Report assessing the likely impact of this system on end user organisations

Deliverable 6.2

Trinity College Dublin
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

D6.2 – Report assessing the likely impact of this system on end user organisations

Due date of deliverable: 31 03 2014
Actual submission date: 07 03 2014

Start of project: 01 February 2011
Duration: 36 Months

Lead Contractor for this deliverable: [Goldsmith College]
### Project co-funded by the European Commission within the Seventh Framework Programme

<table>
<thead>
<tr>
<th>Dissemination level</th>
<th>Public</th>
<th>Confidential, only for members of the consortium (including the Commission Services)</th>
</tr>
</thead>
<tbody>
<tr>
<td>PU</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>CO</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Revision History

Deliverable Administration and summary

<table>
<thead>
<tr>
<th>Project Acronym: ADDPRIV</th>
<th>Grant Agreement no: 261653</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Document Identifier</strong>: D6 2_Final</td>
<td></td>
</tr>
</tbody>
</table>

Leading partner:

Report version: 02

Report preparation date: 07/03/2014

Classification: [classification]

**Nature**: [nature]

**Author(s) and contributors**: Trinity College Dublin, Goldsmiths College London

<table>
<thead>
<tr>
<th>Status</th>
<th>Plan</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Draft</td>
</tr>
<tr>
<td></td>
<td>Working</td>
</tr>
<tr>
<td>X</td>
<td>Final</td>
</tr>
<tr>
<td></td>
<td>Submitted</td>
</tr>
<tr>
<td></td>
<td>Approved</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Date</th>
<th>Edited by</th>
<th>Status</th>
<th>Changes made</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Copyright

This report is © ADDPRIV Consortium 2011. Its duplication is allowed only in the integral form for anyone’s personal use for the purposes of research and education.
Citation

Trinity College Dublin, Goldsmith’s College London, (2014). Deliverable 6.2 – Report assessing the likely impact of this system on end user organisations. 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), Goldsmiths, University of London (GOLD), Avanzit Tecnologia, S.L. (AVANZIT), Hewlett Packard Italiana Srl (HP), Societá Per Azioni Esercizi Aeroportuali Sea SPA (SEA), Renfe Operadora (RENFIE) 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
1 Table of contents

Revision History ............................................................................................................. 4
Acknowledgements .......................................................................................................... 6
1 Introduction .................................................................................................................... 9
2 Current Organisation Practices .................................................................................... 11
  2.1 Interviews ................................................................................................................. 11
  2.2 Outcomes of SEA interviews ..................................................................................... 14
    2.2.1 Current Situation and Policies .............................................................................. 14
    2.2.2 Training ............................................................................................................... 17
    2.2.3 Incidents .............................................................................................................. 17
    2.2.4 Review and Accountability Procedures ............................................................. 18
    2.2.5 Suggested Improvements .................................................................................... 20
  2.3 Outcomes of Renfe Interviews ................................................................................. 21
    2.3.1 Current Situation and Policies .............................................................................. 21
    2.3.2 Training ............................................................................................................... 26
    2.3.3 Incidents .............................................................................................................. 26
    2.3.4 Review and Accountability Procedures ............................................................. 27
    2.3.5 Suggested Improvements .................................................................................... 30
3 End User Demonstrations and Feedback ..................................................................... 31
  3.1 System Interface ....................................................................................................... 31
    3.1.1 Sign In screen .................................................................................................... 31
    3.1.2 Event List screen .............................................................................................. 32
    3.1.3 Filtering of events ............................................................................................. 34
    3.1.4 Reviewing / Editing of Events ......................................................................... 34
3.1.5 User Management Menu ................................................................. 36

3.2 1st Demonstrations: SEA ................................................................. 36

3.2.1 Feedback on ADDPRIV System ....................................................... 36

3.3 Discussion with the End Users’ Advisory Board ................................. 42

3.4 2nd Demonstrations: Renfe ............................................................... 45

3.4.1 System Interface ............................................................................. 45

3.4.2 Operation of System ....................................................................... 47

4 Potential End Users ............................................................................. 53

4.1 Introduction ....................................................................................... 53

4.2 Methodology ..................................................................................... 53

4.3 Results .............................................................................................. 56

4.3.1 Interviews ..................................................................................... 56

4.3.2 Workshops .................................................................................... 69

5 Discussion and Conclusions ................................................................ 72

5.1 Summary of End User Organisations Feedback ................................. 72

5.2 Summary of Potential End Users Feedback ........................................ 79

5.3 Concluding remarks ......................................................................... 80

6 References ......................................................................................... 81
1 Introduction

The aim of the ADDPRIV project is to develop a system for use in CCTV networks which would reduce the impact of those networks on the privacy of individuals whose images are captured in surveillance footage. The project solution aspires to achieve this by detecting events which are relevant to security and mark all related footage. ADDPRIV makes use of a route reconstruction component to assemble footage which contains the subject or object of interest. Once the operator confirms whether or not marked footage is relevant to security, the footage that is irrelevant to security can be deleted, thereby reducing the amount of footage that is retained.

There are many issues to be considered when conducting research into any type of CCTV. Research such as that conducted by, for example, Norris and Armstrong (1999a, 1999b), and Neyland (2006) has contributed to the discourse on privacy and CCTV in society; while others, such as Agustina and Galdon Clavell (2011) and Coudert (2009, 2010), have studied the issues from the perspective of the law. The ethical and legal implications of the implementation of the ADDPRIV system have been investigated and reported on in Deliverables 6.1 (Goldsmith's College, 2013) and 6.3 (Goldsmith's College, 2014) of this project.

The purpose of this report is to investigate the practical implications of implementing the ADDPRIV solution in a transport end user organisation. The end users represented on the project consortium are Renfe Operadora, Spain and SEA Aeroporti di Milano, Italy. The ADDPRIV system was installed in Linate Airport, Milan, in order to test it in real life scenarios. The results of the tests are detailed in Deliverable 5.4 (HP, 2013). The research conducted for this report sought to analyse how the end user organisations currently use CCTV technology as part of their operations and what the roles of the CCTV operators are. Once the ADDPRIV prototype was operational, the system was demonstrated to personnel from both organisations. Their feedback was sought on how, or if, they thought the system could be implemented in their organisation, and what adjustments may be necessary both to the system and within the organisation itself if the ADDPRIV system were to be implemented successfully.
Section 2 of this report explains the information gathered from the two end user organisations, SEA and Renfe, by researchers from Trinity College Dublin about the current working practices within each organisation. Section 3 details the system interface and the demonstrations conducted to gather feedback on the ADDPRIV system from personnel within the organisations. The discussion of the system at the final meeting of the End Users’ Advisory Board is also included in this section. Interviews and workshops conducted with potential end users from outside the consortium by researchers from Goldsmith’s College London are then summarised in Section 4. Finally, the results of the feedback from both consortium members and potential end users are summarised and discussed in Section 5, where the resulting conclusions for the work are drawn.
2 Current Organisation Practices

During the integration phase of the ADDPRIV project, demonstrations of the technology were conducted for employees of the two end user organisations to gather their feedback on how the system would integrate with their jobs, and the responsibilities the organisations have. In order to be able to gauge what impact the introduction of the ADDPRIV technology would have on the organisational practices of the end users, and vice versa, it was necessary first to gather information on how the organisations currently operate. This section explains the procedure by which the information was collected and the results obtained.

2.1 Interviews

The information was mainly collected through interviews with security personnel in the organisations. The main standards on which the questions are based are referenced in the text, to explain the reasoning behind seeking the data. The main documents used for guidance in terms of data collection within the organisations were the ‘Data Protection Audit Resource’ of the Irish Data Protection Commissioner (DPC) (2009), the Closed Circuit Television (CCTV). Management and Operation Code of practice of the British Standards Institution (BSI) (2009) and the ‘International Standards on the Protection of Personal Data and Privacy - The Madrid Resolution’ (Spanish Data Protection Agency (coordinators) and Working group, 2009). The relevant Data Protection authorities of Italy, Spain and Ireland were members of the working group which developed ‘The Madrid Resolution’.

The questions used in the interviews focused on several aspects of the operations of the control rooms. Each topic explored is explained below.

Current situation

These questions were aimed at establishing the current working practices in the organisations where the implementation will take place. It is required in order that a complete background picture can be determined before the technology is put in place.
**Training**

The purpose of this section was to ascertain what the current training policies within the organisation are. It will then be possible to discern if there will be changes required in the training policies to accommodate the new technology. The BSI Code of Practice (British Standards Institution, 2009) includes the following proviso regarding training of employees for CCTV systems:

> “Good training is essential to achieve effective and proper use of CCTV. When a potential incident occurs, the operator has to be able to react, to monitor the event accurately and not lose information that could be pertinent to any future investigation.”

These questions were also intended to identify any potential overlap between the operators’ roles and the intended functionality of the ADDPRIV technology. From the current working practices identified through the interviews, it should be possible to determine if additional training will be required by the operators in the end user organisations, if ADDPRIV is to be implemented. While training on new equipment would be expected, if the ADDPRIV system also introduces any changes to the working practices of the operators, then a new type of training for the new tasks or responsibilities may be necessary. Training is also important from the perspective of data protection and privacy. The Data Protection Commissioner (Ireland) (2009) require information on staff training as part of the audit questions included in the audit resource document and recommends the use of the report resulting from an audit as a “training aid”. In addition to this, ‘The Madrid Resolution’ (Spanish DPA et al) (2009) advocates

> “The periodic implementation of training, education and awareness programs among the members of the organization aimed at better understanding of the applicable laws on the protection of privacy with regard to the processing of personal data, as well as the procedures established by the organization for that purpose”

**Data Protection Policies and Accountability Procedures**

The companies’ policies regarding privacy and data protection are an important part of ensuring robust data protection. The interviewees were asked about the security and
privacy policies within the company, such as employee access to video footage and other databases. It was intended to identify any potential for privacy infringement within the company policy. The questions were mostly based on the practices discussed or suggested in the documents of the BSI (2009) and the Data Protection Authorities (Irish DPC, 2009, Spanish DPA et al, 2009)(2009, 2009).

