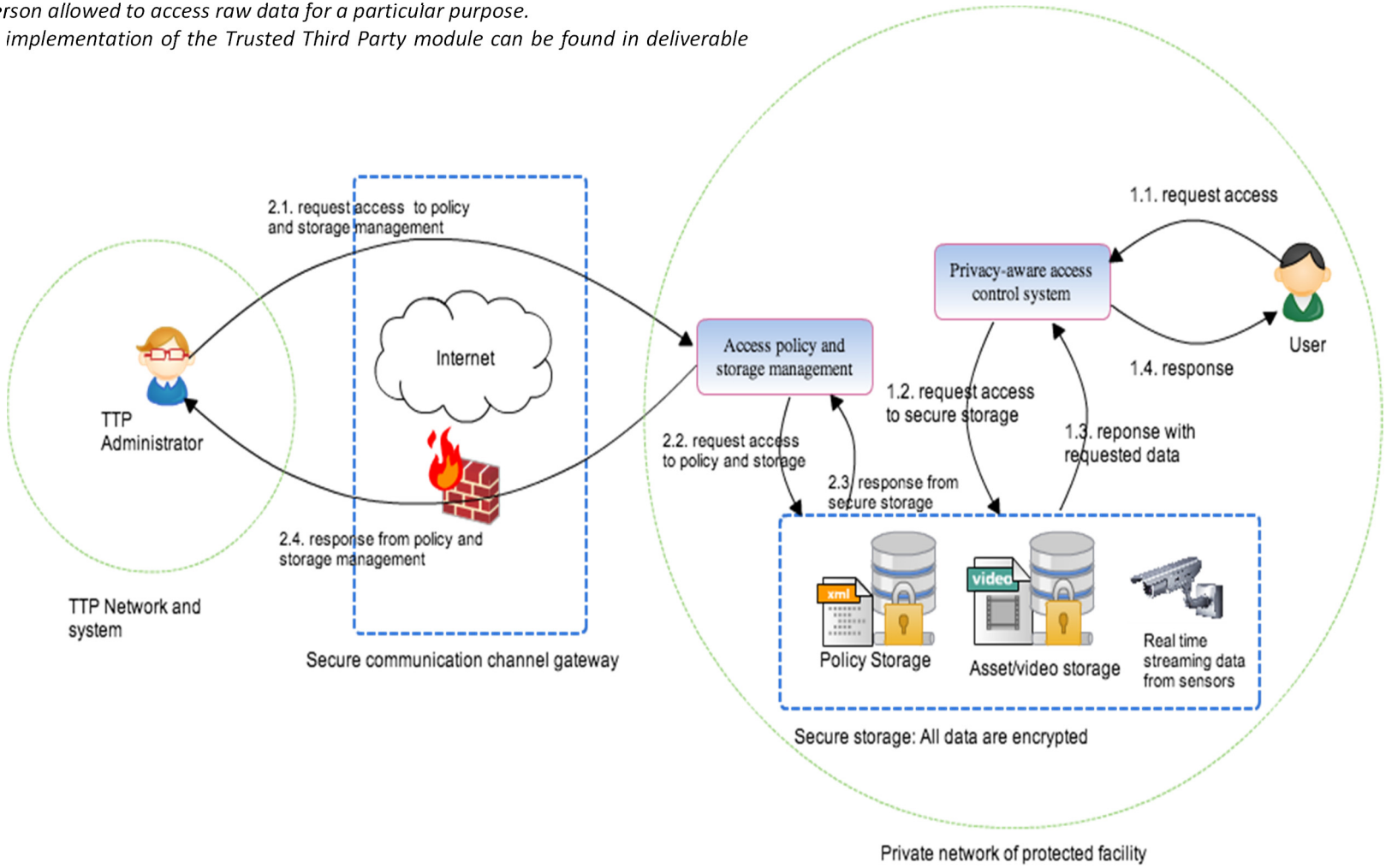


Figure 5. Privacy-aware access control model.

Figure 6. The Trusted Third party concept.

- *TTP administrator can be a trusted private or government entity, which is authorised for the job.*
- *Secure communication channel is a secure communication medium between TTP system and the system installed at the facility.*
- *Access policy and storage management provides some functional features for TTP administrator to manage access control policies and the storage of raw data.*
- *Secure storage is responsible for protecting data in storage (e.g. access control policies and data from sensors).*
- *Privacy-aware access control module is responsible for controlling access to raw data in storage or real- time data from sensors.*
- *User is any physical person allowed to access raw data for a particular purpose.*

Further details about the implementation of the Trusted Third Party module can be found in deliverable D4.2.



