SmartPrevent

Collaborative Project

FP7 - 606952

D7.21—Guidelines of ethical issues in video-surveillance systems

Lead Author: [ASED]
With contributions from: [Treelogic]
Reviewer: [QMUL, ALR]

Deliverable nature:	<Report (R)>
Dissemination level: (Confidentiality)	<Public (PU)>
Contractual delivery date:	M6
Actual delivery date:	M14
Version:	2.02
Total number of pages:	48
Keywords:	CCTV, video-surveillance ethics, research ethics

Abstract

Surveillance ethics has been one of the emerging fields of study with important implications for the practice of surveillance systems. Video surveillance technologies have been used by police agencies, security companies, and other public and private institutions and by citizens to increase security measures and to prevent crimes. However, the use of such technology raises serious questions regarding invasion of privacy and violation of rights of citizens. Therefore, adhering to democratic values and privacy rights of citizens requires developing an ethical code of conduct before implementing a video surveillance system.

The principles in this guideline serve as an ethical code of conduct for SmartPrevent and for any other similar video surveillance research project. This document provides an ethical framework, which has been created in line with the EU rules and regulations on privacy and ethics, video surveillance ethics, and research ethics to incorporate rights of citizens, responsibilities of the authority in charge of the surveillance system, ethical principles in surveillance activities and possible pitfalls and proposed solutions in functioning of the system.

Executive summary

Today's advanced technologies are increasingly enabling private and public sector organizations to capture, store, and to process information about individuals and their activities. This situation raises important questions about civil liberties, privacy, and ethical conduct in using such technologies. On the one hand, security issues make many people, particularly state authorities nervous; on the other hand, privacy and civil liberties reject privacy-invasive government policies in excuse for fighting crime. In this connection, SmartPrevent project challenges the notion that freedom and security can be traded in exchange. We consider that public security/safety and individual citizen's civil liberties are complementary values and there is not a zero sum game between the two. European humanitarian principles such as privacy, dignity and freedom, cannot be bartered with security when they come into conflict with each other. Therefore, in SmartPrevent structure, rights will be prioritized rather than traded.

To strike a necessary balance between public security/safety and individual rights, this Ethical Guideline lays down the fundamental principles and European values for fair and ethical use in SmartPrevent surveillance system to prevent crimes, to ensure public safety while respecting rights of citizens and promoting privacy. In this manual, relevant ethical principles are identified and discussed in detail regarding data acquisition and processing stages of the SmartPrevent surveillance system.

This document is composed of four parts: (1) a general introduction to video surveillance technologies and (2) data protection laws in SmartPrevent partner countries, (3) principles of privacy by design, (4) Ethical principles in video surveillance research.

The first section makes a brief discussion of video surveillance technologies, widely known as closed circuit televisions, or simply CCTVs.

The second part makes a systematic survey of the data protection laws in the SmartPrevent partner countries, namely Spain, the UK, Turkey, and Israel. Further, this section also makes a general evaluation of these laws and pays a specific attention to the rights of children in terms of data protection.

The third section is on Privacy by Design approach. In this part, Privacy by Design principles are discussed in terms of how each principle can reduce the likelihood of privacy invasion and increase privacy protection.

The fourth part is the core component of this report. It includes a set of ethical principles for video surveillance research. The purpose of the study, contents of the study, Privacy by Design principles in the general structure, informed consent from participants and public notifications, anonymisation, privacy, rights of children and the ethical review are the issues covered with these rules. Enforcement of industry-standard data protection procedures and the importance of compliance with the national laws and local ethical review boards are also discussed.

Overall, this report provides necessary legal and ethical guidance for researchers on sensitive matters on video surveillance research ethics with clear rules and explanations.

Document Information

IST Project Number	FP7 – 606952	**Acronym**	SmartPrevent
Full Title	Smart Video-Surveillance System to Detect and Prevent Local Crimes in Urban Areas		
Project URL	http://www.SmartPrevent.eu/		
Document URL			
EU Project Officer	Francesco Lorubbio		

Deliverable	**Number**	D7.21	**Title**	Guidelines of Ethical issues in video-surveillance systems
Work Package	**Number**	WP7	**Title**	Dissemination and Exploitation

Date of Delivery	**Contractual**	M6	**Actual**	M14
Status	Version 2.02		final□	
Nature	prototype□ report X demonstrator □ other □			
Dissemination level	Public X restricted □			

Authors (Partner)				
Responsible Author	**Name**	Prof. Osman Dolu, Ph.D.	**E-mail**	osmandolu@yahoo.com
	Partner	ASED	**Phone**	+90-506-272-8658

Abstract (for dissemination)	Surveillance ethics has been one of the emerging fields of study with important implications for the practice of surveillance systems. Video surveillance technologies have been used by police agencies, security companies, and other public and private institutions and by citizens to increase security measures and to prevent crimes. However, the use of such technology raises serious questions regarding invasion of privacy and violation of rights of citizens. Therefore, adhering to democratic values and privacy rights of citizens requires developing an ethical code of conduct before implementing a video surveillance system. The principles in this guideline serve as an ethical code of conduct for SmartPrevent and for any other similar video surveillance research project. This document provides an ethical framework, which has been created in line with the EU rules and regulations on privacy and ethics, video surveillance ethics, and research ethics to incorporate rights of citizens, responsibilities of the authority in charge of the surveillance system, ethical principles in surveillance activities and possible pitfalls and proposed solutions in functioning of the system.
Keywords	CCTV, video-surveillance ethics, research ethics

Version Log			
Issue Date	**Rev. No.**	**Author**	**Change**
29/08/2014	0.0	Osman Dolu	First version of the text to be included in the deliverable
10/09/2014	0.1	Sergio Garcia Alvarez	Format using template of SmartPrevent deliverable
10/09/2014	0.11	Víctor Fernández-Carbajales Cañete	Review of the previous document and inclusion and additional information
11/09/2014	0.12	David Cabañeros Blanco	Review and comments included
21/09/2014	0.13	Osman Dolu	Revised and updated
07/10/2014	1.00	Sergio García Álvarez	new revision including references to Spanish law
08/10/2014	1.10	Shaogang Gong	Review of several sections data store and protection
09/10/2014	1.11	Osman Dolu	Revised and updated
19/10/2014	1.20	Osman Dolu	Final review
25/10/2014	1.21	David Cabañeros Blanco	Technical improvements regarding anonymitation, non-discriminatory practices and false positives
11/11/2014	1.22	Sergio Garcia Alvarez	Contributions discussed in technical meeting. Comments concerning the review with the PO.
12/01/2015	1.30	Osman Dolu	Revised and updated, added references to EU laws and regulations
11/02/2015	1.31	İsmail Dinçer Güneş (External Expert)	Reviewed
12/03/2015	1.32	Sergio García Álvarez	Reviewed. Minor changes
26/03/2015	1.33	Shaogang Gong	Reviewed
07/06/2015	2.01	Osman Dolu	Fully reviewed, new sections added for privacy by design and data protection laws in partner countries, ethical guiding rules are made more explicit and written again, unnecessary legal provisions are deleted, some of them are moved to the footnotes, the text is enhanced significantly by addressing all the comments of PO and external reviewers.
16/07/2015	2.02	Sergio García Álvarez	Review

Table of Contents

Abstract 2
Executive summary 3
Document Information 5
Table of Contents 7
Abbreviations 9
Definitions 10
1 Introduction 11
2 A Brief Introduction To Video Surveillance Technologies 13
2.1 Basics of Video Surveillance Technologies: Closed Circuit Television (CCTV) Systems 13
2.2 Purposes of Using CCTV Systems 13
2.3 Types of CCTV Applications 14
2.4 A Basic Introduction of the SmartPrevent Video Surveillance System 15
3 Protection Laws in SmartPrevent Partner Countries 17
3.1 Data Protection in Spain 17
3.2 Data Protection in the UK 18
3.3 Data Protection in Israel 19
3.4 Data Protection in Turkey 20
3.5 General Evaluation of Data Protection in SmartPrevent Partner Countries 22
3.6 Data Protection and Privacy Rights of Children in Europe 22
3.7 Legal & Ethical Approval of the Local Authorities in the Pilot Test Site 24
4 Privacy by Design in Video Surveillance Systems 25
4.1 Proactive & Preventive, not Reactive or Remedial 26
4.2 Making Privacy the Default Setting 27
4.3 Privacy Embedded into Design 27
4.4 Full Functionality 27
4.5 5. End-to-End Lifecycle Protection 27
4.6 Visibility and Transparency 27
4.7 Respect for User Privacy 28
5 Ethical Principles in Video Surveillance Research in SmartPrevent: 29
5.1 Purpose of the video surveillance system must be scientific research 30
5.2 No audio recordings shall be made along with video recording 31
5.3 Embracing *Privacy by Design* principles in designing new systems, projects, products, and processes. 31
5.4 Always prioritize the privacy and rights of individuals over all other goals and protect the best interest of individuals who are being monitored. 32
5.5 Do not make discrimination or target a particular individual or group, respect different preferences and backgrounds. 32
5.6 Make sure that you obtained fully informed consent from data subjects. 33
5.7 Inform the public about the video surveillance activity. 34
5.8 Respect and protect commercial signs and names of the stores by masking them whenever they are visible. 36
5.9 Make all recorded video files anonymised permanently and irreversibly. Embed anonymisation techniques (auto-masking of faces, de-identification, etc) as part of the default settings for the surveillance system. 36
5.10 Take a special care for the visual data of children and other vulnerable people, such as the blind, handicapped persons, etc. 37
5.11 Be sensitive and responsive towards citizen complaints and information requests. 37
5.12 Establish an Ethical Review Committee to serve as an internal oversight body on ethical issues and make regular monitoring on all stages of data collection and processing, putting special emphasis on matters that have potential for ethical problems. 37
5.13 Comply with the ethical principles of the national & local authorities and obtain ethical approvals from competent authorities. 38

5.14 Enforce the industry-standard data protection procedures and comply with European, national and local data protection rules. 39
6 Approval of the Ethical Review Committee 40
References 41
Annex A Informed Consent Form 45
Annex B Information Sheet 47

Abbreviations

CCTV	**:**	Closed circuit television systems
EU	**:**	European Union
ERC	**:**	SmartPrevent Ethical Review Committee

Definitions

Informed consent is a process for getting permission before conducting a healthcare intervention or research actions on a person. An informed consent in research involves a clear appreciation and understanding of the facts, implications, risks, benefits, and other possible consequences of the research activities.

