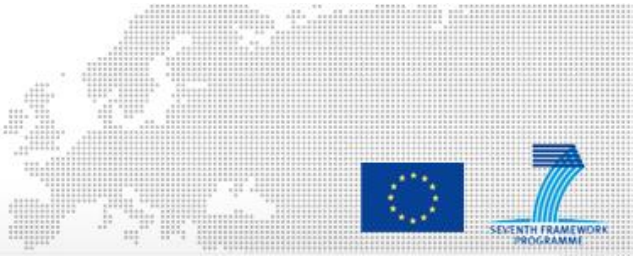
Preliminary Scoreboard for Evaluation of System Compliance with Privacy

Deliverable 1.3

Lancaster University



Automatic Data relevancy Discrimination for a PRIVacy-sensitive video surveillance

Automatic Data relevancy Discrimination for a PRIVacy-sensitive videosurveillance

SEC-2010.6.5-2 - Use of smart surveillance systems, data protection, integrity and sharing information within privacy rules

D1.3 – Preliminary Scoreboard for Evaluation of System Compliance with Privacy

Due date of deliverable: 31/07/2011

Actual submission date: 31/07/2011

Start of project: 01 February 2011 Duration: 36 Months

Lead Contractor for this deliverable: Lancaster University

Revision: 01

Project co-funded by the European Commission within the Seventh Framework Programme		
Dissemination level		
PU	Public	PU
CO	Confidential, only for members of the consortium (including the Commission Services)	

Revision History

Deliverable Administration and summary		
Project Acronym: ADDPRIV		Grant Agreement no: 261653
Document Identifier: ADDPRIV_20113107_WP1_LANCASTER_P_scoreb_R1.pdf		
Leading partner: Lancaster University		
Report version: 01		
Report preparation date: 28/07/2011		
Classification: Public		
Nature: Other		
Author(s) and contributors: Inga Kroener, Daniel Neyland		
Status		Plan
		Draft
		Working
	X	Final
		Submitted
		Approved

The ADDPRIV consortium has addressed all comments received, making changes as necessary. Changes to the document are detailed in the change log table below.

Date	**Edited by**	**Status**	**Changes made**
31/07/2011	Anova	Final	Quality control
26/07/2011	TCD	Final	Final review
26/07/2011	LANCASTER	Final	Final version
04/07/2011	LANCASTER	Draft	

Copyright

Citation

Kroener, I. Neyland, D. (2011). Deliverable 1.3 – Preliminary Scoreboard for Evaluation of System Compliance with Privacy. ADDPRIV consortium, www.addpriv.eu

Acknowledgements

The work presented in this document has been conducted in the context of the EU Framework Programme project with Grant Agreement 261653 ADDPRIV (Automatic Data relevancy Discrimination for a PRIVacy-sensitive video surveillance). ADDPRIV is a 36 months project started on February 1st, 2011.

The project consortium is composed by: Anova IT Consulting (ANOVA), Kingston University Higher Education Corporation (KU), Politechnika Gdanska (GDANSK), Lancaster University (ULANCS), Avanzit Tecnologia, S.L. (AVANZIT), Hewlett Packard Italiana Srl (HP), Societá Per Azioni Esercizi Aeroportuali Sea SPA (SEA), Renfe Operadora (RENFE) and The Provost Fellows & Scholars Of The College Of The Holy And Undivided Trinity Of Queen Elizabeth Near Dublin (TCD).

More Information

Public ADDPRIV reports and other information pertaining to the project are available through ADDPRIV public website under www.addpriv.eu

Table of contents

1. Introduction

1.1 The ADDPRIV Project

The main aim of the ADDPRIV project is to develop privacy sensitive video surveillance systems. The project seeks to reduce the storage of unnecessary data and protect the individual's right to privacy. The project, led by Anova IT Consulting (ES), will last 36 months. The partners involved are: Anova IT Consulting (ES) Kingston University (UK), Politechnika Gdanska (PL), Lancaster University (UK), Avanzit Tecnología (ES), Hewlett Packard Italiana (IT), SEA Aeroporti di Milano (IT), Renfe Operadora (ES) and Trinity College Dublin (IE). The new video surveillance systems and algorithms will be tested in the airports and transport hubs of the partner countries.

ADDPRIV tackles the challenge of determining in a precise and reliable manner private data from video surveillance which is not relevant from the perspective of security and which does not need to be stored. ADDPRIV proposes solutions for automatic discrimination of relevant data recorded on a multi-camera network. Relevant data not only corresponds to video scenes capturing individuals' suspicious behaviour (smart video surveillance), but also automatically extracting images on these individuals recorded before and after the suspicious event and across the surveillance network.

ADDPRIV will have 2 external advisory boards that will ensure that the proposed solution is precisely defined, developed and implemented for privacy enhancement and to protect the human rights of surveilled individuals. One advisory board will be made up of end users; the other will offer advice on ethics in the broadest sense (privacy, human rights, social and political consequences of technology).

1.2 The Ethics Scoreboard

The systems developed under the ADDPRIV project, and the solutions offered, will be validated and guided by criteria and metrics determined by social and ethical experts and end users, establishing the characteristics that a surveillance system must fulfill for effectiveness and integrity in citizens privacy protection. The ethics scoreboard is the first stage in developing system evaluation. It includes a section on legal compliance, detailing the areas that are already implemented under national and EU law, in terms of data and privacy protection. The second section is concerned with ethical compliance. The aim of this second section is to assist in the development of new ethical standards for surveillance systems that go beyond legal compliance. The ADDPRIV technology will attempt to deliver a new benchmark for ethical standards.

2. EU Legal Compliance

This section of the report looks at the legal criteria, which members of the EU must abide by in terms of data and privacy protection. These areas are highly developed and have a long history across the European Union. The Data Protection Directive 95/46/EC regulates the processing of personal data. Alongside this, all member states are signatories of the European Convention on Human Rights (ECHR).

Currently most national data protection is based on the following 8 EU principles of data protection:

Data must be:	
1)	Fairly and lawfully processed
2)	Processed for limited purposes
3)	Adequate, relevant and not excessive
4)	Accurate
5)	Not kept for longer than necessary
6)	Processed in accordance with individual's rights
7)	Secure
8)	Not transferred to countries without protection

These principles are legally binding for all member states of the union and override the myriad diverse regulatory policy arrangements that previously existed across Europe.

Alongside these principles of data protection, the EU also upholds the protection of personal data through the Charter of Fundamental Rights of the European Union.[1]

[1] http://www.europarl.europa.eu/charter/pdf/text_en.pdf

This states that:

> 1. Everyone has the right to protection of personal data concerning him or her
> 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law
> 3. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified
> 4. Compliance with these rules shall be subject to control by an independent authority

These independent authorities are typically data protection, privacy or information commissioners. The data protection principles are not self-enforcing.[2]

In terms of data protection with regard to video surveillance the Article 29 Working Party[3] (which is made up of a representative from the data protection authority of each EU member state and provides expert advice on data protection to member states), states that:

> Data subjects have the right to exercise their freedom of movement without undergoing excessive psychological conditioning as regards their movement and conduct.

This is followed by a warning against a:

> Disproportionate application of video surveillance in public places which would allow tracking of individuals' movement and/or triggering 'alarms' based on software that automatically 'interprets' an individual's suspicious conduct without any human intervention.

This is particularly important for ADDPRIV as the development of algorithms for alerting surveillance operatives to suspicious behaviour forms a large part of the

[2] i.e. they do not hold within them a guarantee of enforcement.
[3] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2002/wp67_en.pdf

project. The European Commission recently (September 2010) communicated the need for a revision of the current EU Data Protection Directive, following the advice of the Article 29 Working Party. Alongside a need for privacy protection to be included throughout the entire life cycle of a product (which is returned to later on in this document), the European Commission has stated that data protection legislation needs to be revised and clarified.[4]

Data protection principles in the context of video surveillance are only applicable where a processing of personal data takes place. Personal data means any information relating to an identified or identifiable natural person (one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, psychological, mental, economic, cultural or social identity). Video surveillance data has to comply with data protection principles:

Even if the images are used within the framework of a closed circuit system, even if they are not associated with a person's particulars, even if they do not concern individuals whose faces have been filmed, though they contain other information such as, for instance, car plate numbers or PIN numbers as acquired in connection with the surveillance of automatic cash dispensers, irrespective of the media used for the processing, the technique used, the type of equipment, the features applying to the image acquisition and the communication tools used.