It is important that companies have procedures which track access to, or dissemination of, data in their systems. Accountability for actions taken with regard to the data is an important consideration for the protection of the data. Various methods are mentioned in the BSI (2009) and DPC (Ireland) (2009) documents, while ‘The Madrid Resolution’ contains an “accountability principal” (2009). Regarding this and the earlier reference to training, Urbaneye, an FP5 project which studied the growing employment of CCTV, and its implications, in various public spheres, had also previously concluded that “official policies, accountable management and operator training are important” (Hempel and Töpfer, 2004).

**Review**

The review of procedures is important to ensure their effectiveness and detect any potential problems or data breaches within the system. Various methods of review are mentioned in the BSI (2009) and the Irish DPC (2009) documents, including, for example, random audits of the logs as part of an independent audit (BSI, 2009), and questions on reviews being conducted for security, or by a “co-ordinator of data-protection” (Irish DPC, 2009), while ‘The Madrid Resolution’ (Spanish DPA et al, 2009) refers to codes of practice which have “elements that allow the measurement of efficiency as far as compliance and level of protection of personal data are concerned”.

**Incidents**

Questions were asked regarding the role of control rooms in any incidents detected, with a view to investigating the applicability of ADDPRIV and also to inform any future development of the technology beyond the current validation scenarios. This will help to determine how well the ADDPRIV technology could integrate with, or augment the
control room procedures and, in turn, how the technology and procedures could be improved for future users.

### 2.2 Outcomes of SEA interviews

This section describes the results of the pre-implementation interviews conducted with the two end user organisations. The descriptions in this section of the working practices of the organisations are based on the responses received. Interviews were conducted with five members of the security team in SEA, two in supervisor or manager roles, two operators and one security guard. The interviews were carried out in September 2012.

#### 2.2.1 Current Situation and Policies

In the SEA control room, the operators’ primary concern is safety within the airport, as opposed to security, which is dealt with by the police. The police have access to the same cameras as the control room operators, and more. The control room operators have no control over the cameras (Pan, Tilt, and Zoom); they only see the images from them, while the police department can control the position of some cameras. The SEA control room has two large screens displaying the camera images. All of the footage from the cameras to which SEA have access is displayed. The screen is split to show all the camera feeds, to which SEA have access, at once. The position on the screen cannot be changed by the control room operators. They can request the IT department to make changes if necessary, however, one respondent remarked that, for the purposes for which SEA require the CCTV in this control room, the current set up is sufficient. The main purpose of the CCTV monitoring in the control room is to detect “when the queue is growing”. Another respondent described the CCTV system in the control room as:

“They are doing passive monitoring, there is nothing indicating that on one of those cameras there is some baggage unattended so they can start the procedure. The procedure starts only when they receive a call…In some cases they can ask for the security guard to go and check if they can identify unattended luggage”.

Apart from the monitoring of queues in the departures area of the airport, the responsibilities of the control room operators involve responding to the requests and alerts received in the control room through various means, coordinating with the police control room in the case of an emergency and the issuing of temporary identification badges for visitors. In the case of an emergency, if, for example, technicians or mechanics require access to a restricted area, then the operators issue them with the requisite visitor badge.

“… they are the front line to react if an emergency occurs... no matter if they are seeing the crew that is going to be directed on the field or they are receiving a call from the police or from any other entities, airport authorities…”

The operators handle requests from aircraft, for example if the loading or unloading of cargo requires supervision; valuables need to be escorted, or a particular aircraft requires a security guard. The operators are in contact with the airside manager to ensure all such requirements are fulfilled. However, the actual airside activity that is the subject of the request is not managed by the control room. If the operators observe a queue developing in the departures area, they also contact the relevant person in charge.

Regarding the safety of the airport, the control room is where the safety systems are based. These systems include the anti-fire systems, the emergency phones from the escalators and elevators, the emergency buttons in the elevators and the TAMTAM, which is a system used to connect all entities in the airport who are involved in an emergency situation. If it starts ringing, the control room operators “know exactly who has to be contacted and if it is an exercise or if it is a real incident”.

The video footage from the cameras is retained in a digital recording system for one week. It is then deleted automatically, unless it is being used in an investigation or is the subject of a request by the authorities. In such cases the relevant footage is extracted from the system and stored separately, and the one week time limit does not apply. Figure 1 contains a summary of the activities of the SEA control room.
Figure 1 Summary of SEA control room activities

 SEA Control

- Contacting relevant person in charge
- Crowd control / Monitoring of queues
- Issuing of temporary ID badges
- Monitoring access gates (eg if opened without ID badge or left open) - Anti-intrusion system not directly managed by control room (managed by police/customs)
- Responding to requests for attendance airside
- Responding to requests for attendance airside
- Contact police in case of receiving security information from airport
- Public safety
- First line / fields calls in case of emergency

- Cameras:
  - Departure areas
  - Some airside
  - Elevators (safety)

- Alarm systems:
  - Escalators
  - Elevators
  - Emergency phones
  - Anti-fire system
  - Anti-intrusion
  - Tam-Tam

- Other:
  - Phone calls
  - Email
  - ID badge requests
2.2.2 Training

The SEA control room operators are provided with training in relation to the operation of the systems installed in the control room. They receive training in both the technical operation of the control room systems and the response procedures for the different alerts they may receive. They learn about the access control system for the CCTV (into which all the CCTV systems and the system monitoring the emergency gates are connected). Retraining occurs when new technology is installed. While they can report what they observe, if they observe something suspicious; it is not part of their training because their main tasks are crowd control and responding to any emergency alarm received in the control room. Retraining occurs on the job, or if there is new equipment introduced into the control room. There is also training for everyone working in the airport in how to react in an emergency, ensuring that the correct information is relayed to all parties in the case of an emergency, and evacuation, to which the control room are “the front line to react”.

Regarding access management, a policy has also been distributed to the company by the IT department, not only in relation to security, but also regarding the correct use of the systems and their passwords. This is a general policy relating to the correct use of all databases and systems.

2.2.3 Incidents

As previously mentioned, one of the principal priorities for the control room is crowd control; the main thing the SEA control room operators monitor on the CCTV is the build-up of queues of passengers, in the departures area, which is open from 4:30am to 10:30pm. The control room is the central point for all the safety alarm systems in the airport, including anti fire. There are also cameras inside the elevators for safety reasons. The CCTV system in the control room does not have any automated event detection.
In an event that the control room operators receive an alarm or notification of some incident (for example if a security guard sees abandoned luggage and contacts the control room), the operators follow procedure and contact the airport police. It is also possible that they could receive information by phone or email from another source, in which case the operators will also contact the police. When the operators call the police to a situation, they also call the SEA security personnel to attend. In the case of a piece of abandoned luggage, once the security threat has been dealt with, the customs officials will also be involved.

The primary mode of communication with the police is by phone. The police are guaranteed to respond in the case of being alerted or contacted by an operator from the SEA control room. The operators first call their person in charge, who will contact the police. This establishes a link between the police and the control room. They could also receive information from the operations department, in which case the control room contact the police.

There are no criteria by which a reaction to an incident is measured as being successful. If there is an incident, the police report back that they have “checked the situation”. If there is no incident the police will not call, “in the case of security the police has the priority in acting”. In some cases, if SEA requests it, the police will provide feedback after an incident.

### 2.2.4 Review and Accountability Procedures

The police are the only ones who review the video footage. The control room operators are not entitled to do this. The operators have access to the ID badge database to issue temporary ID badges, but they do not have access to any sensitive information or the archived video footage. The operators are monitoring the CCTV footage in real time only and are being supervised.

In the case of an incident occurring, in general, they produce a report themselves, without collaboration with others. However, depending on the emergency or the incident in question, the operators can ask for a copy of the police report, or vice-versa.
“so they can match all the things and complete their reports”. There is one report of the office activities completed for the entire office. Each operator does not complete their own version and the entries in the report are anonymous. However, the time of the entry will give an indication of who was on duty in the control room when it was made. The report is a pre-set paper form, which they must complete. The information recorded in the log is related to all the activities carried out on a certain date. For example, the escorting of valuables, or diplomatic materials, hazardous (radioactive) cargo; flights and risk control, any security checks conducted; escorting baggage from the Bag Holding System (BHS) to the aircraft; x-raying of goods for the airport which are for storage inside the terminal; escorting of ammunition; patrols of the airport and any type of interventions, such as in the case of abandoned luggage or a spillage.

In terms of accessing the ID badge database, each operator has a password for accessing the database and the security manager can check the use of the database. There is no procedure in place in the security department to detect data breaches; this is managed by the IT department. The security manager also reviews the surveillance logs; “access to the access control system, the system for the alarms,… the elevators,… escalators” are reviewed.

The control room systems are reviewed with regard to the airport’s requirements and the needs of the “airport operators”. For example, in the case that another department requests the addition of a camera to the system, (for example the airport police), and then the security manager will be involved, as will the IT department (to ensure “compatibility of the additional camera to the system”). A working group is then established to assess the requirement for the additional equipment. The system is not audited by an external authority, such as a data protection authority; although there is a certification body. The respondent who mentioned this felt that this body did not go into as much detail.
2.2.5 Suggested Improvements

At the end of the interview, the respondents were each asked how they felt the current system could be improved. This section outlines some of the suggestions made by the respondents.

- More pro-active roles: One respondent felt that the roles of the CCTV operators could be expanded to be more pro-active in terms of intervention in, or reaction to, an emergency event. The respondent stated that a new National Security Plan was moving in this direction anyway. While he anticipated that the operators still would not be authorised to view recorded footage, they would be more active in responding to an event. He envisaged that a system such as that being studied would aid with their being more pro-active through the introduction of alarms into the control room. Another respondent echoed this when he said that the system could be improved if they had “more possibility to intervene on the cameras”. They would like to have “more activities” in order to be able to provide better support to the police.