5 FAQ & Roadmap

This section contains the results of task 2.5. As a reminder, the task 2.5 is mainly a « documentation task ». Its main objective is to collect and answer Frequently-Asked-Questions about ethics and Technology Assessment. The objective of the task 2.5 is also to elaborate an ethical roadmap and to collect methods and best practices to help other projects to manage the balance between security and privacy.

Before starting, a double warning is necessary. First of all, there is no unique method for managing the balance between privacy and security that could be applicable to all surveillance projects. The reason is that it is impossible to address the privacy issues without considering the context. Following Nissenbaum ("Privacy as contextual integrity", 2004), « in determining privacy threats, one needs to take into account the nature of a situation or context: what is appropriate in one context can be a violation of privacy in another context » (D. Wright 2010 : 200). The choice of a method depends on the context: laws to take into account (EU law, national laws, general and sectoral data protection laws applicable according to the type of system to be deployed, etc.), specific social and ethical questions, etc. There is a multiplicity of methods available. Instead of proposing the best method, a unique method, we propose to present different methods and existing ethical and assessment tools.

Secondly, we must stress that this single task 2.5 may be the object of an entire research project. Many EU projects are dedicated to the "balancing issue" (SAPIENT, PRISMS, etc.). We limit ourselves here to identify major questions to be answered in a project and to orient towards ethical and assessment tools. In a first step (4.1.), we identify questions to be addressed in the course of the development of a surveillance project concerning the security of a Critical Infrastructure. Then, we answered Frequently-Asked-Questions about ethics and technology assessment (4.2.). Thirdly, we provide a list of references relating to assessment tools (4.3), participatory methods (4.4.) and privacy by design (4.5.).

5.1 Legal questions to be addressed in the course of a project

- **Delineation of the legal framework:**
  - What is the critical level of the infrastructure to be protected according to national classification?
  - Have you identified all the relevant security laws (security obligations), general and sectoral, applicable to the area to be protected?
  - Have you identified all relevant privacy and data protection applicable laws, in particular relevant general data protection or specific law (video surveillance)?
  - Are you aware of legal restrictions applicable to the system to be deployed (e.g. avoiding surveillance of private premises)?
  - Have you identified potential other relevant laws to be taken into account (e.g. labour law, administrative law)

- **Design of the system:**
  - Have you carried out an extensive **evaluation of the security needs**?
    - It is important that any surveillance project such as virtual fences rely on an assessment of the security needs at stake in a given context
  - Have you carried out an extensive **privacy and data protection impact assessment** in order to mitigate the risks?

- **Proportionality**
  - Necessity test:
    - Is the system essential to achieve the security objective?
  - Appropriateness, efficiency test:
    - Is the system proposed an appropriate means to achieve the security needs identified?
    - What are the evidences that the system envisaged have produced (in other similar circumstances) or will produce the expected effects?
  - Least-restrictive means test:
    - Is the system proposed the less intrusive solutions (compared to other solutions) to achieve the stated objective?

5.2 Frequently asked questions about ethics and technology assessment

What are the ethical principles that underpin the European Group on Ethics in Science and New Technologies (EGE) recommendations on security and surveillance?

"The core ethical principles that underpin the EGE's recommendations on security and surveillance are the following:

- Privacy and freedom
- Autonomy and responsibility
- Well-Being and/or human flourishing
- Justice

In addition to these basic principles, two procedural principles must be added in order to enable trust between individuals and companies and the state and/ or states:

• Transparency
• Efficacy and proportionality

These principles should be seen as principles that both help to establish security and principles that lead to restraints regarding security and surveillance instruments » (European Group on Ethics in Science and New Technologies, Jim Dratwa (ed.) , « Ethics of Security and Surveillance Technologies », Opinion n° 28, p. 71).

What is « Privacy by design »?

« In the early 1990s, the concept of Privacy by Design (PbD) was developed to address the systemic effects of ICT and networked data systems. The central thesis of PbD is that privacy cannot be protected solely through compliance with regulatory instruments; rather, technologies should be designed with privacy in mind from the outset. Instead of bolting on privacy enhancing features, privacy enhancing tools e.g. minimisation of unnecessary data collection, they should be integrated into systems design » (« Ethics of Security and Surveillance Technologies », Opinion n° 28, p. 32).