Furthermore, data protection safeguards are also in place, which are as follows:

1) The personal data should be obtained and processed lawfully. This implies, amongst others, the processing to fit into the competences or legitimate interests of the controller and to be grounded on one of the motives listed by the Directive
2) In most of the cases, when it comes to public surveillance networks, the lawfulness of the purpose will be based on the existence of an important public interest
3) The processing is usually justified on the need to perform a task carried out in the public interest or in the exercise of official authority vested in the controller

[4] September 2010 'European Commission's Strategy for Data Protection Directive' http://www.edri.org/edrigram/number8.18/ec-strategy-data-protection-directive

4)	The deployment of a video surveillance network has to be proportionate to the objective foreseen
5)	Due to the highly intrusive nature of video surveillance processing, they should only be implemented on a subsidiary basis, when other processing less intrusive could not be implemented or would prove insufficient
6)	Proportionality assessed on a case-by-case basis
7)	Video surveillance with public security needs should be focused on areas that are really at risk, public events that can reasonably be expected to give rise to incidents and more serious crimes
8)	The visual angles, the possibility of zooming, image-freeze functions, etc. should only be implemented when they are deemed proportionate to the purpose foreseen
9)	The use of video surveillance systems is governed by the principle of minimum intervention
10)	The images recorded by the video surveillance cameras can only be used for the specified purpose: they cannot be retained and used for any other purpose incompatible with the original one
11)	Only the further processing of data for historical, statistical or scientific purposes are always considered compatible by the Directive provided that Member States ensure appropriate safeguards
12)	Article 29 Working Party recommended to rule out "that the images collected may be used for further purposes with particular regard to the technical reproduction opportunities – e.g. by expressly prohibiting copying"

In sum, an initial set of dimensions to take forward in this report are provided by these EU level policies and regulations. However, we also need to understand how these have been put into use in the specific members of the ADDPRIV project. In the following section, national regulations in the UK, Spain, Italy and Poland will be considered as these are the countries in which the ADDPRIV technology will be initially tested and developed.

2.1 Country Specific Legislation

This section of the report outlines data protection and privacy legislation across the UK, Poland, Italy and Spain (the partner countries in which the technologies developed under ADDPRIV will be tested). After the legislation has been introduced, the report will describe what this legislation means for ADDPRIV. This section will provide context to the later sections concerned with developing the scoreboard for legal compliance, and subsequently the ethical section of the scoreboard.

2.1.1 The United Kingdom (UK)

The UK Data Protection Act contains the following eight principles:

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless

   (a) at least one of the conditions in Schedule 2 is met, and
   (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.

2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.
4. Personal data shall be accurate and, where necessary, kept up to date.
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.
6. Personal data shall be processed in accordance with the rights of data subjects under this Act.
7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

In terms of video surveillance, the UK Information Commissioner has issued guidance for those organisations using CCTV, to comply with the Data Protection Act. Included in this is the CCTV Code of Practice, which states that:

Principle one:

- Data must be processed fairly and lawfully. CCTV must be operated for a 'legitimate reason', i.e. prevention and detection of crime
- The 'fair' processing of images also requires adequate signage to the public, i.e. who is collecting data and for what purpose

Principle two:

- Data should be obtained only for specified and lawful purposes, and should not be processed in any manner incompatible with that purpose
- This helps ensure the confidentiality of information obtained

Principle three:

- Data should be adequate, relevant and not excessive. This has implications for privacy in terms of ensuring that cameras are not monitoring individuals in private spaces

Principles four and five:

- Personal data should be accurate and where necessary kept up to date and should not be kept longer than is necessary
- Adequate measures should also be taken against unlawful processing. This would include security arrangements in terms of who could access the recorded material

2.1.2 Spain

In terms of the Spanish Data Protection Act the collection of data is allowed (and protected) as follows:

1.	May be collected for processing only if it is relevant and not excessive in relation to the purposes for which it was obtained
2.	May not be used for purposes incompatible with those for which the data was collected
3.	Shall be accurate and updated
4.	If proved to be inaccurate, shall be erased and replaced
5.	Shall be erased when it has ceased to be necessary or relevant
6.	Shall be stored in a way which permits the right of access to be exercised, unless lawfully erased

The collection of data by 'fraudulent, unfair or illicit means' is prohibited. Data subjects are also entitled to withdraw their consent to the holding of data that pertains to them.

In 2006, Spain also published its new regulation on video surveillance: Instruction 1/2006. This legislation defines images obtained by surveillance cameras in public space as personal data. This means that these images and data derived from these images are to be treated as personal data and protected as such. Under this legislation, video surveillance cameras are only to be used when other, proportionate means of surveillance are not easily available, and the collected data must be deleted within one month.[5] Under this legislation, the processing of personal data requires the data subject's consent (although there are exceptions to this in the Spanish Private Security Law.[6] The Spanish Data Protection Authority (AEPD) states that 'collecting the images of a person in a public place constitutes data processing'. Spain therefore recognises the right not to be filmed in public space without prior consent.[7]

[5] https://www.privacyinternational.org/article/phr2006-kingdom-spain

[6] Ley 23/1992 de 30 de Julio, de Seguridad Privada. Available in Spanish at: http://noticias.juridicas.com/base_datos/Admin/l23-1992.html

[7] Instruction 1/2006 available in Spanish at: http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/pdfs/guia_videovigilancia.pdf

2.1.3 Italy

The main features of the Italian Data Protection Code (2003) are as follows:

1. Notification

   To summarise, organisations are only required to notify the Garante when processing higher-risk categories of data (which includes genetic and biometric data).

2. Data minimisation

   The code encourages organisations to make use of non-personal data whenever possible.

3. Data subjects' rights

   The code aims to strengthen individuals' data protection rights. Individuals do not have to demonstrate that damage or distress has been caused as a result of a data protection breach – they only have to demonstrate that their privacy has been breached.

4. International data transfers

   Companies only have to provide notification to the Garante of their intention to transfer data outside the EU in cases in which the transfer of data could prejudice data subjects' rights.

Alongside this data protection code exists the Italian Privacy Code (2003), which states that:

1. Treatment of the data concerned is performed using procedures that guarantee respect for the privacy rights of the user and consists of its collection, registration, organisation, archiving, processing, modification, selection, retrieval, comparison, use, interconnection, grouping, communication, circulation, cancellation and destruction.
2. Treatment of personal data will be performed mainly using automatic and computerized methods … and, in any event, always in full respect of privacy and security rules specified by current law.
3. The data will be preserved, for the length of time specified by law, at the operational headquarters of EAPC and on the servers of the EAPC data processing agency.
4. The user may contact the controller, EAPC, at any time to exercise his rights as indicated in Article 7 of Italian Law 196/03.

Under Article 7, individuals have the right to receive confirmation of the existence or not of personal data of which he/she is subject. Furthermore (and in summary), the individual has the right to know the origin of personal data, the purposes for and conditions in which said data is to be treated, and the identity of the controller and processors, the subject or subject categories to which personal data may be communicated. The individual also has the right, wholly or in part, to oppose the treatment of data of which he/she is subject (even if pertinent to the purposes of the data collection); and to oppose the treatment of data to which he/she is subject for the purpose of commercial communications.

In terms of video surveillance, the Italian privacy watchdog issued new regulations to protect the public in April 2010. These included the need for clear signposting for all areas under surveillance; except CCTV installed for public security purposes (e.g. the prevention of terrorism). With reference to processing personal data and video surveillance, the guidelines from the Italian DPA state that 'image-collecting systems should be carried out in accordance not only with data protection legislation, but also with the requirements set forth in other pieces of legislation where applicable'.

In terms of data retention periods, under Italian legislation the images should not be retained for longer than a few hours, and up to a maximum of 24 hours, except in the case of high-risk activities performed by the data controller (e.g. in the case

of banks). Even in these high-risk cases, the period of data retention should be no longer than one week.