- Another respondent was in favour of more cameras being used, “every day, every moment”. He felt that more cameras would help with reconstructing routes, tracking of passengers or objects and identifying person / people responsible for a particular action.

- Another respondent felt that the staff should be considered before the equipment. The respondent said that even if the camera “do[es] its job, it’s still only a camera”.

- It should also be noted that one respondent felt that there was no improvement necessary, as their relationships with the police and other authorities in the airport are good. He felt that as they are constantly co-operating with the police, there was nothing in need of improvement.
2.3 Outcomes of Renfe Interviews

This section of the report details the results of the interviews conducted with Renfe security personnel. The personnel interviewed worked both in the CECON control room itself and on the CCTV system used by Renfe to monitor the facilities for which they have responsibility. Four security personnel were interviewed in Renfe, 2 technicians with different responsibilities, a CCTV operator and the co-ordinator of the CECON, a central control centre.

2.3.1 Current Situation and Policies

In Renfe, the stations are monitored remotely from the CECON. The CECON visited by the TCD researchers for this project is responsible for remotely monitoring Cercanías stations under Renfe’s management. There are 8400 analogue cameras and 55 digital. In 2011, 658 incidents were recorded in the CCTV logs and 402 of these were acted upon by law enforcement. The control room operators are trying to monitor the security of people in the stations (both passengers and employees) and the security of the facilities. The threats that will cause a risk to the passengers are prioritised. Passengers’ safety is considered from two perspectives; firstly, their personal security throughout the rail system is monitored, to protect them from threats such as theft and aggression from others. Secondly, their safety from the perspective of the facilities, that is, that the facilities are sufficiently maintained such that they will not be the cause of some incident (for example a person falling on damaged stairways). With regard to protecting the facilities, the operators are seeking to protect the technology, prevent against vandalism and protect the facilities such as the ticket machines and offices (which contain cash). In terms of pre-empting any risks, the ability to follow a subject between cameras is considered important, as one respondent explained: “when you have one risk, you can anticipate another”. Information gathered with this technology can then be relayed to the security guards or to the police.

The setup of the cameras is carried out by technicians. Any actions in the system are logged digitally and this log is running at the same time as the recorder. A manual log
exists separately so that if a technician is present and observes something, they can record it.

The operators have an application which contains alarms. An incident may also be brought to their attention by a call from a passenger or from a security guard. There are “seismic alarms” and they can receive alarms from “maybe one of the ticket sales office”. They also have anti-intrusion alarms and technical alarms. The operators monitor the general security for the facilities that are under Renfe’s management, making sure the installations are in order and that there are not, for example, “suspicious” people hanging around. However, watching the CCTV to detect incidents is not their main task. They monitor the CCTV to check the system is working correctly and keep a watch out for security related incidents, for example suspicious persons, those who are not travelling on the trains. The operators take the appearance and attitude of the person into account. The cameras are viewed in real time, however, all cameras are not constantly being monitored, as there are too many cameras for this to be feasible, and the operators have other duties. The operators would be aware of particular black spots in a station and so they could choose to focus on the cameras located in those places. They could also receive an indication from the police as to where they will be and so they could monitor the relevant cameras. If a report of a particular incident is received then they can select to monitor the cameras from that location.

The operators have different roles in the control room. One operator could be assigned to dealing with the alarms and they would have to decide if it was a real or false alarm. Another operator would be watching the cameras, looking out for faults in the system and, in the case of an incident being detected, following it on the cameras, trying to resolve it and putting in train the correct response procedures. There is also a control room manager. The manager may be involved with the more serious incidents which could occur, and they are responsible for coordinating the different operators’ roles and activities. The manager also has to inform management and the higher levels of the organisation about what is happening.
What appears in the video wall can be influenced from within the CECON. For example, if the control receives a report of an incident, like aggressive behaviour, they can call up the footage from the relevant cameras on the video wall and monitor the situation. Which footage is visible on the wall and the arrangement of the screens is decided by the control centre chief. The configuration of the screens on the wall is altered to suit whatever situation they are in at the time, for example, if an incident has occurred, they may try to watch that location. They currently have some movable cameras which allow a subject to be followed, but which do not have tracking. The zoom functions are considered important “specifically when you need to find some detail, and basically for identification”. The pan and tilt functions of cameras allow them to cover a greater area with one camera than is the case with a fixed camera. Currently, the majority of cameras are fixed, however. There are currently no alarms triggered from the CCTV footage. The video footage from all cameras, whether they are digital or analogue, is digitally recorded.

The operators can view the footage in real time, but they do not have access to the recorded video and they cannot extract any video. However, a member of the operations staff may request that an operator view a section of footage, for example, to verify what was extracted.

Regarding the police, they cannot connect to the CCTV system remotely, if they wish to view the footage in real time. They must come to the control centre and formally request to be given access to the room in which case they are allowed access to the control room to see the live footage, but they have no access to the recorded video. The police must sign a confidentiality form in order to access the CECON and view the live video feeds. Visitors to the building must provide identification at the main entrance, and there is CCTV in the building. The identification badges are also used to open doors, allowing for a record.

The system is set so that footage is stored for a period of 30 days, after which it is recorded over. The system could be set up to store certain footage separately, but that would still be subject to the 30 day limit, and there would be a risk that the operators
would omit to delete the separately stored footage, so this function is not used. If the police make an official request for footage, it is reviewed, to see if that footage is within the previous 30 days. If it is not, then they cannot give anything to the police. If it is and the police request that video be extracted, then they are given a copy of that footage. However, all footage, including that which has been the subject of an extraction for the police, will be deleted after 30 days. The information must also be erased from the computer used to make the extraction from the system. Figure 2 contains a summary of the Renfe control room activities.
Figure 2 Summary of Renfe’s control room activities
2.3.2 Training

The CCTV operators’ training involves the technical aspects of their job. They are also given instruction on how to react in the event of certain incidents, based on the prior experience of Renfe. Based on previous experiences, or information from the police, the operators can also be instructed to look out for certain things or people and how certain events could unfold. They are taught when to move the camera and when to zoom in, or not. The operators are also given “some rules of the risk they should anticipate”, how to apply the rules and how to try to pre-empt a situation (to avoid it) using the CCTV. They are also instructed on making a decision when information is received from a caller. Small changes are occasionally introduced into what the operators are doing in order to avoid fatigue or familiarity with the routine causing their attention to slip.

2.3.3 Incidents

The work of the control room is “dynamic”. The protocols for reacting to different events evolve constantly and so it is important they keep updating their information, to ensure that they take the right course of action.

The operators are monitoring the security of people (both employees and passengers) and of the facilities. The type of security used (cameras, alarms, security personnel) is dependent on the level of risk (“major, minor, continuous”). When an incident then occurs, they combine all the information they have from across the video systems, “from the police, from the travellers,… from the workers that are in the station or driving the trains”. From the perspective of protecting the passengers, they look to ensure their security throughout the system, including in stations and on trains. As stated in Section 2.3.1, the risks they are looking out for broadly fall into two categories: 1) risks to the passengers from other people, for example the risk that they could be the victim of theft or aggression, or illegal trading, and 2) risks to individuals due to something wrong with the facilities themselves. For example the risk of slips, trips or falls due to broken installations in the station (like stairs). Incidents which
involve the passengers are deemed to be the most important in terms of monitoring the system. Using the technology they have, they try to protect the facilities from vandalism and to protect the ticket machines and offices where there is money. It was also highlighted that while the efforts in security are intended to protect people and facilities, they are also aimed at reassuring passengers, engendering their trust, that it is safe to travel in these facilities and protecting the company’s image.

The ability to track people between cameras is considered very important to the operators. It allows them to watch a situation, or risk, and to anticipate if a further risk may unfold, allowing them to take the necessary action. They can also relay the information they have from their observations to the police and the security guards. Sometimes they may recognise a known thief and contact the security guards to alert them to this person’s presence.

The operators can also receive calls for assistance from people in the station. They have protocols in place for how to respond depending on the situation (for example, send security guards, call the police or the “health” services).

There is communication between the control room and the police, fire and medical services, and other such bodies, depending on the incident. However, the operators cannot go through all of the footage to look for specific information because of the data protection law (LOPD).

2.3.4 Review and Accountability Procedures

The recorders in each station where the video footage is stored have their own digital logs. These logs record any actions automatically. There is an additional manual log so that if a member of staff is present and observes something has happened, they can record that manually. The actions personnel are authorised to carry out are controlled by a set access structure to which it is necessary to log in with a unique username and password. The level of authorisation associated with a log in to the system dictates whether the personnel can, for example, extract video footage. Some technicians can see the footage for maintenance purposes, but they cannot extract any of the footage.
and only the equipment administrator can access the logs. If an incident occurs and Renfe are informed about it by people in the station or security guards, the administrator can check if the information is in the system. The user ID and date of access are recorded digitally; it would not be possible to bypass the digital recorder and access information without being detected. However, the level of detail recorded in the log depends on the equipment in use (the equipment in the test station is new). The technician can access the recorder database and “control who has access”. The stations with newer technology have access to the technical room using a card. However, in stations where the technology is older, a person wishing to access the technical room would need to request the keys from the chief of the line. They would receive them in person and so it would be known who had the keys. There is also a camera in the room.

There are 3 ways of recording what happens in the CECON. The first is a written record – the personnel write a record of their actions, including calls made and received. Then there is a recording of all of the phone calls, and thirdly, there is the information from the CCTV system. All of these logs are digital. They can record details of a specific incident, or just a summary of the day, or possibly, for example, the number of incidents that occurred; however, they only record information that is relevant to security. They may also record when access is authorised. For the most part, the information is recorded in real time, or as close to it as is practicable. For example, in the case of a serious incident, the operators’ full attention is required to carry out their tasks, to coordinate the response, so the time, date and important details are recorded and then when they have time after their actions are complete, then they can record it in full. There is also a system which is connected to the other response agencies, such as “the police and civil guard” and they manually record what is happening, so that their actions are coordinated.