Anonymisation is the process of changing the format of the data or removing personal information from the data to the extent that remaining data is not sufficient to identify the individual about whom the data was collected.

EuroStat is the statistical office of the European Union situated in Luxembourg. Its task is to provide the European Union with statistics at European level that enable comparisons between countries and regions.

1 Introduction

The Western World has been suffering from high levels of crime and many social problems in the last century. Even though things are getting better, Europe is not an exception to this trend. According to EuroStat, there is a slight declining tendency in the total number of crimes in Europe (Clarke, 2013). However, some crime types are decreasing and some others are on the rise. Statistics on the last 10 years show a relative stability in the number of crimes committed every year in Europe (Harrendorf et al. 2010). At this point, crime prevention, deterring potential criminals, and controlling the raising crime wave becomes a necessity. The use of technology in fighting crime has been the modus operandi in the last several decades. Following revolutionary advances in audio-visual, computing and telecommunication technologies, video surveillance technologies, widely known as CCTVs, have been advanced unprecedentedly. Airports, shopping malls, streets, and virtually any public or private area are kept under surveillance using these technologies. Particularly, for traffic safety, security and crime prevention purposes many places are being watched by police and security organizations. However, striking a fine balance between security and privacy emerges a necessity in using privacy invasive surveillance technologies because justice and security are two pure public goods that every government must provide for its citizens. However, this duty of governments cannot be maintained by invading civil liberties and by investigating the private lives of the citizens.

In this connection, privacy and security seem to be two sentiments at war. However, with the latest trends, such as *Privacy by Design*, we are convinced that it is possible to provide enough security without jeopardizing civil liberties. The SmartPrevent project will be one of the best examples in this field by trying to enhance our security by respecting individuals' privacy. We can avoid the conflict between liberty and safety because we believe that they are not mutually exclusive values. Protection of public not only requires protecting people from crimes but also from the Government.

In principle, there is no need and it is not fair to request citizens to give up their essential freedoms for security because in most cases unnecessary interventions to the freedom of people's private lives do not create a considerable security gain for the public. Further, such measures make people vulnerable to many threats and defenceless against the Government and other authorities. Nobody disagrees that crimes must be fought but it should not be done at the expense of civil liberties. A good European society should always look for a fine balance between social responsibilities and individual rights; between security as a common good and liberty as an individual right. Maintaining this delicate balance is the principle duty of the governments.

In this connection, SmartPrevent project has been developed to increase public safety by protecting privacy. Basically, there are two inherent problems with traditional CCTVs and other similar technologies: (1) compliance with ethical codes, (2) efficiency of human agents to run the system. The first problem has long been a source of concern since CCTV systems are susceptible to misuse and unethical conduct in deploying and running these systems. SmartPrevent minimizes this problem by reducing the need for human agents to actually watch video screens. As for the second problem, even though there is not solid evidence about the limits of attention span of a guard before video screen, it is for sure that human nature has its limits and one

can only watch so many monitors for a limited period of time. At this point, SmartPrevent project has introduced a smart video surveillance system to overcome these limitations. With SmartPrevent's smart algorithm, we will be able to not only reduce the risk of ethical breaches but also increase the efficiency of video surveillance systems. Yet, SmartPrevent is not magic and it should also be subject to certain rules of conduct and ethical principles to guide the operation of the system because there will always be a risk of misuse or unethical conduct in any video surveillance system. To overcome these risks, this document is developed to serve as the ethical guidelines for SmartPrevent and other similar video surveillance research projects.

This document is composed of four parts: (1) a general introduction to video surveillance technologies and (2) data protection laws in SmartPrevent partner countries, (3) principles of privacy by design, (4) Ethical principles in video surveillance research. The first section makes a brief discussion of video surveillance technologies, widely known as closed circuit televisions, or simply CCTVs. The second part makes a systematic survey of the data protection laws in the SmartPrevent partner countries, namely Spain, the UK, Turkey, and Israel. Further, this section also makes a general evaluation of these laws and pays a specific attention to the rights of children in terms of data protection. The third section is on Privacy by Design approach. In this part, Privacy by Design principles are discussed in terms of how each principle can reduce the likelihood of privacy invasion and increase privacy protection. The fourth part is the core component of this report. It includes a set of ethical principles for video surveillance research. The purpose of the study, contents of the study, Privacy by Design principles in the general structure, informed consent from participants and public notifications, anonymisation, privacy, rights of children and the ethical review are the issues covered with these rules. Enforcement of industry-standard data protection procedures and the importance of compliance with the national laws and local ethical review boards are also discussed.

2 A Brief Introduction To Video Surveillance Technologies

2.1 Basics of Video Surveillance Technologies: Closed Circuit Television (CCTV) Systems

Closed circuit television systems (CCTV) form the basics of video surveillance technologies. In a classic television system, audio and video signals released from a central location can be watched by anyone with a compatible receiver. However, in a CCTV system, only a limited number of individuals who are authorized to access and operate the system can reach the streaming and/or recorded content. The system is closed for unauthorized personnel and there are certain rules, procedures and code of practice that governs how the system will operate in compliance with relevant legal and ethical principles.

A basic CCTV system is composed of a camera that captures the images and then transmits them to a monitor via a cable or through a wireless network connection. In advanced versions, the streaming and recorded content can be transmitted to multiple locations for storage and for viewing.

A simple CCTV system is shown in the following diagrams.

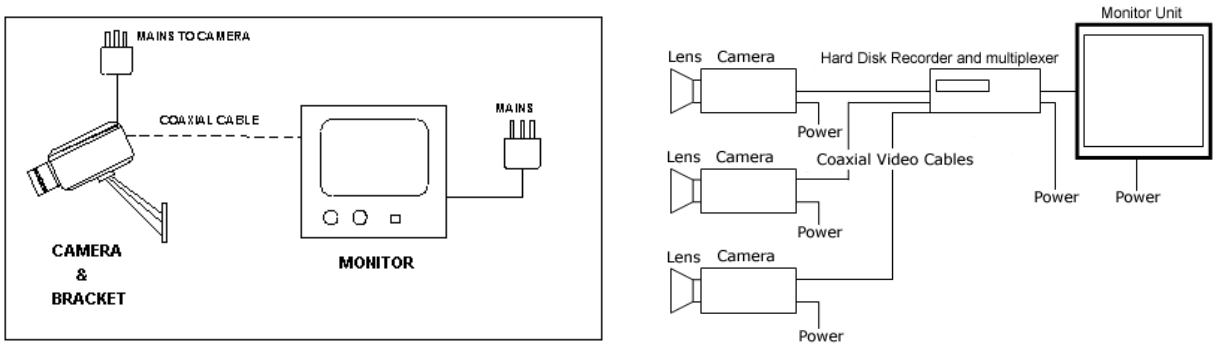

Figure 1: Basic Designs of CCTV Systems

2.2 Purposes of Using CCTV Systems

A CCTV system basically offers extra "eyes" for authorities to keep certain locations under surveillance for crime prevention and many other purposes. We can classify these purposes into eight major categories:

1. **Service-Access Control:** CCTVs are most commonly used to monitor public places such as schools, hospitals, conference halls, shopping malls and stadiums.

2. **Process Control:** CCTV is used in places such as prisons or banks where constant surveillance is needed for security reasons.

3. **Industrial Monitoring:** CCTV is also used to control the working conditions in factories and other production facilities to ensure quality of service and products.

4. **Industrial Protection (work safety):** It has now almost become a requirement to monitor working conditions in mines and other heavy industries to ensure the safety of the workers and to provide rapid response in case of an accident.

5**. Crime Prevention:** Fighting crime is one of the major areas where closed circuit television system is used actively. CCTV has been highly effective in deterring people from committing crimes.

6. **Covert Observations:** Produced in very small sizes, these cameras can record video and audio without being noticed by the subject. These are generally known as hidden cameras and used for intelligence purposes.

7. **Event Log:** CCTV recordings of indoor and outdoor places are often used for evidential purposes when a criminal event happens in the surveillance area.

8. **Traffic Control and City Surveillance:** Controlling and monitoring live traffic is one of the most difficult jobs in modern world. Every passing day controlling roads, bridges, highways and intersections by cameras continue to increase. Urban safety management systems, which are designed for city surveillance, and similar electronic monitoring systems, which are used for traffic control, have evolved into large-scale closed-circuit monitoring systems all around the world.

2.3 Types of CCTV Applications

Considering all purposes of using CCTVs, there are two CCTV applications: (1) overt and (2) covert applications. As the name suggests, the "covert applications" are the hidden cameras and they cannot be easily noticed at first glance.

On the other hand "overt applications" involves using surveillance systems installed in public places and everyone can easily recognize them. These cameras are intentionally made visible as deterrent systems. Technically both applications record what is happening in the surveillance area. In that sense they are not different from each other in terms of what they are doing. However, considering the purpose of use, the "overt applications" seem to outweigh the deterrence factor than the “covert applications”.

Although there are no technical differences between these two applications, the “covert applications” have special legal sanctions. Considering the fact that a CCTV system in itself is a highly problematic technology, deploying such a system in a hidden manner creates additional problems in terms of transparency, accountability, and other legal and ethical concerns regarding civil liberties and privacy. The use of CCTV systems and other video-surveillance technologies have important legal and ethical dimensions. As a highly controversial matter with a potential for abuse, any kind of surveillance application will be subject to legal oversight and approval. In addition to legal regulations, one can argue that overt CCTV systems are governed by established codes of practice and ethical principles whereas using covert CCTVs is a matter of law and court decisions, rather than a matter of ethics.

2.4 A Basic Introduction of the SmartPrevent Video Surveillance System

The increasing crime rates in today's modern societies have been alarm governments to look for alternative solutions tackle this problem. Popularly known as CCTVs, closed circuit television systems are embraced as magical stick to eliminate crime in urban areas. As opposed to the conflicting findings on their crime prevention effect, the number of security cameras has increased exponentially across the globe, particularly in Europe. The SmartPrevent is an ambitious project to help authorities prevent crimes by exploiting the full potential of existing security cameras in urban areas.

The SmartPrevent project aims to enhance detection and prevention of crimes in local urban areas by making full use of video-surveillance systems. The project aims to develop and provide four important benefits: (i) Systematic characterization of usual petty crimes in an area under automatic surveillance; (ii) automatic detection of the most usual and frequent criminal activities; (iii) a set of automated tools capable of alerting the appropriate responders; and (iv) early prevention of crimes by prediction and early detection of crimes.