2.1.4 Poland

The Polish Act on Personal Data Protection (1997) has the following principles:

1)	To eliminate any failure
2)	To complete, update, correct, disclose or keep confidential the personal data
3)	To apply additional measures protecting the personal data files
4)	To suspend the transmission of personal data to third countries
5)	To safeguard the data or to transfer them to different entities
6)	To erase the personal data

Alongside this, Article 47 of the Constitution of the Republic of Poland ensures the legal protection of the private and family life of citizens: 'Everyone shall have the right to legal protection of his private life and family life, of his honour and good reputation and to make decisions about his personal life". Article 51 (of the Constitution) limits the circumstances in which the state can gather personal data, and confers basic rights upon citizens, for instance the right to access. It states:

> Public authorities shall not acquire, collect or make accessible information on citizens other than that which is necessary in a democratic state ruled by law.
>
> Everyone shall have a right to access to official documents and data collections concerning him. Limitations upon such rights may be established by statute.
>
> Everyone shall have the right to demand correction or deletion of untrue or incomplete information, or information acquired by means contrary to statute.

2.2 Summary

In summary, the 8 EU Principles of data protection described at the beginning of the legal section of this report are the fundamental principles found in various countries' national legislation outlined above. All countries subscribe to these principles, however with different emphases and additions. For example, under Italian data protection law (particularly in the context of video surveillance) images are only retained for a certain period of time. In Spain, data subjects are allowed to withdraw their consent to data held about them. For the purpose of this report, the 8 main EU principles have been combined with the various differences and additions in national legislation in the preliminary scoreboard. The next section of this report looks beyond legal compliance to include areas of ethical concern.

3. Ethical Compliance

3.1 Introduction

This section of the report introduces the part of the scoreboard related to ethical compliance. It moves beyond the legal compliance, outlined in the first part of this report, to attempt to develop new ethical standards for surveillance systems in relation to the technology developments proposed within ADDPRIV.

The legal criteria outlined previously in this report do not include issues such as whether a method of data collection is ethical, or whether enough thought has been given to the process of data extraction from the individual. Furthermore, other issues which need to be taken into account are those of data dispersal, the reusing of data, data storage and deletion, and discrimination in terms of data collection. This is not an exhaustive list and is expanded upon below and in the ethics scoreboard.

Current academic literature on surveillance and informational privacy highlights that personal information collected from individuals moves across borders (it is not fixed or static). Individual data is, Bennett argues, 'dispersed and accessible from a multitude of remote locations'.[8] It has been suggested that the current framework for protection of informational privacy is focused too narrowly on three principles: intrusion by government, protection of sensitive data, and protection of private sphere of life. Nissenbaum, for example, argues for 'contextual integrity'. This means data should only be utilised in line with appropriate uses given the context of data collection and only distributed in line with the purposes for which data was given.[9]

Such contextual integrity is difficult to achieve given that digital data now crosses boundaries and borders. Within the remit of the Spanish Data Protection Agency, for example, one of their roles is to 'monitor international movements of data'. However, such movement of data are difficult to regulate. For example, although national data protection legislation is generally based on the principle that data

[8] Bennett, C. (1992) *Regulating Privacy: Data Protection and Public Policy in Europe and the United States* Cornell University Press
[9] Nissenbaum, H. (2004) 'Privacy as Contextual Integrity' *Washington Law Review* 79(1) pp. 119-158

should not be used for any other than its intended or original purpose, movement of data across borders and institutions suggests the original purpose of data collection may not remain exactly the same. Surveillance theorists such as Marx suggest that data protection and fair information codes are not sufficient to protect the data in terms of the appropriateness of the original goals, or the broader context in which the data was collected.[10]

This suggests that more thought needs to be given by those operating, managing and overseeing surveillance systems to the storage and security of information, and information crossing borders and boundaries. Furthermore, issues of fairness, equality, and protection against discrimination by surveillance operators must be taken into account. Norris and Armstrong (1999) for example suggest that surveillance operators shape the targets to be closely scrutinised through their own prejudice.

Further issues arise for surveillance systems in terms of control of information. Individuals are given the right across the EU to request information collected about themselves through the various Freedom of Information Acts. However, consent prior to the collection of data and control over how that data is stored, used, and processed remains difficult for the individual. Flaherty argues that 'individuals want … to exercise some control over how information about them is used'[11] and Lessig suggests 'Individuals should be able to control information about themselves' are also found.[12]

Taken together these issues suggest that surveillance systems based on algorithms picking out suspicious behaviour have potential advantages. The ADDPRIV project proposes developing algorithms for the selection of suspicious behaviour and the deletion of non-suspicious data. Deletion might provide a means to limit the movement and accessibility of data. Also, ADDPRIV will involve the development of automatic triggers for surveillance systems to alert operatives to suspicious behaviour. This may be an advantage in terms of privacy protection due to negating the potential bias of a human controller at the outset. And developing a new surveillance system introduces opportunities for re—thinking how data subjects might be more involved in issues of consent and information control, perhaps through expanding public accountability for the ADDPRIV system. Beyond these issues, there are further issues of ethical concern with an automated system, such

[10] Marx, G. T. (1998) 'Ethics for the New Surveillance' in *The Information Society* 14 pp.171-185
[11] Flaherty, D. (1989). Protecting privacy in surveillance societies
[12] Lessig, L. (2006). Code: Version 2.0

as the occurrence of false positives and false negatives (this is included in the ethical scoreboard).

The scoreboard will therefore take account of data movement, fairness, non-discrimination, consent, control of information (both in terms of *a priori* and *post*-collection of individual data) and accountability for the development of the ADDPRIV technology. These issues will be engaged in the following manner. The next section of the report provides an overview of Privacy Impact Assessments. These are important for ADDPRIV as they are used by organisations (and recommended by privacy commissioners and information commissioners) as a way of assessing and identifying any privacy concerns at an early stage in a project or development. ADDPRIV seeks to address any privacy and ethical concerns during the technology development stage. The second section of the report covers privacy by design. This is important for ADDPRIV as privacy protecting features will be designed into the technology at the outset. The third section of the report looks at alternative codes for privacy protection (moving beyond simply legal compliance). These are important for ADDPRIV due to the project's aim to move beyond legal compliance, to include wider issues of ethical concern.

3.2 Privacy Impact Assessments

This section covers Privacy Impact Assessments (PIAs). These assessments are utilised in organisational and institutional settings to assess and protect against any potential privacy invasions. As stated above, these are important in terms of the ADDPRIV project as they are put into practice during the developmental stage of a new technology.

In order to be effective, the Information Commissioner's Office (UK) (ICO) states that PIAs need to move beyond legal compliance checks in order to 'offer a prospective identification of privacy risks *before* systems and programmes are put in place', and 'have to consider privacy risks in a wider framework which takes into account the broader set of community values and expectations about privacy'.[13]

PIAs are therefore not simply legal compliance checks, which ask 'If we did X, would we be in compliance with the law and the fair information principles upon

[13] Linden Consulting Inc. (2007) *Privacy Impact Assessments: International Study of their Application and Effects* Prepared for the Information Commissioner's Office UK

which the law is based?' Nor are they privacy audits, used to assess existing technologies. A 2007 Linden report for the ICO states that they are most useful for new programmes, services or technologies. However, they are not simply used to warn against potential risks but also to mitigate these risks, and to change the development process accordingly. PIAs therefore move beyond the legal compliance to assess and address the 'moral and ethical issues posed by whatever is being proposed'.[14]

According to the Australian Privacy Commissioner there are five key stages to developing a PIA.[15] These are as follows:

Project description: broadly describe the project, including the project's aims and whether any personal information will be handled;

Mapping the information flows: describe and map the flows of personal information in the project;

Privacy impact analysis: identify and analyse how the project impacts upon privacy;

Privacy management: consider alternative options, particularly those which will improve policy outcomes whilst still achieving the project's goals;

Recommendations: produce a final PIA report, which includes the above information and recommendations.

In this sense the ethical aspects of the ADDPRIV project run along the lines of a PIA; identifying privacy implications and developing the project in ways to combat these potential infringements.