The operators record their own account of the incidents. The information is in different systems, as some information cannot be given to the police and some cannot be given to Adif (the company responsible for the railway infrastructure (Adif, 2014)). There is no one system that contains all the information about what happened. All of
the systems require manual input by the operators. They do not collaborate with the police on what should be included in the report though. The record contains both points of view; the police and the operators write their accounts separately into the relevant system.

Only certain employees within the CECON have the authority to authorise the extraction of video footage. However, this person does not conduct the extraction, although they do have access to the system. Their role is to review the application requesting the video and decide if it is acceptable, and if the request is legal. If it is decided that the extraction should go ahead, then a technician will be given the order to extract the video. The technician then gives the hard copy of the extracted video to this person, who stores it securely until it is handed over to the applicant. The whole process of the video extraction is recorded in a document; who has requested the footage and why, “who received the request”, whether authorisation was given, what information they were looking for, the camera ID, date and time of requested footage. Other information recorded includes when the technician was asked to extract the footage, when it was extracted, when it was received in the control room and when it was given to the party that requested it. In instances when, for example, the police request footage of a specific event, this control room employee sometimes has to watch the extracted footage to make sure it is of the correct event. This employee will also be the one to review footage to verify it in the case of any extractions made for use within the organisation.

The operators have access to other databases too, but they do not contain personal information. The databases include information such as train times, if the train is carrying freight, and if so, what that freight is. Any database that is accessible through the user’s log in will record the ID of the user that logged in. An operator cannot access information for which they are not authorised.

The control room has supervisors and is also recorded by one camera. They also make a record over 24 hours in the control room, which they review the next day. They look at what occurred and what actions were carried out, so that they can identify where
improvements could be made, and if mistakes were made, how to react better in future. It is a form of continuous training. If any doubt arises surrounding the summary of events, they check the recorded information, for example the calls, for clarification.

### 2.3.5 Suggested Improvements

As with the SEA interviews, the Renfe personnel who were interviewed were asked if there was anything about the system that they felt could be improved. This section outlines their responses.

- **Renew the cameras:** One respondent felt that renewing the equipment being used in the system and increasing the number of cameras would improve the system. Another respondent felt that while they worked well and had good tools, it would be an improvement to keep the equipment updated, but accepted that it was necessary to take into account the financial situation.

- **Improve the traceability and security of extracted footage:** One respondent highlighted that, at present, when video footage is extracted, it has a watermark; however, for some recipients of the footage, it is necessary to convert the video to another format, which results in the loss of the watermark in the video. The respondent felt it was not an ideal situation as they take such precautions to ensure the footage is secure “and at the end you have an unsafe file that anybody can change and anybody can view”. He suggested making the extracted footage an executable file.

- **False alarm rates:** One respondent felt that false alarm rates are too high. This statement would be relevant to the development of ADDPRIV too as the respondent felt that following up on false alarms wastes the operators’ time.
3 End User Demonstrations and Feedback

During the course of the integration and live testing of the ADDPRIV system, the interface and system were demonstrated to employees in the end user organisations. This section of the report includes a description of the ADDPRIV user interface and details the feedback from the end users to whom the technology prototype was demonstrated.

3.1 System Interface

This section describes the interface presented to the end users for feedback. As the interface was being upgraded in line with developments in the components, there were alterations to the system between the demonstrations to the two organisations. However, the core facets of the interface remained the same and are presented below.

3.1.1 Sign In screen

The interface is designed so that the level of access is filtered at the login screen, based on the user profile used to login. The menu of actions available to the user once they have logged in is dynamic, so users will only be able to see those tabs that they are able to access. At present the system has a level 1 and a level 0 user defined, the level 0 user is used for testing purposes. This user has full access to the video and event review. It also has the ability to add or delete users, assign user levels, and reset passwords. As this last function (adding/deleting/setting of users and passwords) is not a security related function, the possibility was suggested by one of the interface developers that an IT administrator user level may also be appropriate. He envisaged that this user would only have access to the “manage users” tab and none of the security/video related tabs.
3.1.2 Event List screen

This is the default homepage of the system after log in (Figure 3). This tab shows the list of events that have been detected by the system. The list defaults to showing the 24hrs preceding the last time the list was refreshed. The components of the display are as follows:

- Timestamp: This shows the date and time that the event was detected.
- Type: This is the type of event that has been detected: “abandonedObject”, “counterFlow” and “intrusion”.
- Camera: This is the camera where the event was detected. If two cameras are able to detect the same event, it is likely that the event would register twice (once for each camera).
- ID: This is the ID of the event in the system.
- Status: This is the status of the event. It defaults to undefined; users can set the event to be either correct or incorrect. At the end of the 24 hour period, the incorrect and the undefined events are deleted.
D 6.2 – Report assessing the likely impact of this system on end user organisations

---

**Figure 3 ADDPRIV User Interface (Screenshot 1 February 2014)**

<table>
<thead>
<tr>
<th>Timestamp</th>
<th>Type</th>
<th>Camera</th>
<th>ID</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>2014-02-01 at 17:39:53</td>
<td>intrusion</td>
<td>Filter2</td>
<td>52ed2288aca33b9e17000a0e</td>
<td>Undefined</td>
</tr>
<tr>
<td>2014-02-01 at 14:43:25</td>
<td>abandoned Object</td>
<td>Exit2</td>
<td>52ec931aca33b9e17000a0d</td>
<td>Undefined</td>
</tr>
</tbody>
</table>
3.1.3 Filtering of events

On this page also are the various methods of filtering the list. The events displayed in the event list can be filtered by date, time, and status of the event, the camera name and the type of event. Using these filters, the events list will only display those events which correspond to the selected attributes. The menu to the right of the screen contains the drop down menus for each attribute.

3.1.4 Reviewing / Editing of Events

An operator selects an event to review from the list, taking them to the screen in Figure 4, below. From this screen the operator can view the video of the event, change its status and review the video associated with the past and future routes returned for that event. A map of the location is shown next to the video and the camera where the event was detected is highlighted. There is no additional user verification required to review the event video, as the set of allowable functions for each user should have been defined when they logged in. There is no limit to the number of users who can be logged into the system at one time. However, if two users decide to edit the same event simultaneously, the edit which is saved last will be the one that remains. It would be possible to have one user reviewing events while another is viewing the live stream. When an event is closed, the list is automatically updated. The camera corresponding to the video segment being viewed will be indicated on the map graphic. There is no log of users who log in, or their actions.
D 6.2 – Report assessing the likely impact of this system on end user organisations

Figure 4 Event Review screen (Screenshot 18 July 2013)
3.1.5 User Management Menu

The function of this menu is to allow for the administration of the users of the ADDPRIV system. This allows authorised users to add, delete and set the level of the users in the system. It also allows the authorised user to reset a user’s password. This tab will only be visible to Administrator users (currently level 0). However, it was discussed that possibly an administration level above level 0 users could be created which had access to the whole system, and/or an IT administrator who has access to just this tab. This function could then be removed from the level 0 security user profile (and all security user profiles).

3.2 1st Demonstrations: SEA

The first demonstration of the ADDPRIV system to end users took place on the 16th July in the Linate offices. In attendance at this demonstration were: 3 airport police officers of different rank and the head of the airport police in Linate airport. Also present were the Security Manager for SEA and a SEA security CCTV operator, as well as members of the project consortium. Further interviews were conducted with a second operator and a control room supervisor on the 18th of July.

The demonstration began with the playing of the ADDPRIV video (in English) accompanied by an explanation of the system, followed by discussion and interviews. The discussion was recorded in Italian and a summary provided in English.

3.2.1 Feedback on ADDPRIV System

This section details the feedback of the various security personnel who were present at the demonstrations of the ADDPRIV system in Linate Airport. The feedback about the system was broadly positive; however, some of the respondents indicated that they were making allowances for the system being at the research stage.
Timing

The time taken by the system, as demonstrated to the end users in SEA, was raised by some of the respondents as being an issue. The purpose many of the end users interviewed saw for ADDPRIV was to aid their intervention in an incident, if one is detected. The speed with which they are able to intervene would be hampered by any delays within the system in relaying the required information to the operator. Police officers interviewed described the timing as “crucial” and felt that the timing within the system at that time was not acceptable. Another respondent felt the timing issue was a limitation of the system. He used the abandoned luggage event as an example for why timing is so critical; if a person abandons a piece of luggage which contains explosives, the length of time between them leaving the bag and the bomb exploding could be very short. This potentially short window to react to such an event if it were detected would be further reduced if the system is slow to relay the relevant information to the operator. The respondent stated that the operators need to be “able to intervene rapidly”.

Regarding the length of video required of the event that has been detected. One respondent said that there already existed a similar system for recording the gates when a gate door is “forced open”. He said they have 20 seconds of footage either side of the actual event and similarly, he thought 20-30 seconds of video would be sufficient. However, in relation to additional footage, for investigating an event after the fact, he would be interested in having all relevant footage from when the person entered the terminal, and from across other cameras. Another respondent thought 10 seconds before and 10 seconds after the event would be sufficient, with the option to see if the relevant person was detected on other cameras.

Alerts

Several of the respondents felt that the system would be enhanced by the addition of more noticeable alerts when an event is detected. It was suggested that some sort of visual alert, such as something flashing, might appear on the screen when an event is detected and added to the event list. It was also suggested that some alarm sound
would aid in drawing an operator’s attention to the detection of an event. In addition to this, some respondents felt that the events could be categorised according to the type of the event and the urgency of the response required, level 1, 2, 3 etc. They both referred to the comparison between a counterflow event and a piece of abandoned luggage to illustrate the point; an abandoned bag would be a priority (it could be a bomb), whereas a counterflow event is “a little kind of alarm”. The alerts used could then correspond to the category of the event.