Rather than providing new methodologies or tools, the SmartPrevent focuses on (a) improving already-existing methodologies by means of a set of guidelines for the use of video-surveillance systems, and (b) providing a set of tools capable to improve of the existing crime detection systems. The project consortium plans to validate the crime detection and prevention capacity of their proposed solution with realistic prototype scenarios as well as with real life examples in a pilot study in Spain.

The SmartPrevent system "silently" observes the surveillance area for suspicious human activity. The system will work to detect the following three types of petty crimes at an early stage: (1) graffiti spraying, (2) antisocial behaviour, and (3) illegal parking and illegal circulation in forbidden areas. At this point, video recordings are made for each criminal scenario to "train" the system about "how each crime/anti-social activity looks like" so that the system would compare "suspicious" activities with the "learned" repertoire of human behaviours/actions.

The following chart is a visual representation of how the system operates:

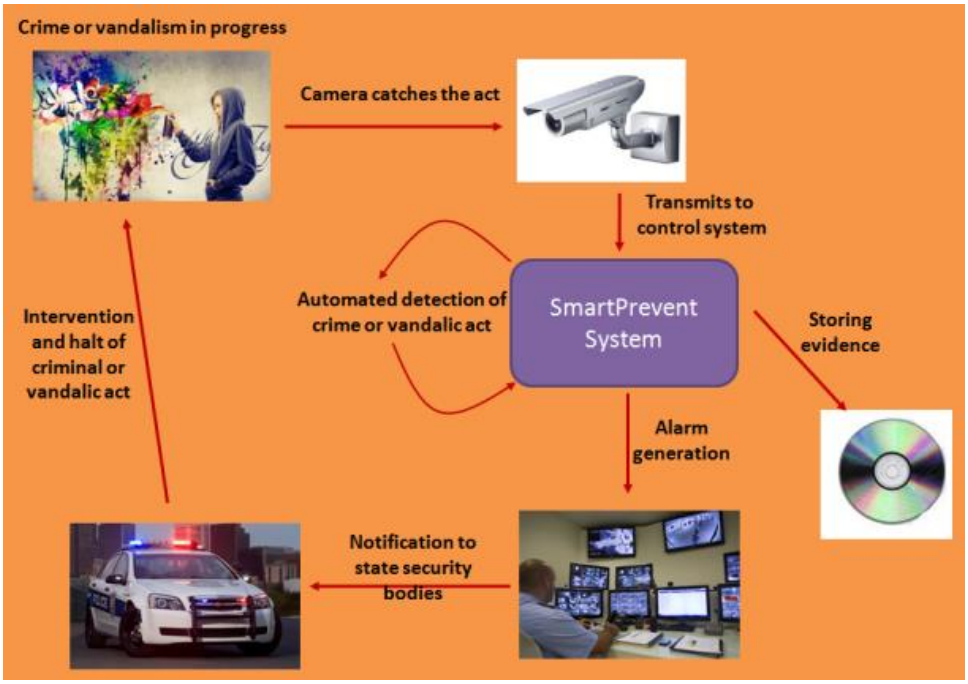

Figure 1. Conceptual example of SmartPrevent system operation

If the system detects a suspicious activity, the human agent will be notified for approval before the system alerts the law enforcement agency. The system will record visual data only if the system detects a "deviation" from the normal.

When the objects being observed are humans, the system will be comparing the human activities at the time of the recording with the sample training videos and the everyday human activities to determine whether the current activities involve any kind of resemblance to the recorded criminal activities or whether these activities diverge dramatically from everyday human activities. Likewise, when the objects under surveillance is non-human objects, for instance cars or waste-bins, the system will compare these objects' locations with similar objects' places in previous recordings to determine whether there is a deviance from the normal. Achieving such an ambitious goal requires collecting and automated processing of vast amounts of image data throughout the pilot test phase.

Writing an ethical guideline is planned to regulate research activities, to prevent unethical conduct, and to provide solutions for controversial matters in SmartPrevent and other similar video surveillance research projects. The << D7.21—Guidelines of ethical issues in video-surveillance systems>> aims to establish the needed ethical principles and rules in video surveillance research. Before presenting these principles, this report will make a systematic evaluation of the data protection laws in SmartPrevent partner countries and the privacy by design approach in video surveillance research.

3 Protection Laws in SmartPrevent Partner Countries

The EU Data Protection Directive and the European Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data are the two chief documents in Europe for the protection of individual data. We have mentioned and referred to specific clauses and provisions from these documents and others up to this point. In this section, we will briefly mention data protection rules in the SmartPrevent partner countries, namely Spain, the UK, Turkey, and Israel and discuss their relevance and implications for a similar project in these countries. At this point, the Article 18 of the EUData Protection Directive asserts that "in order to ensure that individuals are not deprived of the protection to which they are entitled under this Directive, any processing of personal data in the Community must be carried out in accordance with the law of one of the Member States…" It means, the member countries shall not only obey the European regulations but also they are obliged to enact data protection laws compliant with the European principles. Not all partners in the SmartPrevent project are from EU countries but, as the following section shows, almost all countries have enacted laws to include the EU Data Protection Directive and other related European standards on personal data in their national laws.

3.1 Data Protection in Spain

The first country we will consider is Spain. Privacy and protection of personal data is a constitutional right in Spain. The Article 18.4 of the 1978 Spanish Constitution mandates that the state will protect privacy of its citizens, secrecy of communications and personal data with the following clauses:

> *a) The right of honour, personal, and family privacy and identity is guaranteed.*
>
> *b) The home is inviolable. No entry or search may be made without legal authority except with the express consent of the owners or in the case of a flagrantedelicto.*
>
> *c) Secrecy of communications, particularly regarding postal, telegraphic, and telephone communication, is guaranteed, except for infractions by judicial order.*
>
> *d) The law shall limit the use of information, to guarantee personal and family honour, the privacy of citizens, and the full exercise of their rights.*

In 1992, Spain enacted the data protection law known as LORTAD. This law was very much in line with the Directive 95/46/EC on data protection but it underwent a series of amendments to correct some conflicting matters.

In November 1999, Data Protection Directive was formally implemented through the Data Protection Act of 1999 (*Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal*) (LOPD). Generally speaking, LOPD copied many provisions of LORTAD and maintained the legal framework of this law. The Article 1 of LOPD explains the aim of this law as:

> *"…to guarantee and protect the public liberties and fundamental rights of natural persons, and in particular their personal and family privacy, with regard to the processing of personal data."*

The Para 2 of Article 4 of LOPD states that:

"Personal data subjected to processing may not be used for purposes incompatible with those for which they were collected. ***Further processing of the data for historical, statistical or scientific purposes shall not be considered incompatible****."*

In 2007, the Royal Decree 1720/2007 (RLOPD) was accepted in the form of the Data Protection Regulations to enhance the capacity of the Spanish legal system to further enhance the privacy rights of individuals.

In March 2012, a final amendment was made to align RLOPD with new developments in the EU legislation.

Spanish Data Protection Agency (*Agencia Española de Protección de Datos--AEPD*) is the chief institution to implement oversight on the collection, processing, and protection of personal data. The AEPD was founded by the Royal Decree 428/1993 and was amended by Organic Law 15/1999 on the Protection of Personal Data.

The Article 18.4 of the Spanish Constitution of 1978 constitutes the legal foundation of the AEPD: "the law shall restrict the use of informatics in order to protect the honour and the personal and family privacy of Spanish citizens, as well as the full exercise of their rights". For this reason, the Agency has absolute independence from the Public Administration in Spain and it is responsible for enforcement of data protection laws in this country.

In addition to the legal mandates and provisions in the Spanish laws and regulations, the Spanish Data Protection Agency published the "Guide on Video Surveillance" on the 8th of November 2006 to provide technical directions and practical criteria to help citizens and institutions to comply with the current legislation in the country.

3.2 Data Protection in the UK

The United Kingdom is the leading country in Europe in terms of data protection in video surveillance technologies. The Data Protection Act 1998 (DPA) is the main legal document in the UK on the processing of personal data. DPA was enacted after the EU data Protection Directive of 1995 to comply with the European standards on fundamental rights and freedoms in terms of data protection and privacy matters.Basically, DPA is a law that controls how personal information will be used by public and private sector organizations. DPA requires that the authorities must comply with 8 data protection principles.Briefly, all data that is collected and processed must be:

- Used fairly and lawfully
- Used for limited, specifically stated purposes in compliance with the law
- Used in a way that is adequate, relevant and not excessive
- Accurate and up to date.
- Kept for no longer than is absolutely necessary

- Handled according to people's data protection rights
- Kept safe and secure
- Not transferred outside the UK without adequate protection

Further, DPA provides stronger protections for sensitive personal information, such as national/ethnic background, religious beliefs, sexual preferences, health information, political and ideological opinions, and criminal records.

Information Commissioner's Office (ICO) is the data protection agency in the UK. ICO provides control and oversight in data processing and protection matters in this country. Based on legal rules and provisions in DPA and elsewhere, the ICO and the Home Office published a series of guidelines on data protection in video surveillance practices, namely:

- CCTV Code of Practice
- Surveillance Camera Code of Practice
- Privacy Notices Code of Practice
- Data Sharing Code of Practice
- Anonymisation Code of Practice
- Conducting Privacy Impact Assessment Code of Practice
- A Guide to the 12 Principles

We will not go into much detail about the principles and rules mentioned in these guidelines but it would be sufficient to mention that data protection rules in these guides are very detailed and leaves no room for abuse of authority. The limits of liberties and data protection are highlighted with clear statements.

3.3 Data Protection in Israel

Israel is the second non-EU country in the SmartPrevent project. There are several laws and regulations on data protection and privacy matters in this country. The *Basic Law of Israel* is the constitution of this country. Privacy protection in Israel is maintained on the constitutional principle guaranteeing privacy in the *Human Dignity and Liberty* section of the Basic Law with the following statements:

7. Privacy:
a) All persons have the right to privacy and to intimacy.
b) There shall be no entry into the private premises of a person who has not consented thereto.
c) No search shall be conducted on the private premises of a person, nor in the body or personal effects.
d) There shall be no violation of the confidentiality of conversation, or of the writings or records of a person.