[14] Flaherty *Privacy Impact Assessments* p.266
[15] http://www.privacy.gov.au/publications/pia06/index.htm#mozTocld799546

A crucial aspect of these preceding steps for the ADDPRIV project is to assess the flow of personal information. The Australian guidance suggests that the steps to do this could include[16]:

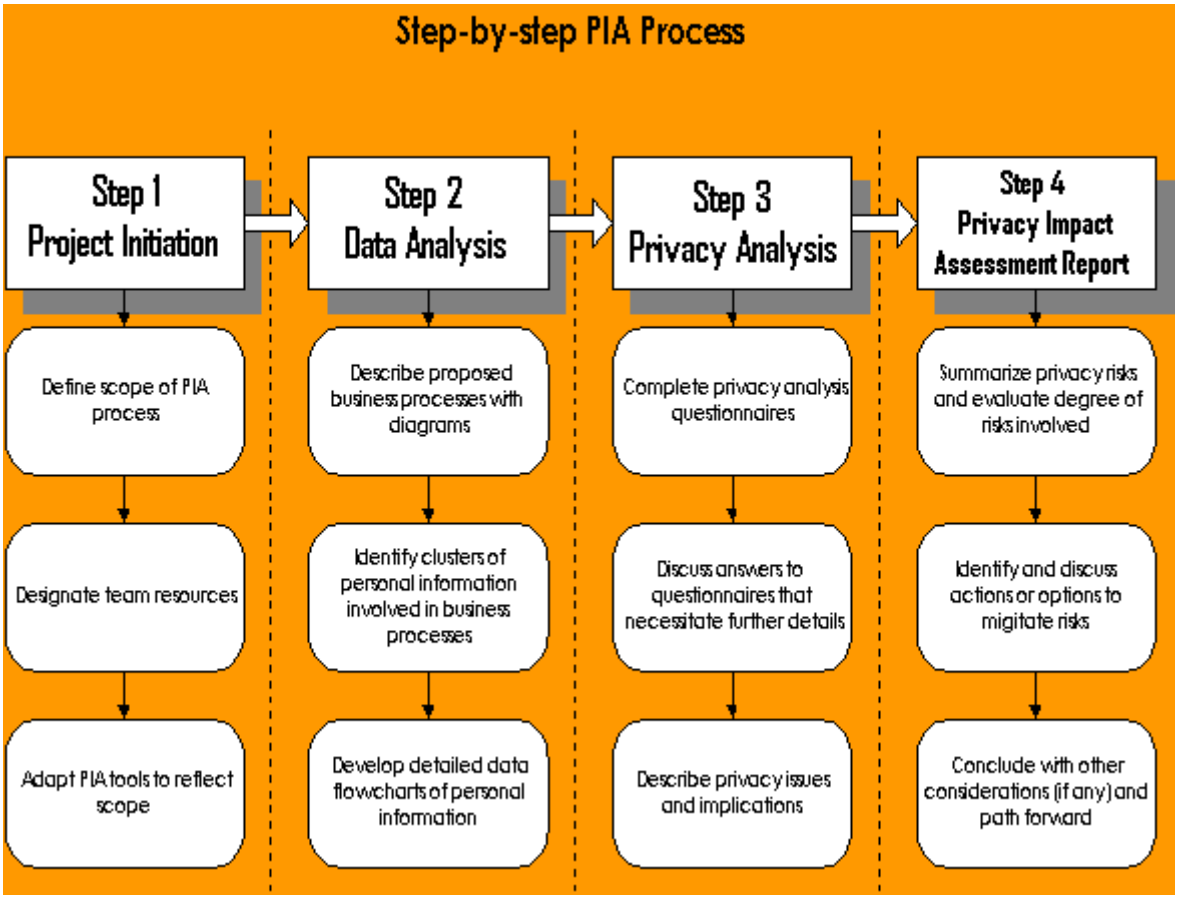
- What personal information is to be handled in the project;
- How the personal information is to be collected;
- How it will be used;
- Internal flows;
- Disclosures;
- Security measures; and
- Any privacy, secrecy and other relevant legislation applying to those flows.

The guidance provided by the Australian Privacy Commissioner is reiterated in the guidelines from the Ontario Data Protection Commissioner with regard to risk managements strategies, or privacy by design. These are taken up in the next section.

3.3 Privacy by Design

The Ontario Information and Privacy Commissioner places emphasis on the management of personal information. Compromising this personal information is argued to cause harm and should be mitigated through a risk management strategy, termed as Privacy Risk Management (PRM).[17] This proactive approach to privacy protection (focused on 'embedded protections' and 'ever present as the default') is also known as 'privacy by design'; a concept developed during the 1990s.[18]

[16] http://www.privacy.gov.au/publications/pia06/index.htm#mozTocId799546
[17] Information and Privacy Commissioner Ontario, Canada (2010) 'Privacy Risk Management: Building Privacy protection into a risk management framework to ensure that privacy risks are managed by default' p.2
[18] Information and Privacy Commissioner Ontario, Canada (2010) 'Privacy Risk Management: Building Privacy protection into a risk management framework to ensure that privacy risks are managed by default' p.3



http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/paipg-pefrld2-eng.asp

The scoreboard reflects the process from project initiation to the privacy impact assessment reports. Although aimed primarily at organisations, this is a useful tool for ADDPRIV in terms of looking at the cycle of data collection and process, leading to an evaluation of risks and issues to consider. The privacy questionnaires provided by the Ontario Data Protection website have been adapted and contribute to the ethical scoreboard.

The Ontario Data Protection guidance states that the 'cyclical nature of the information life cycle must be supported by appropriate policies, practices, procedures, tools and contracts'. With reference to this life cycle of information the guidance states that 'risk must be properly identified, minimized to the extent possible, and appropriately managed where it can't be eliminated' and 'a proper contemplation of the information life cycle includes these concepts'. A Privacy

Impact Assessment is one of the ways that the information life cycle can be managed and privacy risks minimised.[19]

Building on this notion of privacy issues as risks to be managed, the next section of this report looks at privacy frameworks, developed over the last few years by various organisations and data protection institutions. These frameworks go beyond legal compliance to look at broader areas of ethical concern and are therefore important for ADDPRIV in developing a sound ethical framework for developing new surveillance systems.

3.4 Privacy Frameworks

This section of the report outlines three privacy frameworks. These frameworks do not form legislation but are used as a tool for guidance for protecting individual privacy in terms of data collection and storage. They have been utilised in the ADDPRIV project in order to develop further means for addressing the ethics of surveillance systems.

3.4.1 Global Privacy Standard

This was developed in 2005 at the 27th International Data Protection Commissioner's Conference and finalised in 2006 at the 28th International Data Protection Commissioner's Conference. The objective of the Global Privacy Standard is to form a set of universal privacy principles from the various and differing fair information practices around the world.

[19] Information and Privacy Commissioner Ontario, Canada (2010) 'Privacy Risk Management: Building Privacy protection into a risk management framework to ensure that privacy risks are managed by default' p.12

Global Privacy Standard Privacy Principles[20]:

1) **Consent**: The individual's free and specific consent is required for the collection, use or disclosure of personal information, except where otherwise permitted by law. The greater the sensitivity of the data, the clearer and more specific should the quality of the consent be required. Consent may be withdrawn at a later date.

2) **Accountability**: Collection of personal information entails a duty of care for its protection. Responsibility for all privacy related policies and procedures shall be documented and communicated as appropriate, and assigned to a specified individual within the organisation. When transferring personal information to third parties, organisations shall seek equivalent privacy protection through contractual or other means.

3) **Purposes**: An organisation shall specify the purposes for which personal information is collected, used, retained and disclosed, and communicate these purposes to the individual at or before the time the information is collected. Specified purposes should be clear, limited and relevant to the circumstances.

4) **Collection Limitation**: The collection of personal information must be fair, lawful and limited to that which is necessary for the specified purposes.

   i. ***Data Minimization*** – The collection of personal information should be kept to a strict minimum. The design of programs, information technologies, and systems should begin with non-identifiable interactions and transactions as the default. Wherever possible, identifiability, observability, and linkability of personal information should be minimised.

[20] http://www.privacybydesign.ca/content/uploads/2010/06/gps.pdf

5) **Use, Retention, and Disclosure Limitation**: Organisations shall limit the use, retention, and disclosure of personal information to the relevant purposes identified to the individual, except where otherwise required by law. Personal information shall be retained only as long as necessary to fulfil the stated purposes, and then securely destroyed.

6) **Accuracy**: Organisations shall ensure that personal information is as accurate, complete and up to date as is necessary to fulfil the specified purposes.

7) **Security**: Organisations must assume responsibility for the security of personal information throughout its life cycle consistent with the international standards that have been developed by recognised standards development organisations. Personal information shall be protected by reasonable safeguards, appropriate to the sensitivity of the information (including physical, technical and administrative means).

8) **Openness**: Openness and transparency are key to accountability. Information about the policies and practices relating to the management of personal information shall be made readily available to individuals.

9) **Access**: Individuals shall be provided access to their personal information and informed of its uses and disclosures. Individuals shall be able to challenge the accuracy and completeness of the information and have it amended, as appropriate.