**User Interface**

Apart from the need to enhance the way in which a detected event is communicated to the operator, those respondents who answered questions on the user interface gave positive feedback on it. They felt that the interface was “clear” and “simple to use”. One respondent commented that it would be accessible to a broad range of people across different cultures, countries, skills and levels of education.

The police, however, raised the issue that they require surveillance capability for the entire airport. They are not only looking for the events that ADDPRIV would detect if it were implemented, but they would also need to be able to reconstruct routes and dangerous acts, which may be the subject of an investigation. In addition to this, the police could be looking for accomplices to suspicious or dangerous acts. It was deemed necessary that the police should be in a position to observe the whole airport.

**Route Reconstruction**

Several of the respondents mentioned that the route reconstruction element of the ADDPRIV system would be very important and useful. Two respondents saw it as an aid for finding a person of interest after an event has been detected. One explained that, once an event has been brought to the attention of an operator, the operator, using the route reconstruction trees, will be able to see where the person involved went and the search can then begin at that place, rather than the security personnel having to search the whole airport. He felt that being able to follow the whole route a person took was very important. Some respondents also mentioned that if such a
system were to be implemented, it would be necessary to ensure that the routes could be linked from inside to outside the airport.

**Event Detection**

The three events chosen for event detection were endorsed by several respondents as being appropriate. Of the three events, abandoned luggage was the one which was considered to have the most priority by security personnel. One respondent felt the counterflow event could be problematic to implement, as people often go in a direction counter to the flow, but “it is not a crime”. He said, however, that in the case of a fixed barrier, then counterflow “could be important”, but that with flexible barriers, “it’s not a risk, it’s not an event”.

Another issue raised related to the retention of footage of minors. During the demonstrations an example was viewed whereby a child walking under the flexible barriers triggered the event detection. In such cases as these, if ADDPRIV were fully operational, footage of the child would be related to an event and retained. This concerned some of the respondents as surveillance of children is “governed by law”.

One respondent replied that the event detection element of the system would help the operators to detect, and act on, events as they happen, where previously they would only have caught the events after they had happened. This would allow the operators to intervene in an incident. Other respondents felt that the event detection and route reconstruction elements were important. It was commented that someone running from one area to another should be a detectable event; the examples were given of someone running out the exit doors from the terminal, or fleeing having committed a dangerous act. A respondent said that it should also be possible for someone running to be linked with the abandoned luggage detection.

**Deletion**

The automatic deletion of footage that had been deemed irrelevant to security was raised as an issue by some respondents. As mentioned with regard to the user interface, the police require more footage than that which is associated with an event
which may have been detected by ADDPRIV. A SEA representative too was concerned that if the footage not related to events is deleted automatically prior to the deadline set out in the law (7 days), then SEA would not be in a position to produce that footage should another authority request it. He was concerned that the introduction of the ADDPRIV system would result in a loss of “flexibility” for the security department, as only events that are detected and marked as “correct” will be retained.

**Operators and Training**

Training was mentioned by several of those interviewed as being a requirement if ADDPRIV were to be introduced. If the system were to be implemented, the personnel would need to be trained before the system was in place and then there would need to be “on the job” training as they build on their experience of the system. Some respondents saw the potential for a new system to introduce innovation into the training and practices of the personnel. One respondent suggested it may be necessary to have a new job role for people who initiating a response to the event once it is detected. He also thought that, if the system were expanded beyond the test area, it may be necessary to employ an additional operator, given the operators’ existing tasks. Regarding whether or not the monitoring of ADDPRIV would be constant, he thought that it would depend on the timing, on if it was a period of heightened risk for infrastructure. Another said that it would only be possible to determine the resources required when the system design process was complete. One respondent did highlight, however, that the operator would have “much more to do” than he had understood prior to the demonstration, in terms of identifying those segments which are relevant to security.

An issue was raised during one interview in relation to the people working in the airport. The participant pointed out that if the system were to be rolled out across the entire airport, then the people working in the airport could be involved in events that get detected and not only those people passing through the airport would be subject to the ADDPRIV event detection.
**Future Developments**

In terms of possible future implementation of ADDPRIV, it was also suggested by a SEA respondent that a function could be incorporated whereby operators could receive an alert to a handheld device, such as a Smartphone. This would allow them to be alerted to the detection of an event, even if they are not in front of the ADDPRIV interface when it is detected. It was pointed out that this function would be particularly useful in situations where there is only one operator on duty in the control room. It was clarified with the respondent in question that only the alert would be transmitted to the handheld device, no video footage would be made available except when the operator returned to access it through the user interface.
3.3 Discussion with the End Users’ Advisory Board

The third and final meeting of the ADDPRIV End Users’ Advisory Board took place in Linate Airport, Milan, Italy on September 13th 2013. The meeting incorporated a demonstration of the technology by consortium partners HP and a discussion of the technology’s application in the end user organisations.

The representative for a public transport company raised the point that his enterprise, though working in collaboration with the police, was not the police and as such, did not have an entitlement to decide what footage should or should not be deleted. When the police or other authorities request the footage from the company, they must be able to produce it.

He pointed out that technology proposed by him to his enterprise had to be legal, tested and preferably be of use to law enforcement as well. He raised the question of what ADDPRIV was targeting; prevention of crime, rapid response or forensics?

In response to the end user’s perspective, the question was asked: can ethics and privacy be overlooked if the law is adhered to?

A representative for SEA pointed out that the police need the video footage for a long time, whereas the airport’s objective is more focussed on safety. This is also the case for Renfe and the public transport company, according to their respective representatives.

Renfe’s representative on the board suggested that people crossing the tracks was a concern for this organisation and suggested alarms for this would be very useful, and could help monitoring at remote stations.

The representative of the public transport company highlighted graffiti as a serious concern, and CCTV as the main tool in the fight against it. Requests for lost children are also a frequent occurrence.

How the criteria for the system would be defined, and who should be defining them (police, judges etc.) was also a concern. It was suggested that a possible conclusion
would be that the system was not suited to security use and would be more appropriate for logistical and operational requirements of end users. An example of such a situation for SEA was given, whereby passengers, who are to be transferred to their plane by bus, see that their bus is full and decide to put themselves on another bus. However, this other bus may be going to a different plane.

The representative of the public transport company suggested that ADDPRIV may be appropriate to extraordinary events, such as the Expo2015, the pope’s visit, or a football match with an influx of people for only one day, for example. He stated that the pope’s visit had required many man months of work. The deletion could only be used with the police to focus on specific things, but there is always the risk of something unexpected occurring and you can’t know in advance what it will be, so you can’t let it be erased. The system must also consider the timing of the crime. If the security only happens after the event, he said, it will not save lives.

He also raised the issue that footage containing employees cannot be used unless they have committed a crime. It’s different for passengers, but not by much. They have to defend the material assets, inanimate objects. This is the main way the enterprise can use their CCTV. HR and training are also possible issues which could arise. The controllers must be properly trained for the system to work.

The following questions were asked to the attendees:

1) Could the images realistically be erased? And

2) Given that alarm technologies already exist, why have they not been implemented?

The public transport company’s representative suggested fear of not complying with the law and a lack of a precise legal framework were issues, while the representative for a European police force suggested it was the lack of reliability of these technologies that was of concern. They had a system detecting people entering a building, but they disconnected it due to the high false alarm rate.
It was also pointed out that the route reconstruction would be useful if it works, but that end users wanted to use it in a way that was invasive to privacy (that is, to select a person and know all about them). Another point made was that, were tracking to be introduced in certain countries, there would be a strong resistance from the people. The point was also made that end users have little or no control of the footage they record.
3.4 2nd Demonstrations: Renfe

The second demonstration of the ADDPRIV system took place in one of Renfe’s control centres on the 5th February 2014. This demonstration was completed in the form of a focus group. An explanation of the system was given by way of a presentation followed by a live demonstration of the interface. The attendees were given the opportunity to ask questions and give their feedback throughout the presentation and demonstration. After the demonstration was completed, there was further discussion where questions were used to prompt feedback.

In attendance at the demonstration were 3 technicians, each with different responsibilities; one engineer whose job involves planning and development of CCTV projects for the control centre; the coordinator of the CECON and a CCTV operator. The system was demonstrated in the form in which it is set up in Linate Airport.

Subsequently, further discussions took place with Renfe personnel regarding further practical considerations of implementing a system such as ADDPRIV in an organisation such as Renfe. This section of the report describes the outcome of the demonstration and subsequent discussions.

3.4.1 System Interface

In general, the attendees felt that the interface was good, it was easy to follow and simply laid out, although they would require it to be in Spanish. They felt that the ADDPRIV logo could have been smaller to allow more of the event related part of the interface to be visible on the screen at one time. They also would want to define the camera names themselves when the system was being set up for Renfe.

Sign in Screen

During the discussions it was stated that it would need to be possible to integrate the system into existing user applications in the CECON. It would be preferred that every user has only one user profile to access the applications in the control room, as they
have many different applications operating in the CECON and to have a unique identification or set up for each would be unfeasible.

**Event List**

Regarding the event list, the question was raised as to what elements went into the event ID and why it was displayed on the event list. It was felt by those present that the event ID contributed no information on the event for the operator and so the purpose of it being included was queried. The use of “undefined”, “correct” and “incorrect” as the tags for the event were questioned.

The attendees also suggested that the event list should display not only the time when the event was detected, but also a time indicating when the past tree footage began and when the future tree footage ends. In addition to this, it was felt that the filter function for refining the event list should include an option to filter by a time period and date range. It was also suggested that for a distributed system such as that existing in Renfe (the CECON is responsible for monitoring approximately 500 stations) it would be important to be able to refine the list based on location. This would allow, for example, an operator to refine it to show all events which were detected on all cameras in a specific station, as opposed to only those detected by a particular camera.