The Protection of Privacy Law5741-1981,(PPL) is the chief Israeli legal document that regulates data protection issues in this country. However, PPL is also supplemented with a long list of regulations on more

detailed sub-topics of data protection and privacy. Yoheved Novogroder-Shoshan (2012: 235) lists these documents as follows:

- *Protection of Privacy Regulations (Determination of Databases Containing Non-Disclosable Data) 1987;*
- *Protection of Privacy Regulations (Conditions for Possessing and Protecting Data and Procedures for Transferring Data Between Public Bodies) 1986 (Data Possession Regulations);*
- *Protection of Privacy Regulations (Conditions for Inspection of Data and Procedures for Appeal from a Denial of a Request to Inspect) 1981 (Data Inspection Regulations);*
- *Protection of Privacy Regulations (Fees) 2000;•*
- *Administrative Offences Regulations (Administrative Fine – Protection of*
- *Privacy) 2004;*
- *Protection of Privacy Regulations (Transfer of Information to Databases outside of the State's Boundaries) 2001 (Data Transfer Regulations);•*
- *Protection of Privacy Order (Determination of Public Bodies) 1986;•*
- *Protection of Privacy Order (Determination of the Investigatory Authority) 1998;*
- *Protection of Privacy Order (Establishment of Regulatory Unit) 1999.*

The PPL and Israel' other data protection regulations were deemed as appropriate and adequate in terms of complying with the EU Data Protection Directive, with the European Commission's Decision of 31 January 2011pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data by the State of Israel with regard to automated processing of personal data. This decision states that Israel's data protection laws are sufficient to provide minimum standards for data protection for the purposes of the Data Protection Directive.All being said, there are provisions that creates exemptions for scientific research in data protection regulations in this country. A general overview of the Israeli data protection laws can be read from a guide entitled "*A Guide to Data Protection in Israel*" by Ian Bourne (2010), Head of Data Protection Projects, Information Commissioner's Office, UK.

3.4 Data Protection in Turkey

Turkey is one of the non-EU member countries in the SmartPrevent project. However, as an EU candidate, Turkey is working for changing the existing laws and making new ones to abide by the European standards in its legislations.

Turkey does not have an independent data protection law. Even though a draft law was prepared in 2004, it was not brought to the Parliament because of political reasons. Turkish Constitution is the main legal document that encompasses the foundational principles on data protection. There are several Articles in the Constitution which reflects the basic human rights regarding freedoms and privacy.

For example, the Article 20 is on the respect for private life:

"Everyone has the right to demand respect for his private and family life. Privacy of individual and family life cannot be violated.

...Neither the person, nor the private papers, nor belongings of an individual shall be searched nor shall they be seized.

Everyone has the right to demand the protection of his personal data. This right comprises the right to be informed about the personal data concerning himself, access to such data, right to request correction or deletion of them as well as the right to be informed if such data is used in accordance with the purposes for which it was collected. Personal data can be processes only in cases regulated in a law and upon express consent of the subject individual. Principles and procedures regarding the protection of personal data shall be regulated by a law."

The Article 21 is on the secrecy of private life at home:

"*The domicile of an individual shall not be violated*" and "*…no domicile may be entered or searched or the property seized therein*."

The Article 22 is on *freedom of communication:*

"Everyone has the freedom of communication. Privacy of communication is fundamental. ... Communication shall not be impeded nor its secrecy be violated."

At the end of each one of these provisions above, however, the Constitution mentions court orders and the decisions of a competent agency authorized by law can interrupt these rights, and such actions of the agency will be subject to the approval of a judge within 24 hours, otherwise seizure shall automatically be lifted.

In addition to the Constitution, there are a couple of provisions and partial regulations on personal data in other laws, such as the Civil Code, Criminal Code, Labour Law, Banking Law, **Bank Cards and Credit Cards Law,** Medical Deontology Bylaw and Patient Rights Regulation. Turkish Civil Code basically offers citizens the means for asking for compensation in the court of law for their loss in case of an unauthorized use of their personal data, the Criminal Code includes provisions on the punishments for those who invade private life of others and use personal data of people without legal authority (Ergün, 2011). All other laws, bylaws, and regulation basically discusses the limits of using personal data of the workers by their employers, of the clients by the banking authorities, of the patients by doctors and medical authorities. The existence of these laws, however, does not provide appropriate protection of personal data in Turkey because their scope and content are limited and not sufficient to secure data protection in Turkey. ***Unfortunately, there is not any legal rule or an agency for the regulation of video surveillance practices in the country***. A Draft *Law Concerning Protection of Personal Data* was prepared by the Turkish Ministry of Justice to adapt the European laws into Turkish legislation but it has been left in the dark for the last ten years and it is not enacted yet. This draft law was basically a Turkish version of the EU Data Protection Directive. However, the political authority did not

want to get itself restrained by the tight regulations in this law. As a result, Turkey does not have a Data Protection Law and there is not a competent authority in this country to serve as a Data Protection Agency.

3.5 General Evaluation of Data Protection in SmartPrevent Partner Countries

All partners' countries, except for Turkey, in SmartPrevent project have established legal rules for regulation of video surveillance technologies. Even though it is not an EU member state, Israel's data protection laws and regulations are approved by the European Commission in 2012 as being compliant with the EU Data Protection Directive 1995. Therefore, maintaining compliance with the EU Data Protection Directive will produce a law-abiding system in all partner countries. Turkey, unfortunately, does not have a special law for data protection. There are some constitutional guarantees and several articles in a list of laws provides limited coverage for data protection in this country. However, there is not a dedicated regulation on video surveillance practices in Turkey. The proposed Data Protection Law would incorporate EU Data Protection Directive into Turkish laws but it is still waiting to be enacted by the Parliament.

3.6 Data Protection and Privacy Rights of Children in Europe

Rights of children have a very well established foundation in the international documents and European regulations. United Nations Convention on the Rights of the Child is the chief document on rights of children. The Article 16 of the UN Convention is on the child's right to privacy:

> *"1. No child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation.*
>
> *2. The child has the right to the protection of the law against such interference or attacks".*

European Union (2000) recognizes the rights of children in the in Article 24 of the European Charter of Fundamental Rights. The paragraph 2 of this article stresses that:

> "*In all actions relating to children, whether taken by public authorities or private institutions, the child's best interests must be a primary consideration*"

In a communication document entitled "Towards an EU strategy on the Rights of the Child", Commission of the European Communities (2006) mentions "*children's rights as a priority for the EU*". The Commission also puts a special emphasis on this matter in its Communication on Strategic Objectives 2005-2009 with the following phase:

> *"A particular priority must be effective protection of the rights of children, both against economic exploitation and all forms of abuse, with the Union acting as a beacon to the rest of the world".*

Along with the same lines, the Group of Commissioners on Fundamental Rights, Non-discrimination and Equal Opportunities "*decided in April 2005 to launch a specific initiative to advance the promotion,*

protection and fulfilment of children's rights in the internal and external policies of the EU" (Commission of the European Communities, 2006).

The Data Protection Working Party, which was established based on the Article 29 of Directive 95/46/EC, is an independent European advisory body on data protection and privacy. This Working Party prepared a special opinion document on the protection of children's personal data entitled "General Guidelines and the special case of schools". This document prioritizes the protection of the best interest of the child in all situations. The opinion discusses situations which involve a conflict between the best interest of the child and the child's right to privacy and his data protection rights. In any case, the Working Party concludes, the best interest of the child should be preferred over all other rights of the children. Medical matters and issues related to social work are given as examples of such situations. However, this statement should not be misunderstood as children have no privacy rights or the existing data protection rules do not apply to them. Instead, this approach should be properly interpreted as protection of children in all situations.

Rights of children are not limited to those we have discussed so far but these are the leading statements on the privacy rights of children.

Children's data protection and privacy rights are in fact no different than those of adults. In this vein, Seamus Carroll (2014), the chair of CAHDATA (*Council of Europe, Ad Hoc Committee on Data Protection*) asserts that:

> *"Children, like adults, are holders of data protection rights under the Council of Europe's Data Protection Convention ("Convention 108"). They may not, however, depending on their age and their level of maturity and understanding, have the capacity independently to exercise these rights. Children's lack of capacity to exercise Convention 108 rights should not be misunderstood as an absence of such rights".*

Therefore, one should assume at least the same level of sensitivity towards the privacy and data protection rights of children with adults, if not more. In a video surveillance research, all researchers should take extreme caution regarding the privacy rights of children and hold the best interest of the children above all other interest at all times.

Data protection and privacy rights of children are mentioned in all of SmartPrevent partners' laws, except for Turkey. Since Turkey does not have a data protection law, more specific issues like data protection for children are not regulated. However, other partner countries (the UK, Spain, and Israel) have adequate legal safeguards. In fact, data protection laws in these countries apply to people of all ages, not only those 18 and older. However, data protection agencies provide additional guidance for vulnerable groups, mainly for children. These regulations basically advise making sure that the child in question gives her consent and understands the meaning and consequences of her agreement. For example, the United Kingdom's Information Commissioner states that

> *"…children who are old enough to understand what is being asked of them should be given the opportunity to give their own consent with regard to Data Protection issues. ... Although no guidance has been given as to how to establish that a child understands what is being asked of them, … once a child becomes 12 years of age that he or she is likely to be able to understand the implications of what is being asked. This is commonly referred to as the "Gillick Principle".* (Belfast Education and Library Board, 2007:2).

3.7 Legal & Ethical Approval of the Local Authorities in the Pilot Test Site

Compliance with the European, national, and local laws is a legal requirement for any video surveillance system. However, it is not the only condition for setting up such systems because the Article 8 of CFREU states that "*Compliance with these rules shall be subject to control by an independent authority*" in member countries. Since the pilot test site for SmartPrevent project is the ALR Municipality of the Madrid, Spain, the SmartPrevent consortium needs to obtain permission from legal authorities and ethical approval of relevant institutions.

Spanish Data Protection Agency is the chief authority in Spain to implement and oversight data protection matters. To comply with the Spanish Legislation to protect the citizens' rights and the SmartPrevent consortium applied for necessary permissions from the Spanish Data Protection Agency and from Delegation of Madrid Government and the letters to these institutions are presented in Annex 1 & 2 of D2.21 "Data acquisition and ethical review" . These legal permissions and ethical approvals will guarantee the legal & ethical compliance of the Project's data collection, processing and management practices. These institutions made a careful review of the entire Project to clarify the legitimacy of the actions to be taken in the SmartPrevent surveillance system. These approvals were important to make sure that the Project Consortium abides by the Spanish legislation such as the Article 104 of Spanish Constitution and the Organic Laws made based on the Article 81.1 of the Spanish Constitution.