10) **Compliance**: Organisations must establish complaint and redress mechanisms, and communicate information about them to the public, including how to access the next level of appeal. Organisations shall

take the necessary steps to monitor, evaluate, and verify compliance with their privacy policies and procedures.

3.4.2 APEC Privacy Framework

The APEC Privacy Framework was published in 2005 and is consistent with the core values of the OECD's 1980 Guideline on the Protection of Privacy and Trans-Border Flows of Personal Data. It was intended that the framework would provide guidance to businesses and APEC economies on privacy issues, and applies to persons or organisations who control the collection, holding, processing, use and transfer of personal data. It is seen as an important tool in encouraging the development of appropriate information privacy protections and ensuring the free flow of information.

The main principles of the framework are as follows:

1. **Preventing Harm**: Recognizing the interests of the individual to legitimate expectations of privacy, personal information protection should be designed to prevent the misuse of such information. Further, acknowledging the risk that harm may result from such misuse of personal information, specific obligations should take account of such risk, and remedial measures should be proportionate to the likelihood and severity of the harm threatened by the collection, use and transfer of personal information.
2. **Notice**: Personal information controllers should provide clear and easily accessible statements about their practices and policies with respect to personal information that should include: a) the fact that personal information is being collected; b) the purposes for which personal information is collected; c) the types of persons or organizations to whom personal information might be disclosed; d) the identity and location of the personal information controller, including information on how to contact them about their practices and handling of personal information; e) the choices and means the personal information controller offers individuals for limiting the use and disclosure of, and for accessing and correcting, their personal information.

3. **Collection Limitation**: The collection of personal information should be limited to information that is relevant to the purposes of collection and any such information should be obtained by lawful and fair means, and where appropriate, with notice to, or consent of, the individual concerned.
4. **Uses of Personal Information**: Personal information collected should be used only to fulfil the purposes of collection and other compatible or related purposes except: a) with the consent of the individual whose personal information is collected; b) when necessary to provide a service or product requested by the individual; or, c) by the authority of law and other legal instruments, proclamations and pronouncements of legal effect.
5. **Choice**: Where appropriate, individuals should be provided with clear, prominent, easily understandable, accessible and affordable mechanisms to exercise choice in relation to the collection, use and disclosure of their personal information. It may not be appropriate for personal information controllers to provide these mechanisms when collecting publicly available information.
6. **Integrity of Personal Information**: Personal information should be accurate, complete and kept up-to-date to the extent necessary for the purposes of use.
7. **Security Safeguards**: Personal information controllers should protect personal information that they hold with appropriate safeguards against risks, such as loss or unauthorized access to personal information, or unauthorized destruction, use, modification or disclosure of information or other misuses. Such safeguards should be proportional to the likelihood and severity of the harm threatened, the sensitivity of the information and the context in which it is held, and should be subject to periodic review and reassessment.
8. **Access and Correction**: Individuals should be able to: a) obtain from the personal information controller confirmation of whether or not the personal information controller holds personal information about them; b) have communicated to them, after having provided sufficient proof of their identity, personal information about them; i. within a reasonable time; ii. at a charge, if any, that is not excessive; iii. in a reasonable manner; iv. in a form that is generally understandable; and, c) challenge the accuracy of information relating to them and, if possible and as

appropriate, have the information rectified, completed, amended or deleted.

9. **Accountability**: A personal information controller should be accountable for complying with measures that give effect to the Principles stated above. When personal information is to be transferred to another person or organization, whether domestically or internationally, the personal information controller should obtain the consent of the individual or exercise due diligence and take reasonable steps to ensure that the recipient person or organization will protect the information consistently with these Principles.

3.4.3 International Security Trust and Privacy Alliance (ISTPA) Framework

The International Security, Trust and Privacy Alliance (ISTPA) is a multinational alliance of businesses and technology providers. The group's objective is to provide unbiased research and evaluation of privacy standards, tools and technologies.

The framework created by the ISTPA, entitled the ISTPA Privacy Framework, has been developed by the non-profit alliance of companies and organisations, as a proactive tool which is able to support businesses and governments in developing and managing their own privacy policies, even in the absence of law or regulation.

The framework is a creation from an extensive analysis of the fundamental composition of information privacy- government data collection requirements, citizen rights, available technologies, privacy principles and fair information policies and other appropriate factors. Access to the framework is available to all current members of ISTPA.

A set of privacy principles defining fair Information Practices (FIP) supported the creation of the ISTPA Privacy Framework, where privacy standards include:

- **Accountability**: Reporting made by the business process and technical systems which implement privacy policies to the individual or entity accountable for ensuring compliance with those policies, with optional linkages to redress and sanction.
- **Notice and awareness**: Information regarding an entity's privacy policies and practices including: definition of the Personal Information collected; its

use (purpose specification); its disclosure to parties within or external to the entity; practices associated with the maintenance and protection of the information; options available to the individual regarding the collector's privacy practices; retention and deletion; changes made to policies or practices; and information provided to the individual at designated times and under designated circumstances

- **Choice and consent:** The capability, including support for Sensitive Information, Informed Consent, Change of Use Consent, and Consequences of Consent Denial, provided to individuals to allow the collection and/or specific uses of some or all of their Personal Information either through an affirmative process (opt-in) or implied (not choosing to opt-out when this option is provided).
- **Access and Correction:** Capability allowing individuals having adequate proof of identity to find out from an entity, or find out and/or to correct or delete, their Personal Information, at reasonable cost, within reasonable time constraints, and with notice of denial of access and options for challenging denial.
- **Disclosure:** The release, transfer, provision of access to, use for new purposes, or divulging in any other manner, Personal Information held by an entity except with notice and consent of the individual; the information collectors policies must be made known to and observed by third parties receiving the information; and sensitive health information disclosures must be managed.
- **Information quality and integrity:** Ensures that information collected and used is adequate for purpose, relevant for purpose, not excessive in relation to the purposes for which it is collected and/or further processed, accurate at time of use, and, where necessary, kept up to date, corrected or destroyed.
- **Anonymity:** A state in which information is rendered anonymous so that the individual is no longer identifiable
- **Enforcement and recourse**: Mechanisms to ensure compliance with privacy policies, agreements and legal requirements and to give individuals a means of filing complaints of compliance violations and having them addressed, including recourse for violations of law, agreements and policies
- **Sensitivity:** Specified information, as defined by law, regulation or policy, which requires specific security controls or special processing.

- **Security/Safeguards:** Policies, practices and controls that ensure the confidentiality, availability and integrity of Personal Information collected, used, communicated, maintained, and stored; and ensure that Personal Information will be destroyed or de-identified as required.
- **Information Flow:** The communication of personal information across geo-political jurisdictions by private or public entities involved in governmental, economic or social activities use.
- **Limitation**: Controls exercised by the information collector or information user to ensure that Personal Information will not be used for purposes other than those specified and accepted by the individual or provided by law, and not maintained longer than necessary for the stated purposes.

3.4.4 Charter for a Democratic Use of Video Surveillance

The Charter for a Democratic Use of Video Surveillance was published by the European Forum for Urban Security in 2010. This Charter was developed with the aim to provide public authorities dealing with video surveillance, a set of principles and recommendations for an appropriate use of video surveillance, respectful of civil liberties and the right to privacy. This Charter is important to take into account in terms of ADDPRIV as it refers specifically to the use of CCTV in public space and moves beyond simply legal compliance to develop a set of principles, which take into account ethical and privacy concerns.

The principles outlined in the Charter are as follows (in brief):

1. The principle of legality: The design and development of video surveillance systems can only be undertaken in compliance with existing laws and regulations.
2. The principle of necessity: The installation of a video surveillance system must be justified. The decision to install a system should be based upon necessity.
3. The principle of proportionality: The design, installation, operation and subsequent development of video surveillance systems must respect a sound and suitable measure.
4. The principle of transparency: Every authority employing a video surveillance system must have a clear and coherent policy regarding the operation of their system.

5.	The principle of accountability: The right to surveillance of public areas is reserved to carefully limited authorities. These authorities are responsible for the systems installed in their name.
6.	The principle of independent oversight: Checks and measures should be put in place to maintain the correct functioning of the video surveillance systems through a process of independent oversight.
7.	The principle of citizen participation: All must be done to encourage citizen involvement at every stage in the video surveillance system's life.