The concept of « Privacy by design » has been developed by Ann Cavoukian the Ontario's Information and Privacy Commissioner. The privacy by design approach is defined by the following 7 Foundational Principles:

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***

Cf. Cavoukian, A., *Privacy by design, The 7 Foundational Principles,*
https://www.ipc.on.ca/images/Resources/7foundationalprinciples.pdf

What is « Privacy in design »?

"Privacy in Design is distinct from PbD in that it concerns itself primarily with raising awareness about the processes through which values and norms become embedded in technological architecture. Privacy in design looks at the normativity of structural choices in an effort to promote transparency and protect rights and values of the citizens » (« Ethics of Security and Surveillance Technologies", Opinion n° 28, p. 32).

What is "value sensitive design" ?

"Value Sensitive Design is a theoretically grounded approach to the design of technology that accounts for human values in a principled and comprehensive manner throughout the design process" (Friedman B., Kahn P. H., Borning A., "Value Sensitive Design and Information Systems", in *The Handbook of Information and Computer Ethics,* edited by Kenneth Einar Himma and Herman T. Tavani, 2008).

"Some experts have argued that technology is not neutral with respect to values. Among those that argue in favour of Value Sensitive Design, Flanagan, Howe and Nissenbaum say that the design of technologies bears directly and systematically on the realisation, or suppression, of particular configurations of social, ethical and political

values. They also observe that "the values of members of a design team, event those who have no had a say in top level decisions, often shape a project in significant ways as it moves through the design process. Beliefs and commitments, and ethnic, economic, and disciplinary training and education, may frame their perspectives, preferences, and design tendencies, resulting eventually in features that affects the values embodied in particular system" (Flanagan, M., Howe, D. C., Nissenbaum H., "Embodying Values in Technology : Theory and Practice", in *Information Technology and Moral Philosophy*, J. van den Hoven and J. Weckert (eds.), Cambridge University Press, 2008, 335)" (D. Wright 2010 : 209).

What is « Privacy Impact Assessement »?

"Privacy Impact Assessment has also been suggested as a useful tool for engineers and software developers to help them take into account potential negative consequences of particular elements of a technology design. The FP7 funded PRISE project has recommended that privacy impact assessments should form part of the considerations of funders. This could be a mechanism for ensuring that public money is spent on research which is in line with European values and fundamental human rights" ("Ethics of Security and Surveillance Technologies", Opinion n° 28, p. 32).

What is « ethical impact assessment »?

With the expression "ethical impact assessment", the PRESCIENT project (Deliverable 4, 2013) « refer to an instrument, which is currently usually conceived as a framework for examining the ethical implications of new technologies, which should aim at (a) identifying, and (b) addressing current or emerging ethical issues arising from the development (research and development stage) and deployment (application stage) of new technologies, particularly in the field of ICTs".

What is « virtual fence »?

"Virtual fences" can be defined as a set of interconnected technologies composed of radars, acoustic and thermal sensors, lasers and cameras. Merged together, those technologies allow for permanent and automated monitoring of protected areas, through a system architecture which allow to gather and put together various fluxes of information.

Virtual fences redefine the politics of defence, protection and surveillance. The situation evolves from the one of a line, a drawn, physical line, such as a wall or a fence, to a zone, a perimeter. Virtual fences redefine the very notion of "border", unfolding a particular politics of space that Olivier Razac calls "management of permeability" (2009, 2013).

In this context, the objective is less to control the opening and closing of the space than managing the flow of an open space, « managing its permeability ». It is about managing what Michel Lussault - called « trans-spatiality » that is to say «l'action spécifique qui consiste à franchir» (Lussault, « Transpatialités urbaines », p. 71). Even more than the passage or crossing, the movement itself becomes the object of control and surveillance.

5.3 Assessment tools

European Group on Ethics in Science and New Technologies, Jim Dratwa (ed.), « Ethics of Security and Surveillance Technologies », Opinion n° 28.

Palm E. And Hansson S., "The Case for Ethical Technology Assessment (eTA)", in *Technology Forecasting and Social Change*, 73, 2006, pp. 543-558.