4 Privacy by Design in Video Surveillance Systems

Privacy by Design a well-known approach for establishing high standards for privacy in data collection and processing systems. Privacy by Design as a concept was developed in the early 90's as a solution to privacy invasive technologies, particularly after the unprecedented advancements on the computing, telecommunications, and video processing technologies. Privacy by Design asserts that privacy cannot be secured solely by compliance with regulatory frameworks because laws can be violated and rules can be broken. In the beginning, Privacy-Enhancing Technologies (PETs) was seen as the solution but then it was realized that a more substantial approach is required to provide real safeguards against privacy invasive technologies. Privacy by Design requires that privacy assurance must ideally become an organization modus operandi.

Privacy by Design is one of the most important priorities that any authority planning to collect visual data of real persons should consider before establishing the surveillance system. In addition to the legal mandates and rules, there is a special duty for the data controllers to make any effort to guarantee a privacy compliant system. Therefore, the Privacy by Design approach is necessary in installing preventive measures in the initial design of such systems (Cavoukian, 2012), then employing privacy enhancing technologies (Cavoukian, 2008:12-14), and finally adopting institutional safeguards to reduce and stop the abuse of these systems. Principles of Privacy by Design may be applied to all types of personal information. However, as a rule, the strength of privacy protection requirements tends to be commensurate with the sensitivity of the data.

Privacy by Design has been adopted as a new standard in surveillance technologies and it has been adopted by the EU (2010) in the *EDPS Video Surveillance Guidelines*. This guideline stresses the importance of this approach with the following sentence: "Data protection and privacy safeguards should be built into the design specifications of the technology that the institutions use as well as into their organizational practices" (p.10).

The Recital 30 of the "Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions: A comprehensive approach on personal data protection in the European Union" points out the importance of privacy enhancing technologies and describes the principle of 'Privacy by Design' with the following statement: "*privacy and data protection are embedded throughout the entire life cycle of technologies, from the early design stage to their deployment, use and ultimate disposal*."

Privacy by Design is composed of a constellation of principles to ensure privacy to help individuals gain control over their personal information by providing guidance for organizations in building safeguards for individual rights in the beginning of establishing such systems. In fact, it is an approach that prioritizes the privacy rights and well-being of the research subjects over all other interests and goals.

Benefits of adopting a *Privacy by Design* approach are priceless in many ways and it is a valuable tool for building trust and minimizing privacy risks. Having privacy in mind in the beginning of designing

new systems, projects, products, and processes can help organizations (1) to identify potential problems at an early stage and address them in due time and for less cost, (2) to increase privacy awareness and alert them for the importance of data protection, (3) to meet legal obligations and to avoid making mistakes that would breach data protection rules, (4) to decrease the likelihood of privacy invasive actions and to minimize negative consequences for individuals (United Kingdom Information Commissioner's Office, 2015:128).

There are seven foundational principles of Privacy by Design: (1) being proactive and preventive, (2) privacy is set as the default setting, (3) privacy is embedded into the design of the system (4) seeking to accommodate all legitimate interests, being positive-sum, not zero-sum, (5) providing full lifecycle protection for the data, from beginning to the end, (6) visibility and transparency, being open for independent verification, (7) respect for user privacy (Canada Information and Privacy Commissioner, 2015).

Privacy by Design encompasses applications in three areas, namely IT systems, accountable business practices, and physical design and infrastructure. However, the application areas continue to grow. Dr. Ann Cavoukian is the chief name behind the Privacy by Design approach and we will explain these principles in the lights of the work of Dr. Cavoukian (2008, 2011, and 2012).

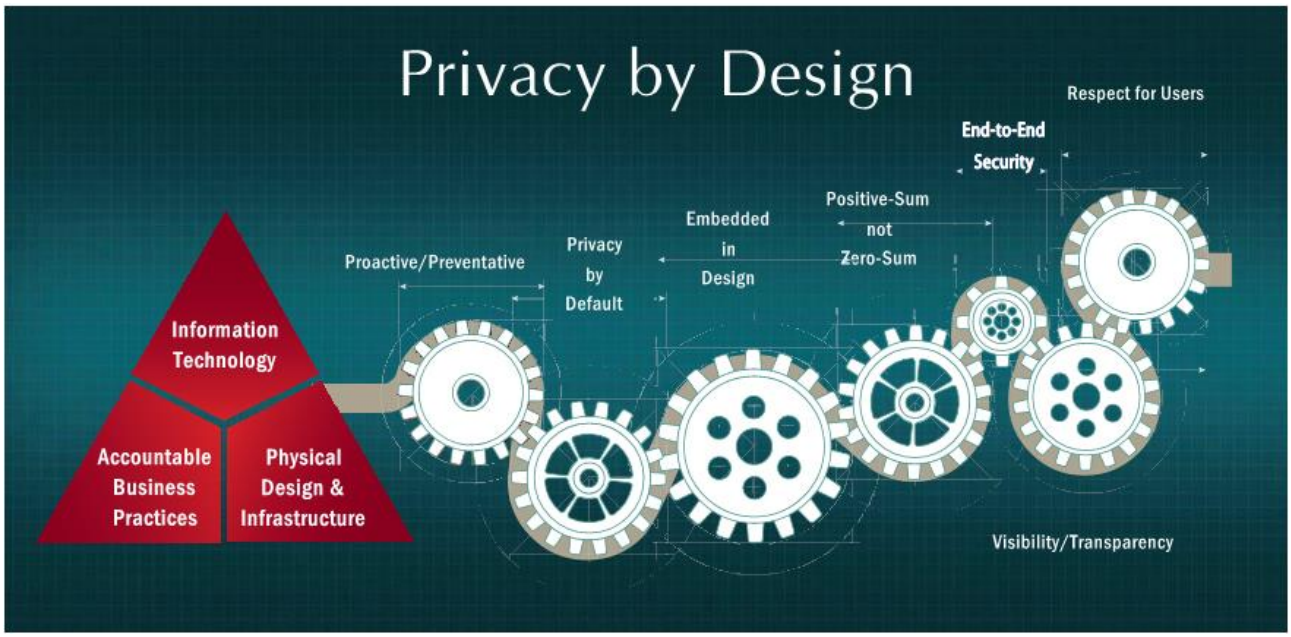

Figure 1: Privacy by Design (Source: Privacy by Design: Time to Take Control, p.16)

4.1 Proactive & Preventive, not Reactive or Remedial

Privacy by Design approach anticipates threats to privacy in any scenario before they happen. For this reason, it is a proactive approach rather than being a reactive one. Instead of waiting for emerging threats to

cause harm to our privacy or looking for some band-aid solutions for privacy infractions afterwards, Privacy by Design aims to foresee and then prevent those risks before they happen.

4.2 Making Privacy the Default Setting

Privacy by Design aims to make privacy as the default setting in any information system. Taking privacy of individuals as the lead priority, Privacy by Design acts proactively and influences the rule-making process to make privacy as the default setting for information systems and organizations. When institutional rules are made to reflect a preference for the privacy of individuals over all other priorities, the built-in privacy safeguards will be sufficient to protect individuals from negative influences even if individuals do nothing.

4.3 Privacy Embedded into Design

Privacy by Design requires taking a before-the-fact approach, not after-the-fact. Therefore, privacy needs to be integrated in the IT systems and organizational systems, by embedding the privacy at the core of the main architecture. It is not attached to the system as an additional module, as an add-on, something peripheral, but made as an integral part of the system. This strategy places privacy at the centre of the system, makes it an essential component of the system.

4.4 Full Functionality

Privacy by Design is a "win-win" approach. It aims to give voice to all parties and accommodate their demands and interests of different parties in a "positive-sum" manner. There is no need to make mutually exclusive choices between privacy and any other priority. Such zero-sum approaches force people to choose between false dichotomies. Privacy by Design, however, makes it possible to accommodate their interests in the same melting pot and helps everybody win, without making unnecessary sacrifices.

4.5 5. End-to-End Lifecycle Protection

Making privacy the default setting and embedding privacy at the core of the system in the first place, Privacy by Design provides an end-to-end protection for personal data, from the very beginning till the end. Such a holistic protection approach provides highest possible security for sensitive data. Data is used as long as it is necessary and it is destroyed irreversibly at the end of the process. Privacy by Design provides a total data management strategy which encompasses end-to-end protection for privacy of individuals.

4.6 Visibility and Transparency

Transparency is a key element for accountability, particularly in Privacy by Design approach. It is easier to maintain the integrity of the privacy-respecting system and hold everybody and every partner involved in using the technology accountable. Establishing a transparent system guarantees all stakeholders to abide by the stated principles and objectives in operating the system. Further, transparency of the system makes the

system's component parts visible to all parties and allows independent verification of the promises made in the beginning. Trust is necessary, but transparency and verification are even vital.

4.7 Respect for User Privacy

In addition to all the principles above, Privacy by Design necessitates the system operators to offer users strong privacy settings by default, to notify them in advance and appropriately about new policies and changes in those policies, and to encourage developing user-friendly alternatives and options for everybody. All these are contained in this approach to empower the individuals and keep their interests as the first priority in developing all data systems. Privacy by Design is not only interested in boosting privacy sensitive technologies but also making them accessible and user-centric for all people.

5 Ethical Principles in Video Surveillance Research in SmartPrevent:

In this part of the report, the ethical principles in operating the SmartPrevent and any other video surveillance research projects will be discussed. The SmartPrevent surveillance system will function according to the professional, ethical and legal provisions and regulations in Europe and in the partner countries, particularly in countries where the pilot testing will be made. In principle, an impact analysis should be performed on ethical & privacy issues, environmental concerns, and proportionality of the application before installing any CCTV system. To avoid any legal or ethical violations, the decision as to whether to use the CCTV system or not should be made before performing these evaluations.