In terms of future plans, the partners involved in the production of the charter call for a European label and certification to be put in place. Furthermore, they support the idea of creating a common language of video surveillance for European citizens that would translate into the creation of a European sign to indicate surveilled zones.

The principles included in this Charter have been adapted as one aspect of the ethics scoreboard. Taken together the three codes suggest specific ways of engaging with the risks posed to privacy by surveillance systems. These include principles of necessity, prevention of harm, accountability, participation (including access and correction) and transparency (including openness, independent oversight and certification). An important aspect of the technology developed in the ADDPRIV project is the focus on building ethics and privacy protection into the surveillance system. The next section of the report builds on these privacy codes and explores the possibility of building protections into technology through Privacy Enhancing Technologies.

3.5 Privacy Enhancing Technologies

This section of the report provides a brief introduction to Privacy Enhancing Technologies (PETs). ADDPRIV has a stated aim to build a new ethical standard into its surveillance technology; questions regarding the need to only collect the information that is necessary and to protect the privacy of individuals to as great an extent as possible, are vital to the success of ADDPRIV.

For the Information Commissioner's Office UK (ICO) the best protection of individual privacy is that "their personal information is only collected where this is

essential".[21] The ICO considers that privacy enhancing technologies (PETs) are not limited to those that provide anonymity (or a degree of anonymity) but also those that protect or enhance an individual's privacy. Including:

- Encrypted biometric access systems that allow the use of a fingerprint to authenticate an individual's identity, but do not retain the actual fingerprint;
- Secure online access for individuals to their own personal data to check its accuracy and make amendments;
- Software that allows browsers to automatically detect the privacy policy of websites and compares it to the preferences expressed by the user, highlighting any clashes; and
- 'sticky' electronic privacy policies that are attached to the information itself preventing it being used in any way that is not compatible with that policy'

In terms of PETS, the ICO states that these help to build trust and signal intention and integrity in relation to the holding of information by a given organisation. They provide potential questions which might be asked in relation to the design of PETS, including:

- Do I need to collect any personal data at all?
- If so, what is the minimum needed?
- Who will have access to which data?
- How can accesses be controlled to allow only those which are for the purposes stated when the data was collected, and then only by those employees and processes that have an essential need?
- Can individuals make total or partial use of the system anonymously?
- How can I help individuals to exercise their rights securely?

The ADDPRIV technology under development will need to take these issues into account. Hence these questions have been incorporated as an aspect of the ethical scoreboard. In order to look at how privacy risk management, codes, principles, designs and technologies have been used by others, the final section of this report will now turn attention to privacy projects that have taken place over the last few years.

[21] Information Commissioner's Office (2007) 'Data Protection Guidance Note: Privacy Enhancing Technologies (PETs)

3.6 Privacy Projects

Over the last few years there have been various projects focused on increasing accountability in terms of data protection, and enhancing privacy rights for citizens. The lessons learnt from these projects are useful for ADDPRIV in developing new standards of ethical protection and attempting to move beyond the legal frameworks utilised currently.

3.6.1 The Accountability Project

The Accountability Project is a three stage project undertaken by the Centre for Information Policy Leadership and facilitated by the office of the Data Protection Commissioner. The purpose of the project was to develop essential, commonly accepted elements required of a company to establish and demonstrate accountability for its information processes. Experts were selected from privacy enforcement agencies, industry and civil society. Meetings convened in three stages:

1) The Galway Project
2) The Paris Project
3) The Madrid Project

<u>The Galway Project</u>

The Galway Project (completed in October 2009) aimed to: define aspects of accountability, to work out how to facilitate accountability as a means to govern and protect information and protect privacy; and to consider how accountability would work in practice. The conclusions from this part of the project were based around the idea of increased complexity: that advances in speed, volume and complexity of data flows across national borders challenge existing models of data protection; and that an accountability based approach could help address these concerns. The Galway Project defined accountability as a requirement that organisations which collect, process and use personal information take responsibility for its protection and use beyond mere legal requirements.

<u>The Paris Project</u>

The Paris Project followed the Galway Project and was completed in October 2010. It asked further questions about accountability such as: How do organisations demonstrate accountability? And how do regulators measure it? The document 'Demonstrating and Measuring Accountability' produced by this project proposed conditions that accountable organisations should be prepared to implement and demonstrate to regulators. The project concluded that accountability has assumed increased prominence in international and national discussions about data protection regimes, and that to be deemed accountable, organisations need to demonstrate and regulators need to measure certain fundamentals. These fundamentals (in brief) are as follows:

1. Policies: The organisation needs to have written data privacy policies that reflect applicable laws, regulations and industry standards. These need to be communicated to individuals. The organisation needs to develop procedures to put these policies into effect in light of the specific circumstances of its own organisations (e.g. what is collected, how it is used and how systems and organisations are connected).
2. Executive oversight: Organisations need to put in place a privacy leader who will be supported by appropriate resources and personnel.
3. Staffing and delegation: Organisations need to ensure that the privacy programme is sufficiently staffed by trained personnel. There should be sufficient staff on the privacy program.
4. Education and awareness: Organisations need to be able to provide up to date education and awareness programmes to keep employees and on site contractors aware of data protection obligations.
5. On-going risk assessment: Organisations need to implement a process to assist them in understanding the risks to privacy raised by new products, services, technologies and business models. Risk assessment is an on-going function.
6. Programme risk assessment oversight and validation: The accountability programme should be reviewed periodically to assess whether it needs modifying.
7. Event management and complaint handling: The accountable organisation needs a procedure for addressing data protection problems when they arise, i.e. misuse.

8. Internal enforcement: Policies must be in place for enforcing internal data protection rules.
9. Redress: Mechanisms need to be put in place whereby individuals may have their complaints heard and resolved.

These fundamentals are important in terms of ADDPRIV due to their concentration on continuous assessment and reassessment of policies, on-going assessment of risks (of which one example is a PIA), and a need for demonstrable awareness of privacy and accountability issues.

The Madrid Project

The Madrid Project meeting was held on the 9th February 2011. Documentation regarding findings is not yet available. The aims of the meeting were as follows:

> To examine the negative and positive incentives that regulators may provide to encourage general and validated accountability.
>
> To explore the full range of validation methods and how each might effectively serve compliance with accountability requirements.
>
> To consider an architecture for validation methods and their application to different data activities.

3.6.2 European Projects

It is also useful for ADDPRIV to be aware of other European projects working in the area of privacy.[22] Some examples include the FESTOS (Foresight of evolving security threats posed by emerging technologies) project, which assesses evolving security threats posed by the abuse or inadequate use of technologies (including nanotechnologies, biotechnologies and information technologies), and attempts to produce ways of preventing threats and security issues; the DETECTER (Detection Technologies, Terrorism, Ethics, and Human Rights) project, which contributes to

[22] The European Commission is currently calling for a revision of the current EU Data Protection Directive to encourage 'privacy by design' and data protection compliance 'embedded throughout the entire lifecycle of technologies and procedures. http://www.edri.org/edrigram/number8.18/ec-strategy-data-protection-directive

work on detection technologies, counter-terrorism, ethics and human rights, and raises ethical questions such as: are significant intrusions into privacy justified by the need to save life or protect democracy? This project argues that counter-terrorism policy in the EU can be made more just if those responsible for formulating it are aware of its ethical implications; and the PrimeLife (Privacy and Identity Management in Europe for Life) project, which aimed to create privacy and identity management for future networks and services by assessing and understanding privacy-enhancing identity management 'for life', thus counteracting the issue of lifelong personal data trails without compromising on function; bringing privacy to the internet and its applications; and creating tools for privacy friendly identity management; and the EGAIS (Ethical GovernAnce of emerging technologies) project, which aims to create guidelines on ethical governance methods that could be applied during Information and Communication Technologies development, consequently stopping or limiting the possibility of ethical issues occurring.

The following three sections provide some further detail on European Projects to gain an idea of the content and processes followed in these projects.

EUROPTA Project

Commencing in March 1998 and completing in December 1999, the EUROPTA project 'Participatory Methods in Technology Assessment and Technology Decision-Making' was conducted on the issue of participatory technology assessment (PTA). The intention of this project was to advance, within a multinational perspective, the knowledge of the role of participation in technology assessment (PTA) by decisively gauging the experiences of various European national participatory initiatives. This project was driven by the lack of applicable theoretical and empirical analysis on PTA. From this, criteria for the feasible implementation of participatory methods at varying decision making levels were determined.