A further suggestion regarding the list filter was that it should be capable of being used to search through events rather than just filter. The participant made the distinction that with the filter, you already have to know what you are looking for, but that with a search engine you could search for information that was not already in your possession. The ability to refine the list by location would help with this. Given the number of cameras monitored by Renfe, he felt this would be more practical.

The question of the way in which new events should be indicated on the event list was put to the attendees. They were asked if they agreed with previous suggestions that the events should be accompanied by a visual and/or aural alert. They thought that the sound of the alarms could be too much; given the number of cameras in their network,
it could lead to the control room being too noisy. However, they felt that the option should be available at the set up stage of the system so that certain events could be configured as needing to be accompanied by an alert of some sort. Setting levels of importance for the events was considered as a possible function for inclusion. However, it was pointed out that the level of importance of types of events could be too variable to allow for setting a level of urgency, as the urgency level may be different depending on the day and time of day. The attendees suggested intrusion as an example; whereby intrusion during the night is of more importance than intrusion during the day. It was felt that it should be an option that could be selected at the configuration stage. Another participant, however, suggested that different events should require different types of responses. For example with vandalism the footage could be used to try to identify those involved, and the police would be informed, whereas people crossing the tracks requires an immediate response.

**Event Review**

The attendees felt that the video clip of the event was too short. They suggested that an additional few seconds before and after the actual event itself would give context to the event by showing when it happened. Regarding the length of the future tree, the attendees felt that for the real time intervention, the length of the video available did not matter as much. However, for the purposes of the subsequent investigation, it would be necessary to have all of the video of the person of interest while they were in the station.

### 3.4.2 Operation of System

**Integration**

The attendees at the demonstration felt that the ADDPRIV system would complement the existing systems in the CECON. In the course of the subsequent discussions, the importance of ADDPRIV’s integration with the existing framework was highlighted. There are approximately 300 applications currently being used by Renfe, and it would be impractical for each to have its own operating procedures, or user profiles.
Further to this, during the demonstration, the possibility to incorporate an option for viewing live video into the ADDPRIV interface was discussed. It was said that, while they can already view live footage through their existing applications, a level of integration between the existing applications and ADDPRIV would reduce the length of time it would take to intervene in an incident, as the operator would know the location of the detected event and they could then check the live video of the camera at this location.

A question was raised by one of the attendees at the demonstration as to how the system would cope with detecting events when the camera was in motion, that is, when an operator is panning, or tilting the camera. It was pointed out to the attendees that the system is currently designed to operate on fixed cameras, but feedback was requested about whether they thought it would be feasible to have the camera having pre-set positions to which it could move, and thus detect events at these positions, or if it would be necessary to have the camera detecting all angles. The attendees felt that in order for a camera to constantly monitor every angle to which it could be moved, it would have to move too frequently.

**Video Analysis**

A concern raised during the discussions was the practicality of implementing the ADDPRIV system in an organisation such as Renfe in which the existing system is quite distributed. At present, the operators access the video footage for each station remotely and so the implementation of ADDPRIV raises the issue of where the video would be processed. If the processing were to be centralised in the CECON, it would necessitate all feeds, from all cameras, being transferred from the stations to the CECON. Those involved in the discussion felt that this was not viable, not only was the quantity of footage to be communicated to the CECON a concern, but there would also be new security measures required for the data that would be sent to the control centre. The alternative they considered would be to have the video analysed at the station level. However, this would require the system to be installed in about 500 individual stations. Another possible configuration considered was for only the
detected events to be sent to the CECON rather than all feeds. However, there would still be the matter of secure communication between the stations and the control centre. The potential loss of the video watermark was also raised as a concern if the footage was to be processed centrally. One participant commented that an organisation such as Renfe may be too big for the system to be implemented, based on its current design.

One-off events

Following on from the End Users’ Advisory Board meeting wherein a suggestion was made by one participant that a system such as ADDPRIV would be better suited to unusual events (such as football matches) than to the day to day running of infrastructure, the attendees at the Renfe demonstrations were asked if this would be a way in which they could envisage the system being applied in Renfe.

The attendees did not think that this would be appropriate for the Renfe stations on busy days. They were concerned that in a very busy environment, where there were large numbers of people, the algorithms would not function properly. In addition to this, they said that the video footage of such unusual events was not only used to detect security events, it would also be reviewed in full to analyse if the security plan put in place had worked. This allows them to plan for future such events. In order to make this type of review, they need all the footage, not just that which is associated with “suspicious” events. The Renfe personnel responded that, were ADDPRIV to be implemented, there would need to be a function which would allow such occasions to be marked for exemption, so that the entirety of the footage for such events or days would be retained. They proposed perhaps associating an event with “crowds” of people, so that footage from that period would be retained. However, they raised the issue that at peak rush hours, there are crowds of people, and these crowds are not security relevant. One attendee suggested that a possible solution could be to allow the system to be configured based on the station, day and time, so that it would be possible to make certain exceptions within the system for all footage to be retained for analysis.
Automatic Deletion

In addition to the comments about retaining footage from one-off events, another concern the attendees raised with regard to the automatic deletion of footage was that the judicial system may not necessarily request any footage they require promptly. At present, requests for footage that is more than 30 days old, cannot be fulfilled due to the 30 day retention period. However, if the automatic deletion were to be implemented, then even a request which arrived within the 30 days could potentially relate to deleted footage. In addition to this, problems arise as a request could be received from an international agency relating to a person who is of interest to them because of an incident which occurred elsewhere. So for example, they could believe a certain person was in the train station at a certain time, without having caused the incident there, and request that footage as part of their investigation. Were ADDPRIV to be in use, as no event would have occurred within Renfe’s stations in such a scenario, the footage could have been deleted. Ultimately, the attendees decided that as the law currently says 30 days, they will need to keep it for 30 days. It was further commented that when the system is being configured to detect certain events, the events chosen are from the perspective of Renfe and its operators, however, an external authority may have a different requirement or point of view and if the automatic deletion is in place, then only events of relevance to Renfe will have been retained.

Timing

Two main issues were raised by the attendees regarding timing. The first related to needing to know how much time lapses between when the video is recorded and the video is analysed. The other related to the feasibility of having 24 hours of events saved. This second concern had two aspects, the first related again to the need to keep all the footage for 30 days instead of some of it being deleted after 24 hours. However, the issue was also raised that, because that the CECON deals with footage from so many cameras, they were concerned that it may not be possible to review all of the events which would be detected in 24 hours. One attendant commented that one day
was not long enough to review the number of events that would be detected across so many cameras. It was felt that it would require a dedicated member of staff just to review the event list in order to keep up to date, and this would be true regardless of how many hours or days of events were displayed on the interface. This posed the further problem of whether the operator responsible should review the events in the order that they appear on the event list, or should they skip older events when a new one appears on the screen.

**Logistical uses**

While the deletion element of the technology has been identified as an issue for Renfe with regard to possible implementation of the system, the attendees at the demonstration saw a use in the route reconstruction element as a tool for aiding the investigation of incidents after the event. According to the attendees, the route reconstruction element of the ADDPRIV system would allow them to reduce the number of hours of footage they needed to view in order to find footage relevant to an event. They pointed out that the existing recorders, which have their own proprietary format, have functions which allow for the analysis of the video for issues such as intrusion or counterflow, but that these functions are not active on the live footage due to too many false alarms. However, even reviewing the video in a subsequent investigation, it is still necessary to view the video in real time to find what you are looking for. They see the benefit of ADDPRIV as having the ability to search by events, thus reducing the amount of footage to be reviewed.

In considering what applications there could be for ADDPRIV on railways, the attendees suggested for use when there are large crowds, although as previously mentioned this would not be considered a security relevant issue at all times of day. Aggressive behaviour of people in the stations was also mentioned during the discussions, as was a person falling. The intrusion event was considered as possibly having an application when trains are parked overnight. Vandalism of train carriages is a concern, and they expensive to repair. One participant in the discussion mentioned the possibility of using the intrusion event to detect when people entered the area.
where the trains are kept after hours. People crossing the rails had also been mentioned during the End User’s Advisory Board, and on further discussion the point was made that trains also “trespass” on the tracks, and more frequently than people. As such, this would need to be allowed for in the ADDPRIV system to avoid having trains causing false alarms. Questions also arose regarding ownership of the relevant camera systems, as Adif may own some of the cameras in the areas where the trains would be stored overnight.
4 Potential End Users

4.1 Introduction

A central goal of the research carried out by the Goldsmiths’ research team was to assess the impact of the ADDPRIV technology. The ethical, legal and human rights issues raised by this assessment of impact are detailed in Deliverables 6.1 and 6.3. However, the research team also explored impact through potential end uses of the ADDPRIV technology. Through engagements with a range of stakeholders – such as police forces, data protection officers interested in an ethical and accountable surveillance system and transport organisations – the Goldsmiths team collected data from those who had an interest in the potential future uses of the ADDPRIV technology. This section of the deliverable will offer a brief introduction to the methodology used to engage stakeholders in assessing the impact of ADDPRIV. It will then offer an analysis relevant to potential future uses of the ADDPRIV technology. Finally this section of the report will offer a brief summary of the Goldsmiths team analysis of end use impacts.

4.2 Methodology

This section of the report outlines the methodological approach for this research adopted for engaging organisations in assessing the potential impact of the ADDPRIV technology. An approach was adopted which involved assessing both the ethical, legal, human rights impact of ADDPRIV and its potential impact on end users. The potential ethical impacts of a surveillance technology are important to give a full picture of the potential future of ADDPRIV. These ethical impacts are detailed in Deliverables 6.1 and 6.3. However, assessing the impact of ADDPRIV could not be restricted to ethical aspects alone. How the ADDPRIV technology might be used, by whom, for what purpose and with what consequence also needed consideration.
The methodology for assessing impact through potential end users of ADDPRIV involved two parts. Firstly, a series of interviews were conducted with experts. These interviews were semi-structured and in-depth, giving interviewees the opportunity to express their views at length. The interviews were then transcribed and coded into an initial set of themes around which the analysis in this section of the report could be constructed.