1. In this paper, Palm and Hansson propose a new form of technology assessment that will focus on the ethical implications of new technologies; ethical technology assessment (eTA). This eTA serve as a tool for identifying adverse effects of new technologies at an early stage. eTA can be conducted on the basis of a check-list that refers to nine crucial ethical aspects of technology; (1) Dissemination and use of information, (2) Control, influence and power, (3) Impact on social contact patterns, (4) Privacy, (5) Sustainability, (6) Human reproduction, (7) Gender, minorities and justice, (8) International relations, and (9) Impact on human values.

PIAF project (A **P**rivacy **I**mpact **A**ssessment **F**ramework for data protection and privacy rights), « Deliverable D3: Recommendations for a privacy impact assessment framework for the European Union », 2012,
http://www.vub.ac.be/LSTS/pub/Dehert/506.pdf

> Executive Summary: "This deliverable offers recommendations with regard to policy-making and practice on privacy impact assessments (PIAs). These recommendations are split into two sets. The first set is addressed to policy-makers intending to develop a PIA policy in their jurisdictions or improving existing ones. This part analyses the rationale and methods of introduction of a PIA policy, identifies and describes the constitutive elements of a PIA and discusses the role of data protection authorities (DPAs) in the process of PIA. The second set of recommendations is addressed to the assessors actually carrying out PIAs for whom the guidance on the best practice is offered".

PRESCIENT project (Privacy and emerging fields of science and technology: Towards a common framework for privacy and ethical assessment), « Deliverable 4 : Final Report – A Privacy and Ethical Impact Assessment Framework For Emerging Sciences and Technologies », 2013,
http://observatory%2Drri.info/sites/default/files/obs%2Dtechnology%2Dassessment/PRESCIENT_deliverable_4_final.pdf

> Excerpt from the Executive Summary : "The Prescient project aimed at providing an extended understanding of privacy embracing different approaches and at providing policy-makers and researchers with a *tool* by means of which not only privacy and data protection risks, but also *ethical* issues related to the design, development and use of emerging technologies can be identified and addressed early on. The PRESCIENT framework is modelled along the structure of the recently proposed Privacy Impact Assessment Frameworks (PIAs). The idea is to broaden this model to include also *ethical* issues (Privacy and Ethical Impact Assessment, P+EIA), beyond data protection and privacy aspects".

PRISE project (Privacy enhancing shaping of security research and technology – A participatory approach to develop acceptable and accepted principles for European Security Industries and Policies), "PRISE Concluding Conference Statement Paper",
http://www.prise.oeaw.ac.at/docs/PRISE_Statement_Paper.pdf

> "The PRISE project has developed criteria for performing a privacy impact assessment to be used in the FP7 security technology proposal evaluation and other research funding programmes as (part of the) basis for funding decisions".

SAPIENT project (Supporting fundamental rights, Privacy and Ethics in surveillance Technologies), « Deliverable 4.4.: A guide to surveillance impact assessment: how to identify and prioritize risks arising from surveillance systems", 2014, http://www.sapientproject.eu/D4.4%20%2D%20SIA%20Manual%20%28submitted%2001%20August%202014%29.pdf

> "The SAPIENT project that is expected to provide strategic knowledge on the state of the art of surveillance studies, emerging smart surveillance technologies, and the adequacy of the existing legal framework. In addition to addressing these core research goals, the project will entail the development and validation of scenarios around future smart surveillance systems, and will apply the best elements of existing PIA (privacy impact assessment) methodologies to construct a surveillance related PIA framework" (SAPIENT, Deliverable 4.4., p. 2).

Wadhwa, K., "Privacy Impact Assessment Reports: A Report Card", *info*, Vol. 14 Issue 3, 2012.
http://www.emeraldinsight.com/journals.htm?issn=1463%2D6697&volume=14&issue=3

> Excerpt from the summary: "Privacy impact assessments (PIAs) are an important tool for managing risk in both public and private sector projects. The best evidence of how PIAs are being conducted is the PIA reports published at the conclusion of the process. This paper aims to consider PIA reports from five countries and assesses their strengths, weaknesses and impacts".

Wright, D., "A Framework for the Ethical Impact Assessment of Information Technology", in *Ethics Inf Technol*, 2011, 13:119-226, 2010.

> In this article, David Wright proposes a framework for an ethical impact assessment which can be performed to any policy, service, project or programme involving information technology. The framework is structured on the four principles posited by Beauchamp and Childress. In connection with each of these principles, he proposes a list of question that could raise the ethical issues raised by technologies. For instance:
>
> - Autonomy: "Will the project use a technology to constrain a person or curtail their freedom of movement or association? If so, what is the justification?"
> - Nonmaleficence: "Is there any risk that the technology or project may cause any physical or psychological harm to consumers? If so, what measures can be adopted to avoid or mitigate the risk?"
> - …

Wright, David, and Paul de Hert (eds.), *Privacy Impact Assessment*, Springer, Dordrecht, 2012.