Basically, these type of research aims to to enhance the security of Europeans and safety of communities but it should be done without forcing individuals to make a choice between their freedoms and security. We believe that we cannot have security or civil liberties in their true sense if we do not promote both values at the same time. Liberty without security is fantasy; security without liberty is tyranny. Therefore, benefitting from established ethical values and principles on video surveillance and research ethics, this guideline introduces the ethical principles that will govern SmartPrevent and any similar video surveillance research:

1. Purpose of the video surveillance system must be purely scientific research, which has appropriate ethical approvals from competent authorities. Data must be processed for limited purposes and not in any manner incompatible with those purposes. No hidden agendas, no dual uses.
2. No audio recordings will be made to accompany visual data.
3. Embracing Privacy by Design principles in designing new systems, projects, products, and processes.
4. Always prioritize the privacy and rights of individuals over all other goals and protect the best interest of individuals who are being monitored.
5. Do not make discrimination in targeting a particular group or individual. Respect preferences and differences, such as age, sex, race, political or religious preferences.
6. Make sure that you obtained fully informed consent from data subjects.
7. Do not fail to inform the public about the video surveillance activity. Post/put notification signs on visible places in the surveillance area (i.e., walls, polls, etc).
8. Respect and protect brand names/trade marks and names of the stores by masking their names and special signs whenever visible.
9. Make sure that all recorded video files are anonymised permanently and irreversibly. Embed anonymisation techniques (auto-masking of faces, de-identification, etc) as part of the default settings for the surveillance system.
10. Take a special care for the visual data of children and other vulnerable people, such as the blind, handicapped persons, etc.

11. Be sensitive and responsive towards citizen complaints and information requests.

12. Establish an Ethical Review Committee to serve as an internal oversight body on ethical issues and make regular monitoring on all stages of data collection and processing, putting special emphasis on matters that have potential for ethical problems.

13. Comply with the ethical principles of the national & local authorities and obtain ethical approvals from competent authorities.

14. Enforce the industry-standard data protection procedures and comply with European, international, national and local data protection laws.

In the following section, detailed explanations are provided regarding the definition, scope, content, and extend of one of these principles.

5.1 Purpose of the video surveillance system must be scientific research

Purpose of the video surveillance system shall be purely scientific research, which has appropriate ethical approvals from competent authorities. Data shall be processed for limited purposes and not in any manner incompatible with those purposes. The authority in charge of the video surveillance system must not allow anybody to exercise any hidden agendas. Strict policies should be put in place to prevent diversion from predetermined purposes. Further, dual uses of visual data shall not be allowed. Video surveillance research is allowed by the EU Data Protection Directive and by national laws of the SmartPrevent project partners basically mimics the provisions in this document[1].

1. The purpose of the SmartPrevent video surveillance research is to help legal authorities (i.e., police and other security agencies) to prevent crimes and to catch criminals by early detection of criminal activities, and to demonstrate the possibility of software-based monitoring of public spaces to detect criminal and antisocial activities.
2. The image data obtained from the surveillance research shall only be used in testing the smart software to detect crime at an early stage.
3. No part of the actual visual data shall be shared with the public, with the media or will be published on Internet for financial gain, for recreational purposes, or for any other purposes.

[1]As the Article 16 of 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" maintains, processing of sound and image data for public security, defense, national security purposes and for activities which fall into the realm of criminal are exempt from this directive. However, with the Article 34 of this Directive, when such actions are realized for scientific research and government statistics, Member States should "provide specific and suitable safeguards so as to protect the fundamental rights and the privacy of individuals". The Article 18 of the Directive also asserts that "in order to ensure that individuals are not deprived of the protection to which they are entitled under this Directive, any processing of personal data in the Community must be carried out in accordance with the law of one of the Member States…"

4. Anonymised image data and other data produced with informed consent from the participants, however, can be used for dissemination activities, in academic publications and in other research & development activities by the researchers and project partners.

5.2 No audio recordings shall be made along with video recording

CCTV cameras often transmit only images. However, sometimes these systems are also equipped with microphones and capable of recording audio data in the surveillance area.

In video surveillance research, no audio recordings shall be made along with visual data. Because audio data adds an important risk dimensions to video surveillance, it is a serious threat to privacy of individuals. Therefore, no audio recording shall be allowed. To prevent this from happening, only devices with image recording capabilities will be used.

5.3 Embracing *Privacy by Design* principles in designing new systems, projects, products, and processes.

All systems, technological infrastructure and organization of the entire research project should embrace privacy by design principles in video surveillance research. Following the principles of the Privacy by Design, a video surveillance research system shall be proactive in sensing privacy risks to participants and data subjects. Therefore, built-in privacy safeguards shall be embedded into the core of the system and privacy shall be made the default setting as a rule and possible integration of current achievements in privacy-sensitive surveillance shall be considered. A full lifecycle protection for the data subjects, from beginning to the end, should be guaranteed by using anonymising the data, permanently and irreversibly. An Ethical Review Committee shall act as an internal oversight body on ethical issues throughout the research to ensure the anonymity of the data and privacy compliance of the research.

Therefore, the surveillance system shall be designed to respect privacy and it will prioritize individual rights over all other goals. In this respect:

1. No camera shall target private lives of individuals, in private settings or in public space. Windows or balconies of houses and hotel rooms are examples for private setting. If it is unavoidable, all private settings will be marked with a special algorithm and blackened permanently and irreversibly so that no intrusion into private lives will be allowed.
   "Privacy in public" is a tricky concept but privacy of individuals must be respected in public settings as well. No camera shall zoom in on any persons or track them. People shall be let alone, no special attention shall be directed at any person in the surveillance area.
2. All the names of the stores and shops shall also be blackened permanently and irreversibly to protect the best interest of the owners of these places from any negative impact.
3. All recorded data shall be anonymised using industry-standard algorithms and this process shall be permanent and irreversible.

5.4 Always prioritize the privacy and rights of individuals over all other goals and protect the best interest of individuals who are being monitored.

Under the Common Law and in international documents, the right of privacy[2] is described as the right of people to lead their lives in a manner that is reasonably secluded from public scrutiny, whether such scrutiny comes from a neighbour's prying eyes, an investigator's eavesdropping ears, or a news photographer's intrusive camera. Any CCTV system must take serious cautions in order not to breach any individual rights and European and national rules and regulations when such systems are designed, deployed, and implemented. At this point, perhaps the most important of the rights that these systems should respect is the privacy rights of individuals.

Prioritising privacy and rights of individuals over all other interests and goals shall be the default setting for video surveillance research projects. Particularly the right to private life shall be promoted in such research endeavours. Therefore:

1. Whenever researchers have to make a choice between the individuals and the research, they should always choose the individuals and their rights as the first choice.
2. No research objectives can be used as an excuse for violating the data subjects' rights and their privacy. Particularly in video surveillance research, the operator shall be very careful in not jeopardising privacy and other rights of individuals.
3. If the researcher or the operator encounters an ethical dilemma or a difficult situation, they shall bring this issue to the attention of the Ethical Review Committee immediately and proceed with the Committee's directions.

5.5 Do not make discrimination or target a particular individual or group, respect different preferences and backgrounds.

European regulations prohibit processing of special categories of data[3]. Therefore, video surveillance systems shall not be used to target any person or group of individuals based on their features such as age, sex,

[2] The Article 8 of the European Convention on Human Rights explains what is the right to private life:

> *(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 wellbeing 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.*

[3] The Article 8 of the EU Data Protection Directive prohibits discriminatory data collection and processing activities:

> *Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.*

ethnicity, race, nationality, religion, or political preference. Focusing on certain groups of people, using the surveillance system for social sorting or discriminatory purposes shall not be allowed. Therefore:

1. Surveillance area shall not be restricted to a particular area where people with a certain background lives (i.e., race, ethnicity, nationality, minority status, religion, low-SES and being disadvantaged etc) unless the whole or part of the research is about that particular group. However, the researcher shall make sure that there are appropriate approvals from competent ethical boards before engaging this type of research.
2. Surveillance shall not target particular individuals or groups of people because of their racial, ethnic, or national background, because of their minority status, or because of their sexual, religious, or political preferences.
3. Surveillance data shall not used for discriminating people, for profiling, or for categorizing individuals into groups that can be used against these people. Surveillance system or the data obtained from this system shall not be used for social sorting or discrimination purposes.
4. Surveillance system shall not be used to trace people's activities (i.e., political or religious activities, etc.).
5. Surveillance system shall not target the entrance doors of special places such as churches, mosques, schools, private clinics, lawyer's office, etc.
6. Researchers shall consult with the local authorities in deciding where to site the cameras to avoid biased observations and to prevent discriminatory violations.

5.6 Make sure that you obtained fully informed consent from data subjects.

Many European and international regulations mandate obtaining fully informed consent before working on human subjects[4]. It is not only a legal requirement but also an important ethical precondition for any research on real persons. It is an ethical requirement to explicitly express all the expected advantages, disadvantages, risks, and benefits to the persons who will participate in the research and serve as a data subject.

Obtaining a fully informed consent requires providing a detailed description of how and for what purpose the data will be collected and used. The researchers shall not use any kind of deception, concealment or incomplete disclosure of information to the participants.

In obtaining informed consent, data subjects have the right:

[4] The Article 2 of the EU Directive 95/46/EC defines informed consent as "*any freely given specific and informed indication of his or her wishes by which the data subject signifies his or her agreement to personal data relating to him or her being processed*." The Article 7, under the Section II of the Directive, sets the basic criteria for making data processing legitimate: "…*personal data may be processed only if (a) the data subject has unambiguously given his consent*." Furthermore, the Articles 10 and 11, under the Section IV of the Directive regulates minimum standards for information to be given to the data subject.

- To know that participation is voluntary
- To ask questions and receive understandable answers before making a decision
- To know the degree of risk and burden involved in participation
- To know who will benefit from participation
- To know how their data will be collected, protected during the project and either destroyed or reused at the end of the research
- To withdraw themselves and their data from the project at any time
- To know of any potential commercial exploitation of the research.

The following issues must be stated and explained in the Informed Consent Form:

- Explanation of the research, purpose, duration,
- Description of the study,
- Foreseen risks,
- Benefits,
- Alternatives,
- Confidentiality,
- Treatment/compensation,
- Information,
- Contact for rights/claims,

A copy of the informed consent is presented in Annex A.