25 interviews were carried out with representatives from the following groups:

- Data protection officers / Information Commissioners 4
- Academics 10
- End users 5
- Policy makers 2
- Independent researchers 1
- Technical experts 1
- Civil liberties groups 2

These interviewees were drawn from across the geographical composition of the ADDPRIV project (the UK, Poland, Italy, Spain and Ireland). After initial contact was made with potential interview participants, a detailed overview of the ADDPRIV project was provided along with details concerning data handling, confidentiality and sensitivity. Potential participants were invited to ask questions and seek clarification concerning their involvement and about ADDPRIV more generally.

Secondly, dialogue workshops were conducted. These events were designed as an opportunity to provide an ADDPRIV technology demonstration in order to foster a focused discussion of the technology and its potential impacts. Dialogue workshops provide a structured forum for a facilitated group discussion that allows participants to consider issues in-depth. The purpose of this aspect of the project was to allow an opportunity and forum for audiences to hold the system to account, and for any
concerns to be addressed. Participants from various sectors were involved in the dialogue workshops, ranging from: academia, the private sector, the public sector, trade associations, technology organisations, transport organisations, consultants, the police and security forces, data protection officers, academics, civil liberties groups, and members of the public.

Four dialogue workshops were held in 2013 in Brussels, London, Barcelona and Nottingham. The dialogue workshops were attended by audiences that ranged in number:

- Brussels 34
- London 22
- Barcelona 41
- Nottingham 15

Before the technology demonstration, audience members were given a feedback form to provide comments on the ADDPRIV technology. Within each session audience members were also invited to take part in discussion. Participants were also provided with an anonymous web feedback form that they could complete.

The two methods provided a means of assessing potential end uses of ADDPRIV, the potential impact ADDPRIV might have on end users and provided a space for discussing any potential advantages or limitations with the ADDPRIV technology for end users. The following sub-section will provide an analysis of the results derived from this methodology.
4.3 Results

The following analysis is divided into two sections in order to present results from the analysis carried out of the potential impacts of the ADDPRIV technology on end use. The first section will be focused on interview results and the second section on dialogue workshop results. The results from the two approaches will be drawn together in a final summary section.

4.3.1 Interviews

The 25 semi-structured interviews produced an array of relevant discussion points for ADDPRIV end use. These have been coded and arranged into six themes which are presented briefly and then analysed in more depth below:

1. Business case
2. Technical sophistication
3. Evidence handling
4. Operator role
5. Technology shaping the end user
6. Ethics/law and end use

In the following in-depth analysis of end use impact, the interviewees’ own views are presented in detail. What will become clear in this analysis, is that each point is important to the interviewees but also somewhat uncertain. This uncertainty arises because the interviewees are not experts in ADDPRIV, but are being asked to respond to our presentation of what ADDPRIV could achieve. The uncertainty for interviewees also emerges from the future orientation of the technology – it is still under development. The interviewees’ responses therefore need to be treated with caution and their uncertainties are made clear in the following analysis. Each theme is discussed by interviewees in terms of an issue that ADDPRIV could potentially resolve or potentially create.
Business case:
A prominent theme of discussion for end user organisations was the business case for ADDPRIV and for ‘smart’ surveillance systems in general. The interviewees, as the following quotes show, wanted to know about the efficiency of the system for their own processes, whether or not the spaces under surveillance are kept safe and how much efficiency and safety will cost:

End User Organisation Representative 1:
People are more likely to invest in [smart CCTV] because it is seen as value for money. Human resources are quite expensive in that they have to be trained, if you had three hundred cameras, the task is challenging, so if you can apply the technologies … it a lot easier and doesn’t rely on human resources in the same way.

End User Organisation 2:
What is the purpose here? …. our role is to provide technology that keeps the network moving, keeps it safe, and reduces costs, you take those three things, it’s got to meet those three things.

For this end user, the potential business case for ADDPRIV can make sense in relation to other ‘smart’ applications they have been in contact with:

End User Organisation Representative 2:
Unfortunately when we looked at facial recognition, a lot of the technical people behind it were trying to sell us, or potentially trying to sell us the notion that it would save us, and save us in time and people’s time and particularly in police time, and when we looked at it, in fact nothing could have been further from the truth because what the technology had done, in fact it had made CCTV more intelligent, it still required some human intervention, it still required someone to say yes, the face you have pulled up against these three
faces here is the person we’re looking for. And we don’t have that human intervention at the moment and so we would have to pay for that, there’s a further backroom, whole other set up that we require and then what are you going to do? It’s a bit like ANPR, I remember working on some of the early days of ANPR and the police said that they could only respond to 8% of all ANPR hits, they just didn’t have the capacity, and bear in mind it was pinging up all positives, of 100% positives they could only respond to 8%, so it was a technology that they had to refine further. So far that they had to ask, even in an algorithm, what is the priority of event that we want to intervene in here. So ... from a business perspective we want to make sure that it enables the network to flow, that it has a safety and security purpose beyond what we already provide and certainly has some, may bring some savings to us, maybe in the long run, but that it will be cost effective.

Another way in which this end user could assess the business case was in terms of adding to existing investments made in surveillance systems, that ADDPRIV would not require a new surveillance network:

End User Organisation Representative 2:

I totally applaud what [ADDPRIV] is trying to do, but we, as I say, in mass public transport, will it meet the business needs and we have to keep coming back to that. ... The good thing about it is that it can be adapted to any existing system, because it’s usually software based isn’t it, it’s usually add ons so you can keep the existing cameras. And that’s the problem with a lot of the intelligent stuff, like the facial recognition for example, you need new cameras and better technology, better quality lighting, better high definition cameras and so on, and it’s all as well as the algorithm at the back end. Whereas this, if you’ve got a fairly decent camera then movement’s easier to detect.

Data Protection Officers were also cautiously positive about the business case for ‘smart’ technologies like ADDPRIV that could also take ethics into account. They hoped
that more ethical technologies would make their job easier, but also that having a recognisably ethical technology could be promoted to organisations that use surveillance equipment so that they might enhance their own brand image. Data Protection Officers hoped to see a market emerging for ethical surveillance technologies:

Data Protection Officer 4:
companies can be encouraged that there is a commercial value to using privacy enhancing technologies, because people do, I don’t think people always think that the general public are bothered about this, but I think they actually are and we certainly know that they are from the work that we do and I think there is actually a commercial benefit to companies if they can say yes we’ve done the impact assessment and as a result of that we’ve also implemented this technology that actually limits the impact, you know, it meets our needs, but it limits the impact on your privacy.

This initial theme thus suggests a cautious advocacy of the ADDPRIV technology for potential end users, such as mass transportation networks, but also for other beneficiaries such as Data Protection Officers and the public. A potential public benefit derived from ADDPRIV, was identified as a possible element of justifying investment in the technology – that it could help end users situate themselves at the forefront of an emerging privacy market, fulfilling public expectations.

Technical sophistication:
Following from the preceding discussion theme of the business case for end users, it was perhaps no surprise that a major concern for potential end users was the technical sophistication of the system and the extent to which it could deliver its aims. This concern derived from what appeared to be multiple recent experiences of end users subjected to approaches from sales teams trying to promote ‘smart’ solutions that appeared to fail to deliver on the promises offered by sales teams.
End User Organisation Representative 3:
New technologies, for instance, where software can recognise faces or patterns of behaviour are being worked on, they’re generally not ready for operational environments. They’re not sophisticated enough. Facial recognition and behaviour recognition have been trialed in transport environments, but they’re not good enough, too many errors for them to be taken up. They could be used, for example if someone falls onto a track a trigger could sound, or the current cut, but for crime they’re not ready. Any technology has to work with existing elements of police and security systems, and complement them. It’s useless to have technology that hinders police work. For any new CCTV to be adopted, or run, it would need to benefit system operators, the police and the criminal justice system.

Other end users raised questions regarding the technical details of operation in the ADDPRIV system and how this might fit with their working practices of retaining data and maintaining a proportionality principle (in line with Data Protection legislation):

End User Organisation Representative 1:
We have a requirement to keep things, under the [Data Protection] Code, to keep things for a minimum of thirty-one days. In order to adhere to the Code we would have to keep data for thirty-one days, but I can imagine how smart software could then be deleted after that…. I think as well you’ve got to go back to that question [of proportionality] and we’re under the spectre of a certain terrorist risk and you’ve got to ask if these technologies are available, from a security perspective I might expect them to be used because of their proportionate to the risk. However there’s me saying that, whereas other people say no you can’t do that because it’s surveillance beyond that proportionate level, you know, because it’s too intrusive.
Other end users were more interested in having a surveillance system that was technically efficient by being both proactive and straightforward (this also seemed to stem from a general suspicion that more sophisticated systems did not work):

End User Organisation Representative 2:

The problem with CCTV at the moment is that its passivity makes it a system of response whereas [ADDPRIV], these are technologies which I hope are trying to make CCTV more dare I say it proactive or preventive in nature. So this identifies the behaviour or the event, and then with the human you can get an intervention in before it happens and that can only be good. And I think you need to keep it simple, I mean we have cameras out there which literally have only one purpose, it could be just to monitor a signal, or to monitor a platform, or to monitor a door. It’s got to be simple, keep it fairly simple with the technology and with the humans.

Technical sophistication, in line with many of the themes discussed by interviewees, were both a potential challenge for ADDPRIV (raising questions such as how sophisticated is this the system, how easily can it match existing organisational practices and legal concerns) and a potential opportunity (following poor experiences with other supposedly ‘smart’ systems and given ADDPRIV’s particular kind of focus on event detection).