The project strived towards three main objectives:

1) To develop a theoretical and analytical framework on the function of PTA.
2) Compare sixteen participatory arrangements in the countries involved in the project, permitting the study of a vast variety of methods, as well as of comparable projects.
3) Form recommendations about the use of PTA at a national.

The breakdown of the project is outlined in five papers where an analysis of the case studies is made and models for understanding of the function and workings of PTA are presented.

The first paper resulting from this project was entitled *Implementing participatory TA.* The paper proved that PTA methods where suitable for exchange between countries and organizations. The critical objective of all countries involved in the project was to identify what the function of public participation in policy analysis and technology assessment would be.

The second and most relevant paper *Project Management- a matter of ethics and robust decision* declares that effective management should follow *discourse* ethical rules.

Discourse ethics were described as the "social ideal" and gained high credibility and trust when used. Examples of discourse ethics processes features include:

1. Equal empowerment of participants (equality)
2. Being based on truthful, proper information (enlightenment)
3. Fair in relation to interpersonal relations (fair)
4. Rules of communication is known and accepted by all parties (transparency)
5. All parties are invited into dialogue (legitimacy)
6. Restrictions to scope of view points kept to a minimum. (open minded)
7. Processes are self-documenting, and striving to be communicative, so that the need for interpretations are kept at a minimum (authentic)

It states that the credibility of a debate is closely related to the ethical quality of the debate and the impact of the technology assessment (TA) is closely related to its creditability. The paper also acknowledges difficulties in PTA are frequently due to managerial problems that arise from poor ethical standards.

The third paper was *The choice of PTA methods related to institutional and problem setting*. It suggests that the selection and objectives of the method of PTA are connected to the problem and to institutional motivation. Two types of PTA were prominent; the expert-stakeholder PTA was deemed suitable when technical issues were the problem and public-PTA was suitable when ethical or moral issues were debated.

The fourth paper *The Role of PTA in the Policy-Making Process* examines several potential political roles PTA may play. Many of the case studies had weak political functions.

The fifth paper was "*The Impacts of PTA on its societal environment".* The paper evaluates that the state of public and political debate are important factors for the success of PTA in relations and negotiations.

More generally in the project it was noted various ways of 'assessing' related social issues of technology, including evaluating public opinions on immerging technology and resolving conflicts between public and shareholders. Through participation, in methods of debate and scenario workshops, public understanding of PTA can aid to social interaction with shareholders.

The project observed that credibility of experts and stakeholders is required for successful PTA. Credibility was found to feed trust to the public and thus add to the experience of TA. It was found also that PTA was defined by social and cultural ideologies of the people involved. Development of communication procedures and associated 'best practice' of methods of PTA between concerned parties was recognised as another requirement to aid PTA. These ideas have been used to develop the ADDPRIV ethical scoreboard and to start thinking about participatory forms of public accountability for the surveillance system.

SIAM Project

This project aims to widen the decision making process of the end user (e.g. transport sector including aviation, rail networks and public transport) on how to invest into security measures and technologies through conflicting perspectives e.g. privacy concerns and ethical dilemmas. As policy and decision makers must take numerous aspects into consideration from scientific to cultural interests, the SIAM project will provide a structured decision support system with guidelines, a data

base, analysis of security technology, SIAM methodology handbook and threat and impact analysis. The project will provide security assessments that will concurrently avoid infringing the freedoms of European citizens. SIAM aims to transfer the required information in a prepared manner to the decision maker. The experimental basis for this is produced by involving four case studies (London underground; Metro of Turin, Italy; Ben-Gurion Airport Tel Aviv, Israel; Berlin Brandenburg International Airport) for the development of the decision support system, with methodologies ranging from concepts of freedom infringements, definition of threat scenarios, examination of future security technologies and classifying due their functionalities and limits and analysis of legal frameworks and regulatory techniques. This project runs from March 2011 – March 2014 and aims to provide a decision support system for security technologies via its outputs of a decision support system and database, a security technologies analysis, and a threat and impact analysis.

ETICA Project

The ETICA project is a project on the Ethical Issues of Emerging ICT Applications, funded by the European Commission under the seventh framework Programme. It was started April 2009 and completed in May 2011. The main objective of the project was to identify ethical issues of new emerging technologies and their possible use in areas where ethical issues could arise from. The objectives of the project were to understand the capabilities and limits of emerging technologies and identify ethical issues related to the emerging technology and finally prevent such issues arising or determine ways to deliver quick solutions when ethical issues do arise. This also included providing recommendations to policy makers.

Recommendations for policy makers include providing a regulatory framework to promote ethics in new ICTs, suitable tools and methods to identify ethical issues and tackle them and permit ICT personnel to use their knowledge to support strategies into ethical issues. A framework based on "Ethical Impact Assessment for ICTs" was promoted in order to address issues of privacy and equality and to connect with issues of responsibility in emerging ICTs.

3.6 Summary

This background report to the ethical aspects of the ADDPRIV project, designed to feed into the development of the ethical scoreboard, has worked in two main sections. These comprise legal compliance and ethical compliance. The two sections will briefly be summarised in turn.

3.6.1 Legal Compliance

The ADDPRIV project needs to demonstrate that it complies with national and international legislation in the area of data protection (prior to moving beyond legal compliance to the ethics of surveillance systems). According to the legislation covered in the background report, the following are the main principles of data protection legislation that a system must comply with:

1) Identifying purposes
2) Openness
3) Limiting collection
4) Limiting use
5) Accuracy
6) Safeguards
7) Individual access
8) Challenging compliance
9) Storage, disclosure and retention

3.6.2 Ethical Compliance

Although many of the same principles are found in the privacy principles and guidelines as those found in the data protection legislation, there are a few key differences, which must be taken into account when developing an ethical framework for a new surveillance technology. Alongside the similar principles of: collection limitation and data minimization, accuracy of data, storage and security, openness, access, and compliance, are the key privacy principles of: consent, preventing harm, choice, and use, retention and disclosure, accountability, education, oversight, certification, openness, participation, correction, on-going assessment, mapping information flows and assessing risks to privacy. The

prevention of harm is a prevailing idea in privacy literature (as far back as John Stuart Mill's work *On Liberty* (1859)). The idea of consent is also a major issue in the privacy literature – to provide consent as a data subject is to minimise privacy intrusion (this is a key question for ADDPRIV – is it possible to obtain consent from individuals under a video surveillance system?). Providing data subjects with choice over the uses to which their individual information is put also provides a form of protection in terms of privacy, as well as an enhanced accountability in terms of the data collector. Finally, guidelines surrounding the possible uses to which data is put (and limitations on its retention and disclosure) provide a greater protection to the individual data subject, as well as (once again) a form of accountability in terms of the data collector. This is a key issue for ADDPRIV as the project seeks not only to limit the unnecessary collection of data but to ensure a secure storage and deletion of information.

The Ethical Scoreboard

The ethical scoreboard moves beyond the legal compliance presented in the first part of this report to also incorporate issues of ethical concern. The ethical issues and questions have been compiled in the scoreboard from the various privacy frameworks, such as Privacy Impact Assessments, privacy projects, privacy questionnaires, and privacy guidelines. Alongside the main ethical questions, which have been derived from the privacy documents in this report, the issue of deletion has also been included in the scoreboard. This ethical issue is not found in the privacy documentation but is of particular relevance to ADDPRIV (this point will be developed further in the list below).

The main ethical questions to arise from these privacy documents are as follows and are included as headings in the scoreboard:

- **Data Collection**: This is an important issue for ADDPRIV due to its focus on minimising the amount of unnecessary data collected from individuals.
- **Use**: This ethical issue needs to be taken into account for ADDPRIV as the information collected by the video surveillance systems being developed will potentially be required by a number of authorities (due to the use of the technology in major transport hubs and public space).