5.7 Inform the public about the video surveillance activity.

European regulations[5] and privacy laws of many European countries, and their CCTV guidelines have mandates about informing the public about video surveillance systems. Informing the public is an important

[5] The Article 10 of the EU Data Protection Directive lays down the basics of public notifications. However, the Article 12 of the Regulation (EC) No:45/2001 (*Regulation (EC) No 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*) has a wider scope. This Article maintains that:

> *1. Where the data have not been obtained from the data subject, the controller shall at the time of undertaking the recording of personal data or, if a disclosure to a third party is envisaged, no later than*
>
> *the time when the data are first disclosed, provide the data subject with at least the following information, except where he or she already has it:*
>
> *(a) the identity of the controller;*
>
> *(b) the purposes of the processing operation;*
>
> *(c) the categories of data concerned;*
>
> *(d) the recipients or categories of recipients;*
>
> *(e) the existence of the right of access to, and the right to rectify, the data concerning him or her;*
>
> *(f) any further information such as:*
>
> *(i) the legal basis of the processing operation for which the data are intended,*

matter that has both legal and ethical implications. Therefore, researchers shall inform the public about the video surveillance activity before initiating the system by putting notification signs on visible places in the surveillance area such as walls, polls, etc, and on the local authority's website. Particularly in today's interconnectedness, using social media and other Internet tools helps authorities to convey such messages effectively and makes information flow easier.

These signs are important to notify the public about the video surveillance system to allow people to know what is being done and for what purpose. A typical sign simply tells public that <<the area is being watched by CCTV cameras>> and it would look like this:

Figure2. Sample of CCTV signs

A video surveillance warning sign should provide information to the public about following matters:

- Identity of the data controller: Who is operating the video surveillance system?
- With whom people can contact if they have any questions
- The purpose of the surveillance practice
- Any third parties with whom the data may be shared.

(ii) the time-limits for storing the data,

(iii) the right to have recourse at any time to the European Data Protection Supervisor,

(iv) the origin of the data, except where the controller cannot disclose this information for reasons of professional secrecy,

insofar as such further information is necessary, having regard to the specific circumstances in which the data are processed, to guarantee fair processing in respect of the data subject.

However, the second paragraph of this Article also creates an exception for processing of data for historical or scientific research with the following phrase:

2. Paragraph 1 shall not apply where, in particular for processing for statistical purposes or for the purposes of historical or scientific research, the provision of such information proves impossible or would involve a disproportionate effort or if recording or disclosure is expressly laid down by Community law. In these cases the Community institution or body shall provide for appropriate safeguards after consulting the European Data Protection Supervisor.

5.8 Respect and protect commercial signs and names of the stores by masking them whenever they are visible.

The researchers shall blacken/mask the store names and their commercial signs if they are visible in the surveillance area. This is particularly important for commercial interests of entrepreneurs. If a bad incident happens in, at or in front of a commercial place and it is recorded in the surveillance video, there is a good possibility of risk for the owners of these places if these videos are somehow shared with public. Therefore, in order to protect the best interest of shop owners, the researchers shall mark these fields in the image frame and blacken them permanently and irreversibly. Taking such measures and making them an integral part of the video surveillance algorithm will provide the highest possible protection for the best interest of these individuals. After following these steps, if the software fails to block these names, the masking should be done manually to provide total anonymity.

5.9 Make all recorded video files anonymised permanently and irreversibly. Embed anonymisation techniques (auto-masking of faces, de-identification, etc) as part of the default settings for the surveillance system.

Anonymity is an important safeguard for individuals to protect their privacy in video surveillance research. In fact, in all video surveillance research, it is highly recommended to make anonymity of subjects as *modus operandi* of these systems. Therefore, privacy shall be an embedded as an essential component of the surveillance system and all recorded visual data shall be anonymised permanently and irreversibly. Even though European regulations require very strict data protection measures to be taken. However, if the data is rendered anonymous, these rules will not apply to anonymised data[6].

1. If the surveillance system detect faces of individuals in the surveillance area, the system shall blur/mask them automatically. A fail-safe mechanism shall be envisioned so that if the system fails to de-identify a person by masking her face, the researcher shall do it manually. This process will be permanent and irreversible.
2. The system shall only make video recordings if it detects a criminal activity in the surveillance area. These video files shall be inspected against any failure in the anonymisation process as described above.
3. A special emphasis shall be placed on false positives, which means non-criminal acts are mistakenly identified as criminal acts by the surveillance system.

[6]The Recital 26 of the EU Data Protection Directive: "*... the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable; whereas codes of conduct within the meaning of Article 27 may be a useful instrument for providing guidance as to the ways in which data may be rendered anonymous and retained in a form in which identification of the data subject is no longer possible;*"

4. Data shall be transmitted from the cameras to main computers using industry-standard encrypted channels.
5. The Ethical Review Committee shall review all video files against privacy violations. Further, the ERC shall also approve the anonymisation of the recorded video footage.

5.10 Take a special care for the visual data of children and other vulnerable people, such as the blind, handicapped persons, etc.

The researchers shall take every precaution to protect the best interest of children and other vulnerable groups such as the handicapped and blind people in the surveillance area. Even though the researchers take all necessary steps to meet all the ethical requirements, still, vulnerable groups might always be considered once more before engaging in the implementation of research. How images of children shall be treated and how different needs of the vulnerable groups will be met are important questions in social research and European regulations are very sensitive about these matters.

In informing the public, the researchers should consider different alternatives in informing the children, handicapped and blind people to make sure that everyone is "really" informed fully about what is going on in the surveillance area. For example, researchers might consider informing the families by sending flyers to houses or posting extra information for children on their website there they announce the details of the surveillance program to the public.

Since all data will be anonymised, there will be no need to worry about how the images of children will be treated because these images will also be anonymised permanently and irreversibly, along with others. However, the researchers and the project consortium as a whole should be alert in expecting and responding any possible risks to the well-being of children and vulnerable groups of people.

5.11 Be sensitive and responsive towards citizen complaints and information requests.

The research consortium shall be sensitive about the citizen requests and complaints about the surveillance research. It is their right to know what is going on in their neighbourhood. Therefore, the consortium and the local authorities shall be very responsive towards citizens and their information requests. A contact person shall be assigned from the research consortium to work closely with the local authority in responding to citizens.

5.12 Establish an Ethical Review Committee to serve as an internal oversight body on ethical issues and make regular monitoring on all

stages of data collection and processing, putting special emphasis on matters that have potential for ethical problems.

Naturally, there are many risks to privacy and so many potential ethical problems in video surveillance research. Therefore, establishing an Ethical Review Committee to serve as an integral oversight body on ethical issues and to make regular monitoring on all stages of data collection and processing will create an important safeguard against such violations before they happen.

ERC shall provide guidance on the project's activities and their adherence to the relevant European regulation. ERC shall maintain the following functions throughout the project's lifespan:

- Examining the yearly work plan for ethical or legal questions;
- Monitoring and reviewing project deliverables where ethical questions arise;
- Monitoring for upcoming ethical implications;
- Proposing solutions to legal and ethical questions coming from the participants
- Supervising and approving anonymisation processes in all data files,
- Ensuring the approval of ethical procedures by the competent legal local/national ethics boards, bodies, or administrations in the countries where the different end-user validation will take place (i.e. Spain).

The ERC takes anonymous decisions when it comes to make a decision.

Having ERC in video surveillance research should be considered as a must to provide an important safeguard against ethical misconduct and to secure the highest ethical standards in this type of research.

5.13 Comply with the ethical principles of the national & local authorities and obtain ethical approvals from competent authorities.

In video surveillance research, researchers shall obtain appropriate legal permissions and ethical approvals of competent authorities to ensure the compliance with the ethical standards of the national and local governments. Therefore, the researchers must comply with the data protection rules and ethical principles, and established code of conduct regarding how video surveillance systems should be running. Basically, these authorities are national data protection agencies in European nations and the ethical review boards of local authorities. Obtaining necessary approvals from these entities working closely with them will help the researchers to avoid making serious mistakes. Further, ethical approvals are an essential component of the research funded by European institutions.

5.14 Enforce the industry-standard data protection procedures and comply with European, national and local data protection rules.

The researchers shall use industry-standard data protection systems, rules and procedures that complies with the European, national, and local data protection laws. European regulations require authorities to take necessary measures to protect personal data with highest-level protection standards[7]. Therefore:

1. The research consortium shall embrace the European, national and local data protection rules in all stages of data processing.
2. The data transmission lines (wired, wireless, or with any other technique) shall use industry-standard encryption techniques,
3. The access to data systems shall only be limited to the authorized personnel.
4. All recorded data shall be stored in a secure environment in anonymized format.
5. No part of non-anonymised data shall be retained in the computers or in data storage systems.
6. Erasure that non-anonymised data shall be destroyed irreversibly using industry-standard erasure techniques.

[7] The Article 7 of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data: "*Appropriate security measures shall be taken for the protection of personal data stored in automated data files against accidental or unauthorised destruction or accidental loss as well as against unauthorised access, alteration or dissemination.*"

6 Approval of the Ethical Review Committee

After careful examination, review, and discussion of this ethical review report on the data acquisition practices in SmartPrevent Project, we as the member of the Ethical Review Committee (ERC) attest to the validity of this report. We approve the SmartPrevent data acquisition techniques in the presented form. ERC expects to be informed about the progress of the study, any legal & ethical problems occurring in the course of the study, any revision in the protocols, information sheets, and informed consent forms, and asks to be provided a copy of the D7.21 Ethical Guidelines, the First Ethical Report, and the Final Ethical Report.

Prof. Osman Dolu, Ph.D.
Chairman of the Ethical Review Committee

Chief Manuel López
Head of ALR Police Department

Prof. Shaogang Gong, Ph.D.
Representative of the Scientific Committee

Prof. İsmail Dinçer Güneş, Ph.D.
External Expert
Turkish National Police Academy

Dr. Zeev Smilansky
Representative of the Security Committee

References

Belfast Education and Library Board (2007). *The Eight Data Protection Principles*. Full text electronically available at: http://www.belb.org.uk/downloads/foi_data_principles.pdf.

Bourne, Ian (2010). *A Guide to Data Protection in Israel*. The Israeli Law, Information and Technology Authority (ILITA), January 2010. Full text electronically available at: http://www.justice.gov.il/NR/rdonlyres/C7DE27A2-4CC2-4C5E-9047-C86CC70BD50B/18333/AguidetodataprotectioninIsrael1.pdf

Canada Information and Privacy Commissioner (2015). "7 Foundational Principles of Privacy by Design". Retrieved from https://www.privacybydesign.ca/index.php/about-pbd/7-foundational-principles/, on June 10, 2015.