Wright, David, "The state of the art in privacy impact assessment", *Computer Law & Security Review*, Vol. 28, No. 1, February 2012, pp. 54-61.

5.4 Participatory tools

Different participatory methods have been developed for assessing the social acceptability of technologies: consensus conference, focus group, a method of scenario workshop, a method of deliberative polling, etc. As we said in the introduction of this section, there is no best method. The choice of a method depends on different aspects: the objective (identify the stakeholders interests, anticipate future uses of the technology,

examining the ethical implications of new technologies, reach a consensus or show the diversity of opinions, etc.), the budget available, the time available, the fact that the technology assessed is an emerging technology or not, etc. Here follows a list of manuals, reviews and documents which present different participatory methods.

European Participatory Technology Assessment (EUROPTA), *Participatory Methods in Technology Assessment and Technology Decision-Making.* Copenhagen, Denmark: Danish Board of Technology, 2000, http://cordis.europa.eu/docs/publications/7078/70781441%2D6_en.pdf

Health Canada, Corporate Consultation Secretariat, Health Policy and Communications Branch *Health Canada Policy Toolkit for Public Involvement in Decision Making*. Ottawa, Ontario: Minister of Public Works and Government Services Canada, 2000, http://www.hc%2Dsc.gc.ca/ahc%2Dasc/pubs/_public%2Dconsult/2000decision/index%2Deng.php

OCDE, Citizens as Partners: Information, consultation and public participation in policy-making, 2001 .

Slocum, N., *Participatory Methods Toolkit, A practitioner's manual*, joint publication of the King Baudouin Foundation and the Flemish Institute for Science and Technology Assessment (viWTA) in collaboration with the United Nations University – Comparative Regional Integration Studies (UNU/CRIS), 2003, http://archive.unu.edu/hq/library/Collection/PDF_files/CRIS/PMT.pdf

Van Asselt, M., Mellors, J., Rijkens-Klomp, N., Greeuw, S., Molendijk, K., Beers, P. and van Notten P., *Building Blocks for Participation in Integrated Assessment: A review of participatory methods*, Maastricht, International Centre for Integrative Studies, 2001.

5.5 About Privacy by design

Cavoukian, A., *Privacy by design, The 7 Foundational Principles,* https://www.ipc.on.ca/images/resources/7foundationalprinciples.pdf

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

Privacy by design, Strong Privacy Protection - Now, and Well into the Future, A Report on the State of PbD to the 33rd International Conference of Data Protection and Privacy Commissioners, https://www.ipc.on.ca/images/Resources/PbDReport.pdf

6 Conclusions

As mentioned in the Description of Work, the major challenge of the working package 2 “privacy” was to integrate the privacy dimension (based on legal, social and ethical issues) as a design criteria in the P5 technology. In particular, the objectives were to explore the legal, social and ethical issues related to privacy by the P5 system and translate those issues into operational requirements.

The present deliverable discussed the legal impacts of virtual fences from a human rights perspective, including both the right to private life and the right to data protection. In particular, the analysis of the relevant ECHR caselaw allowed us to identify the human rights requirements applicable to the installation of virtual fences in a specific context. Besides, a presentation of the legal framework of data protection applied to the context of video surveillance in EU legislation and some national legislations contributed to illustrate the complexity of the legal framework to be taken into account prior to the deployment of such technology in a specific given context.

In the same time, this deliverable has summarized how core data protection requirements have been taken into account in the design of the P5 technology, following high level principles further translated into operational requirements for system designers: (1) a privacy-aware filter prevents excessive usage of personal data; (2) a privacy-access control module prevents unauthorised access and usage of personal data; (3) a Trusted third party module ensures accountability of personal data usage.

(This marks the end of document D2.2)

(Blank page)

P5 is a European project funded by the EC and coordinated by
The Swedish Defence Research Agency, FOI.
In P5 we aim to improve the security around infrastructures that are critical for the future well-being of the European Citizens.

Coordinator of P5, FOI
Box 1165, SE-58111 Linköping
coordinator@p5.foi.se
www.p5-fp7.eu