- **Communication/Compliance**: This is an important issue for ADDPRIV and one that requires careful consideration. Due to the nature of video surveillance systems in open public space it is difficult to obtain consent from surveilled individuals (prior to their data being collected). Is the notion of obtaining consent a requirement of an ethical surveillance system, and can ADDPRIV comply with this?
- **Deletion**: This is of particular importance to the ADDPRIV project due to its focus on the deletion of unnecessary data (that which is not relevant from a security perspective).
- **Results**: The issue of results is of particular importance for the ADDPRIV project due to its focus on the possibility of enhancing privacy through providing alerts to human controllers at the outset. Questions arise such as: is there an acceptable level of false positives? At what level do false positives produce an unacceptable level of privacy intrusion?
- **Storage**: This is an important issue for ADDPRIV due to its focus on reducing the amount of data stored. Any data which is stored needs to be securely stored and utilised as soon as possible.
- **Accountability**: This is an important issue for ADDPRIV due to its focus on enhancing citizens' rights in terms of privacy. The issue of accountability is of particular importance when developing new technological systems. Privacy frameworks stipulate the importance of accountability and enhancing citizen involvement in relation to data collection systems. In terms of developing a sound ethical framework, ADDPRIV therefore needs to take into account questions arising around the nature of accountability, and the possibility for public participation in the development of the system.

4. Legal Compliance Scoreboard

The principles in the table below, as well as the legal requirements and questions which follow have been compiled from the various countries national legislation involved in the ADDPRIV project. The EU legislation covering data protection has also been included.

Principle	Legal Compliance	Question
Identifying purposes	Data controller	Who is the data controller?
	Public interest	Defined/not defined? Does this fit appropriate national legislation?
	Clear purpose	Is the purpose of data collection clearly defined?
Openness	Purpose communicated	Communicated/not communicated
Limiting collection	Proportionate application	Proportionate/disproportionate? (Is the collection of data necessary and proportionate to what it seeks to achieve)
	Subsidiary basis	Other means available?
	Minimum intervention	Data only collected for a specific purpose?
	Technological capabilities (proportionate)	Zoom? (Is the zoom function necessary?)Freeze function? (Is the freeze function necessary?)Biometrics? (Is biometric information collected? Is this necessary?)
Limiting use		Is data only used for the specified purpose?
	Private space	Is there an intrusion into private space? Is this

Principle	Legal Compliance	Question
		necessary? Technical remedies?
Accuracy	Accurate and kept up to date	Tested for accuracy? Option for individual to challenge accuracy? Data kept up to date?
Safeguards	Technical measures Organisational measures (physical and administrative)	Security measures in place for access to the control room? Access restrictions? Additional measures?
Storage	Period of data retention	Maximum period of data retention in place?
	Secure	Is data stored securely?
Disclosure	Data transfer/copy to third party	Is the data transferred/copied to a third party? Is there a data transfer/copying policy? Is it for commercial purposes? Is it for legal process? Does the transfer contravene the limiting use principle?

Principle	Legal Compliance	Question
	Access to data within the setting	Access control policy? Data adheres to limiting use principle?
Individual access	Right of access	Stored in a way to allow right of access to be exercised?
Challenging compliance	Right to challenge	Individuals have the right to challenge compliance? Individuals notified of existence of procedure to challenge compliance?

The above table outlines the legal aspects that a CCTV system must comply with across the UK, Poland, Italy and Spain; incorporating both national and international legislation. The next section of this document moves beyond legal compliance to attempt to develop new ethical standards for surveillance systems in relation to the technology developments proposed within ADDPRIV.

5. Ethical Compliance Scoreboard

The initial questions within the scoreboard are colour-coded along a traffic light system. A green light highlights little ethical concern or that concerns have been addressed; an orange light highlights some ethical concern to be managed, and a red light highlights an area of major ethical concern that requires attention.

Principles	Questions for analysis		Notes
Risk Assessment	Is there an ongoing risk assessment in place?		Have data flows been mapped? Have risks been identified? Have strategies been put in place for risk management? Will this management be ongoing?
Data Collection	Authority to collect personal information?	Yes/No	What is your authority to collect personal information?
	Other means available?	Yes/No	
	Are the goals valid?	Yes/No	
	Does the information cross borders?	Yes/No	What controls are in place? If personal information crosses borders/used for a secondary purpose,

Principles	Questions for analysis		Notes
			is consent required? Is there interconnection to other systems that read the footage? Is there interconnection to other databases?
	Is there a principle of minimisation in place?	Yes/No	Have all options to minimise the routine collection of data been considered?
	Are images pre-loaded?	Yes/No	
	Are there community goals set out (i.e. Does the system benefit the community?)	Yes/No	
	Is there a principle of avoidance of harm in place?	Yes/No	
	Does the system impact on third parties (i.e. not the data subject)?	Yes/No	
Use	Authority to use personal information?	Yes/No	What is your authority to use personal information?
	Are the uses of the information limited?	Yes/No	Are the uses of the information limited to what a reasonable person might consider appropriate in the

Principles	Questions for analysis		Notes
			circumstances?
	Are processes automated?	Yes/No	Is human intervention and decision making circumvented?
	Are there problems with on-going use of images?	Yes/No	Once identified, are 'suspicious' individuals subject to long-term tracking? Are 'suspicious' individuals' images passed onto other security organisations?
	Do uses of the system change over time?	Yes/No	Is there a policy to prevent function creep? Is the policy effective?
	Are there commercial spin offs?	Yes/No	Is this scoreboard retained for commercial spin offs?
Communication/ Compliance	Has the data subject provided consent?	Yes/No	Is there a policy that defines consent? Is consent obtained directly from the individual? (If not, why not?) How has consent been obtained? Does consent

Principles	Questions for analysis		Notes
			require an action by the individual, rather than being assumed as the default? Is there a right to refuse data collection in place?
Principles	**Questions for analysis**		**Notes**
	Is there a right to challenge in place?	Yes/No	
	Is there covert surveillance taking place?	Yes/No	Any covert surveillance is not acceptable under an ethical system
Deletion	Is the obsolete data deleted immediately?	Yes/No	Immediately After 24 hours After 48 hours Kept up to 7 days Kept for longer than 7 days
	What is meant by deletion?		Password protected deleted data? Data removed from the system? Has the route changed? Is it more difficult to get access to the data?
	Are different types of images treated differently?		Are different types of images kept for longer? Are stored images

Principles	Questions for analysis		Notes
			reviewed for deletion? If so, when, and by whom? Are images from different spaces treated differently?
Results	Is data authenticated?		Are there technical or organisational measures in place to ensure authenticity of data?
	False positives? People Objects Actions Route reconstruction	Yes/No	What is an acceptable level of false positives? 0.98 (This is the i-Lids benchmark)[23]
	False negatives People Objects Actions Route reconstruction	Yes/No	What is an acceptable rate of false negatives? 0.98 (This is the i-Lids benchmark)[24]
	What is the level of certainty for: Individuals? Objects? Groups?		What is an acceptable level of uncertainty? What is acceptable in terms of third party association (i.e. a non-suspicious individual becomes potentially

[23] I-Lids is the UK government's benchmark for video based detection systems. http://tna.europarchive.org/20100413151426/scienceandresearch.homeoffice.gov.uk/hosdb/cctv-imaging-technology/i-lids/index.html

[24] A rate of 0.98 means that 1 in 50 events would be missed, with 1 in 50 alarms being false.

Principles	Questions for analysis		Notes
			suspicious)?
	How many alerts are there per hour?		What is a manageable number of alerts per hour? What is an acceptable number of alerts per hour?
Storage	Is the data encrypted?	Yes/No	
	Are there levels of access in place?	Yes/No	What is the process by which individuals are authorized to access the system? Password protected? What are the points of access? Is access set to a particular individual? Is access set to a particular action?
	Is there data loss?	Yes/No	Percentage of data loss that is acceptable? 0% 15% 30% 45%
Accountability	Is there a principle of transparency in place?		Is this principle reviewed? How often and by whom?
	Are there signs to indicate presence	Present/absent?	

Principles	Questions for analysis		Notes
	of cameras?	Clearly positioned?	
	Is the controller held to account?	Licensed?	Does the licensing body provide oversight in terms of enforcement?
	Are there contact details provided?	Present/absent? Clearly positioned?	
	What is the positioning of the cameras?	Covert/open?	
	Accountability to the public? Is there anything that moves beyond 'normal engagement'?		Website Twitter Facebook Rfid Mobile phone app.
	Accountability of the system – is there a system in place?		Who oversees the system? (i.e. data protection officers in each country)? Are the operatives held to account? Will there be a lay oversight committee? Will there be independent oversight and certification?
	Is there reflexivity in terms of the system (internal)?		Will there be a CPO responsible for and accountable to on-going running of privacy risk

Principles	Questions for analysis		Notes
			management? Will there be education initiatives? Is there a process for correction of error or redress?