Carroll, Seamus (2014). "Data protection rights of children". Full text electronically available at: http://www.coe.int/t/dghl/standardsetting/dataprotection/CAHDATA/Data%20protection%20rights%20of%20children_En%20&%20Fr_Seamus%20Carroll.pdf.

Cavoukian, Ann (2008). *Privacy and Video Surveillance in Mass Transit Systems: A Special Investigation Report.* Ontario, Canada: Information and Privacy Commissioner. Full text available at: https://www.ipc.on.ca/images/Findings/mc07-68-ttc_592396093750.pdf.

Cavoukian, Ann (2011). *Privacy by Design: The 7 Foundational Principles*. Full text electronically available at: https://www.ipc.on.ca/images/resources/7foundationalprinciples.pdf.

Cavoukian, Ann (2012). *Operationalizing Privacy by Design: A Guide to Implementing Strong Privacy Practices*. Ontario, Canada: Information and Privacy Commissioner. Full text available at: https://www.privacybydesign.ca/content/uploads/2013/01/operationalizing-pbd-guide.pdf.

Clarke, Steve (2013). "Trends in crime and criminal justice, 2010" EuroStat Statistics in Focus 18/2013: Populations and conditions. Report electronically available at: http://epp.eurostat.ec.europa.eu/cache/ITY_OFFPUB/KS-SF-13-018/EN/KS-SF-13-018-EN.PDF.

Constitution of Spain 1978 with Amendments through 2011. Full text electronically available at: https://www.constituteproject.org/constitution/Spain_2011.pdf

Constitution of the Republic of Turkey 1982. Full text electronically available at: https://global.tbmm.gov.tr/docs/constitution_en.pdf.

Council of Europe (1981). European Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981) (Convention 108). Full text electronically available at: http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm.

Ergün, Çağdaş Evrim (2011). "Data Privacy in Turkish Law". *IT, Internet and Outsourcing Bulletin,* April 8, 2011. Full textavailable at: http://www.whitecase.com/articles-04082011-1/#.VXKz7aa222w. Accessed on June 1, 2015.

European Commission (2006). Communication from the Commission: Towards an EU Strategy on the Rights of the Child. COM(2006) 367 Brussels, 4.7.2006, final http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0367:FIN:en:PDF.

European Commission (2010). *Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions: A comprehensive approach on personal data protection in the European Union*. Full text available at: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52010DC0609&from=EN.

European Commission Data Protection Working Party (2009). Opinion 2/2009 on the protection of children's personal data (General Guidelines and the special case of schools). Full text available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp160_en.pdf.

European Commission Data Protection Working Party (2009). Opinion 2/2009 on the protection of children's personal data (General Guidelines and the special case of schools). Full text available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp160_en.pdf.

European Commission Decisionof 31 January 2011pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data by the State of Israel with regard to automated processing of personal data. Full text available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:027:0039:0042:EN:PDF

European Convention for the Protection of Human Rights and Fundamental Freedoms (1950). Full text electronically available at: http://conventions.coe.int/treaty/en/treaties/html/005.htm

European Data Protection Supervisor (2010). *EDPS Video Surveillance Guidelines*. March 2010. Full text electronically available at: https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Supervision/Guidelines/10-03-17_Video-surveillance_Guidelines_EN.pdf

European Union (2000). "Charter of Fundamental Rights of the European Union", Official Journal of the European Communities, C 364, pp.1-22, Full text available at: http://www.europarl.europa.eu/charter/pdf/text_en.pdf.

Harrendorf, S.; Heiskanen, M.; Malby, S. (2010). *International Statistics on Crime and Justice*. Helsinki:EuropeanInstitute for Crime Preventionand Control (HEUNI). Electronically available at: http://www.unodc.org/documents/data-and-analysis/Crime-statistics/International_Statistics_on_Crime_and_Justice.pdf.

Novogroder-Shoshan, Yoheved (2012). Data Protection& PrivacyJurisdictional Comparisons: Israel.European Lawyer Reference Series. First Edition. YigalArnon& Co Law Firm, Jerusalem: Israel. Full text available at: http://www.arnon.co.il/files/e3b84790d602b8d3179de6a92b2be89a/127.%20Data%20Protection%20-%20ISRAEL.pdf.

PbD (2011). *Privacy by Design: Time to Take Control*. Full text electronically available at: *https://www.privacybydesign.ca/content/uploads/2011/02/2011-01-28-pbd-toronto.pdf*

Spanish Data Protection Agency (N/A). *Guide on Video Surveillance*. Full text available at: http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/pdfs/guia_videovigilancia_en.pdf

Spanish Data Protection Law (*Organic Law 15/1999 of 13 December on the Protection of Personal Data*). Full text available at: www.legislationline.org/documents/id/9044.

Spanish National Institute of Communication Technologies (2011). *Video Surveillance and Personal Data Protection Guide*. Edition: June 2011. Full text electronically available at: https://www.incibe.es/file/hTpGu-OiEIX5jJXCucHxhQ

The United Kingdom Data Protection Act 1998. Full text available at: http://www.legislation.gov.uk/ukpga/1998/29/pdfs/ukpga_19980029_en.pdf

The United Kingdom Home Office (2013). *Surveillance Camera Code of Practice*. June 2013. Full text electronically available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/204775/Surveillance_Camera_Code_of_Practice_WEB.pdf.

The United Kingdom Information Commissioner's Office (2010). *Privacy Notices Code of Practice.* December 2010. Full text electronically available at: https://ico.org.uk/media/for-organisations/documents/1610/privacy_notices_cop.pdf.

The United Kingdom Information Commissioner's Office (2011). *Data Sharing Code of Practice.* May 2011. Full text electronically available at: https://ico.org.uk/media/for-organisations/documents/1068/data_sharing_code_of_practice.pdf.

The United Kingdom Information Commissioner's Office (2012). *Anonymisation Code of Practice.* November 2012. Full text electronically available at: https://ico.org.uk/media/1061/anonymisation-code.pdf.

The United Kingdom Information Commissioner's Office (2015). *CCTV Code of Practice.* Version 1.1, 21/05/2015. Full text electronically available at: https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf.

The United Kingdom Information Commissioner's Office (2015). *The Guide to Data Protection*. Edition: March 2015. Full text electronically available at: https://ico.org.uk/media/for-organisations/guide-to-data-protection-2-2.pdf.

The United Kingdom Surveillance Camera Commissioner (2012). *A Guide to the 12 Principles.* Full text electronically available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/368115/Leaflet_v6_WEB.pdf.

The United Kingdom Surveillance Camera Commissioner (2014). *Conducting Privacy Impact Assessment Code of Practice*. February 2014. Full text electronically available at: https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

United Nations (1948). *United Nations Declaration of Human Rights*. Full text electronically available at: http://www.un.org/en/documents/udhr/.

United Nations (1989). *Convention on the Rights of the Child*. Full text electronically available at: http://www.refworld.org/cgi-bin/texis/vtx/rwmain?docid=3ae6b38f0.

Annex A Informed Consent Form

Research Project: SmartPrevent

Researcher's Statement

We are asking you to participate in a formal, EC-supported (FP7) research study. The purpose of this consent form is to give you the information you will need to help you decide whether or not participate in the study. Please read the form carefully. The participation to this study is voluntary. You may ask any questions you wish about the purpose of the research, what we will ask you to do, the possible risks and benefits, your rights as a volunteer, and anything else about the research or this form that is not clear to you. When all your questions are answered, you can decide if you want to be in the study or not. This process is called "informed consent." We will give you a copy of this form for your records if you kindly agree to take part in this research.

Purpose and Benefits

The purpose of this study is to enhance detection and prevention of crimes in local urban areas by exploiting the full potential of video-surveillance systems. Through your voluntary participation, this research will fulfill its aims more properly. Thus, you will make a significant contribution for safer societies around Europe and all over the globe.

Procedures

I will ask you to answer several interview questions related to the research project set forth above. I will audio- tape our conversation, only if you permit me to do so, for later study. The interview will take about ten minutes. You may refuse to answer any particular question, and you may stop the interview at any time. Your responses will be kept confidential. After that, we will ask for your participation in the recording of a series of videos that simulated acts of vandalism, with the possible roles, criminal, victim or public. Your participation in the videos will take about one hour [or more as you decide]. You may refuse to participate in any particular criminal situation, and you may stop the intervention in the videos at any time. Your recordings will be kept confidential.

Risks, Stress, or Discomfort

During the interviews or other research activities, should you not feel comfortable with any question /activity please let us know; you do not have to answer the questions that you do not feel comfortable about. If you experience any discomfort or stress from the interview, you may stop it at any time. Should you have any questions after the interview, please contact with us using the information listed below:

On behalf of SmartPrevent/ALR Municipality

Representative's Name: .....

Phone: .....

Fax: .....

Email: .....

Participant's Statement

This study has been explained to me. I have understood everything I was told. I volunteer to take part in this research. I have had a chance to ask questions. If I have general questions about the research, I can ask to the researcher listed above. If I have questions regarding my rights as a participant, I can call the.....

This project has been reviewed and approved for human participation by the SmartPrevent Ethical Review Committee and ALR Ethics Committee.

I will receive a copy of this consent form if I request it.

Participant's Signature:.....

Date:.....

Annex B Information Sheet

Dear Participant,

You are participating in a European Commission supported (FP7) research project entitled <<Smart Video-Surveillance System to Detect and Prevent Local Crimes in Urban Areas>> with the acronym SmartPrevent. This research project aims to detect criminal activities earlier and to help police intervene criminal events faster and catch criminals. We have listed a number of regulations for your information. We kindly request you to read these statements below.

1. Participation in this exercise is completely voluntary.

2. Before taking part in this study, please bear in mind that you can always quit participation in this study at any time.

3. You will be properly briefed about the study before you decide to participate in the study.

4. Your rights and privacy is always our top priority. All data collected in this study will be anonymized irreversibly to protect your identity. We will never jeopardize your privacy or violate your personal rights throughout the study.

5. Your privacy is to be safeguarded by the Ethical Review Committee, you will be properly informed about how your data will be collected and protected during the project.

6. All data collected in this participation will be used only for scientific purposes and they will not be shared with third parties. At the end of the research, all data will be destroyed.

7. In case of debate you are entitled to be heard by the Ethical Review Committee and/or the Project Manager.

8. We kindly request you to sign this participation consent form to confirm that you are aware of the regulations stated above.

On behalf of SmartPrevent/ALR,

Participant Name:.....

Signature:.....