Evidence handling:

A key concern for end user organisations was the process of evidence handling and how this could work in concert with the ADDPRIV technology. The issues raised here related to concerns raised regarding the admissibility of evidence from the ADDPRIV system in general and whether thought had been given to the chain of custody required for video evidence to be used in courts of law and whether any algorithmic processing of that evidence raised questions regarding its integrity. The following response from an end user summarises many of these issues:
End User Organisation Representative 4:
We have to be very careful in how we treat images, it’s evidence, and there are concerns with any evidence and ways to ensure that evidence isn’t altered, tampered with or whatever so that it can be used in court. Now, with CCTV on a VHS that’s relatively straightforward, with digital evidence we’ve got to be a lot more careful with that... I’m really not against using the technology, I think it’s great, it makes life easier a lot of the time, like anything, but from our point of view, for policing we’ve got to be able to use these images and recordings for evidence in court. If technologies can be developed that ensure evidence is maximised in interview and at court, great. And we’re a long way from that at the moment.

Concerns were also raised regarding the deletion of data. For example, interviewees asked what the impact would be on any court cases where a history was required surrounding an event, but where surrounding footage had been deleted.

Academic 3:
I can think of some real criticisms from a police and operator point of view. One thing that comes to my mind is what happens with investigations and the need for footage? What happens if someone passes through an airport or a train station who you subsequently wish to identify? There are police officers who spend their time going through footage assembling the evidence for cases to be taken to court. And that’s all post imaging stuff and that’s often because the cameras are on all the time and the images have been caught on the cameras and even then they have difficulties. I can see police and potentially other agencies wanting to do retrospective viewing of footage which is a lot of what they do.

This concern here is not that footage that has been detected as potentially relevant might be lost – interviewees were clear that footage detected as relevant was stored. The concern instead was how decisions were made regarding relevance, that
something may only become relevant at a much later date. The following interviewee wondered if the business case for ADDPRIV might be bolstered by looking into evidence handling:

End User Organisation Representative 3:
Police and police staff work to process information and create data packages of incidents for evidential purposes. This can involve several CCTV surveillance systems and a lot of analysis. It’s a time consuming and costly effort. A system that could collect and handle that data, and provide a data package would be useful. For obvious reasons that would have to be precise and would always need to be monitored and evaluated by whoever had ultimate responsibility for the data and the images. There would need to be a quality control of sorts.

The issue of evidence handling was once again a potential strength and a potential challenge for the ADDPRIV system. Alongside the potential challenge of losing data surrounding an event and losing integrity of images through algorithmic treatment, there was the potential positive of having a system that made the work of certain kinds of end user more straightforward (particularly police officers and police staff who needed to prepare evidence for courts).

Operator role:
A further issue raised by interviewees in relation to end use was the role of operators. Again the interviewees identified both challenging and advantageous aspects of the ADDPRIV technology for issues involving operatives. The following interviewee suggested that the ADDPRIV technology would offer one means to reduce an issue that has long been prevalent among anti-surveillance/pro-privacy campaigners: that operatives tend to have a narrow frame of reference for selecting likely events and perpetrators of events leading to a kind of bias in surveillance systems, derived from operatives following events that have previously proven fruitful:
Academic 3: I can see a real advantage to [ADDPRIV] in some ways, and one of the ways is that with the public street CCTV the major criticism from the social perspective has been the prejudice and bias of operatives of who they focus on.... And amplify certain patterns and so on. So it would actually eliminate that so an operator would only focus on a movement, it would be a movement of a human body. So they're not going to be identifying people by race or gender, so from that point of view it's a big plus.

Other interviewees were concerned not to lose the unique skills, awareness and knowledge built up by operatives of surveillance systems. The concern here was that having a semi-automated system like ADDPRIV would reduce the skill levels of operatives but also that organisations would lose out their skills and knowledge. The following interviewee discussed the possibility of combining semi-automated relevancy detection in ADDPRIV with the current skills and knowledge of operatives:

End User Organisation Representative 1:
Something you might want to think about is the relationship between the individual operator and a control room. If you go into control rooms and ask them about what they’re doing quite often they’ll tell you about their routine, so they’ll be looking at certain cameras at certain times of the day and they have an understanding of what’s normally happening and what they need to be doing. I don’t think you should forget that these operators have their knowledge of that particular locality, so you might want to bolt the technology on to give them support and assistance. Sometimes that can be a lot cheaper ...
You can imagine that you can optimise the relation between the smart technology, the individual’s skill and the level of training you might want to give them.

Other interviewees worried that ‘smart’ surveillance systems were simply reducing the level of input operatives could have:
End User Organisation Representative 2:
We do a bit of training at the moment which is all about behavioural baselining, to our front line staff. We tell them this is the norm, you know the norm, you see it and we wouldn’t want to lose that or for them to become reliant on technology they think will do that, we wouldn’t want that or to risk that. What we need to say to them is that they know what the norm is, we can tell them that and then the important next step is for them to know what to do in those situations, to know if they should intervene, call someone in an emergency, make a note of it, depending on the severity of it. And if you take staff out of the equation ...

Returning to the first interviewee featured in this section, their suggestion was that ADDPRIV might lead to a reduction in the level of importance that the individual surveillance operative might have, a loss of autonomy, but also at the same time require that they had a range of new skills to learn:

Academic 3:
I think their role [operatives] would change a lot with this sort of technology. Part of what they enjoy about their job is that ... they get to feel important in the security hierarchy. They have this knowledge and skill and it gives them a sense of occupational merit. It gives them a certain sense of value to their occupation and it would be a big transformation in their position. And it would strip them of some of their autonomy. I’m imagining that they also might have to be considerably more skilled than they are now and that has its own problems.

Interviewees suggested that operatives might have to adopt new roles in relation to the introduction of the ADDPRIV system, that these roles could be significantly different in terms of working practices and status than their current roles. The interviewees also suggested that operatives’ unique skills might be lost or at least marginalised by ADDPRIV. However, interviewees could also see that ADDPRIV might
lead to new skills and new training opportunities, new ways to deploy staff, making their work more straightforward and ADDPRIV might even address long held concerns regarding operative bias.

Technology shaping the end user:
Interviewees questioned the extent to which the ADDPRIV technology would shape the practices of end user organisations. This was presented as both a positive and negative issue. On the positive side, interviewees were broadly supportive of the idea of introducing a privacy enhancing technology that might introduce a new standard for ethical surveillance technologies. On the negative side, interviewees questioned who had made design decisions – for example, regarding what counted as suspicious – and how those design decisions might have consequences that needed to be held to account. In the following excerpt, a Data Protection Officer draws together these issues:

Data Protection Officer 2:
The general problem with this intelligent video technology, certainly it is conceivable that technology might be useful to restrict the amount of capture and the amount of data that is being collected in the first place, the question is under what criteria, or who has decided what kind of behaviour should be captured, what is normal behaviour, what is abnormal behaviour, where the camera should start running as it were. That is the crucial question...
The responsibility should certainly be with the designers and the institutions applying these technologies. We would certainly feel in a position to give advice in this process and say there should be certain principles to keep in mind, and to put it bluntly ... [it] should not be for a machine to decide under which conditions video surveillance should take place or not. That is a decision that in the end, what happens to the data collected is a decision that should be taken by humans and not by machines.
These concerns were developed further by another Data Protection Officer, who was concerned that new technologies for collecting data, delivered at lower costs to organisations some distance from state regulation, might make accountability challenging:

Data Protection Officer 4:
Where I worry, we’re seeing what I regard as some more proactive uses of CCTV, I’ll put it that way, rather than what was once the benign eye there that would record things. Your smart technology is one proactive way of using CCTV, but we’ve seen it with ANPR and to a much lesser extent with facial recognition, and how the cost base with ANPR equipment has dropped so this isn’t just what the state gets up to, this is what car park operators get up to, and that’s produced a step change in the amount of vehicle information that’s available and you’ve created a pretty robust framework of surveillance around the country. That causes all sorts of challenges about that information who it can get exchanged with and so on. I’ve seen a direction of travel of the cost base dropping and so it can be used in ways that I wouldn’t think were warranted.

Within this issue, we can note that Data Protection Officers in particular were concerned with the ways in which design decisions might shape the practices of end user organisations and how those design decisions might be made accountable. Of the issues discussed thus far, this was a concern only held by a small number of interviewees.

Ethics/law and end use:
A number of interviewees wanted to discuss the relationship between end user settings, the ADDPRIV technology and either legal regulation or moves towards developing an ethical technology. The concerns articulated here were that any move towards ethics also had to be legally compliant (as we have already noted with discussions of data retention and proportionality). However, moving beyond this way
of framing the issue, some interviewees also wanted to discuss who the end users were for surveillance footage and what was their view on ethics, law and, for example, deleting. These issues are drawn together by the following end user representative:

End User Organisation Representative 4:
With the images, with how we get them, if they're transferred, disseminated, processed.... There are lots of challenges involved in locating and extracting usable CCTV material and presenting that ... CCTV control rooms aren’t the end users, we’re [police forces] not the end users, it’s the courts who are the end users and to get a result, to get a result with CCTV we’ve got to make sure that the evidence is sound and I’m worried that with technology and with intelligent technologies we’re going to have a lot, lots of problems with how we present, with the law and admissibility of CCTV in evidence. We’ve got to be practical, we’re humble police officers trying to catch the bad guys and for us, it’s about protecting the public, using images for evidence purposes and if technology innovations help us then great, but I’m not convinced with how that’s going and especially when we’re talking about forensic images, it’s people and processes that are more important than technologies. I think that’s always the case.

The response here suggests that careful thought needs to be given to a range of potential ‘end use’ settings and what it would mean for those setting to move to, for example, reducing the amount of video surveillance data that is seen or stored. The suggestion that courts of law might be considered as end users could significantly re-shape the end use impact assessment of the ADDPRIV project.

Prior to offering a summary of the issues raised by interviewees in considering end use impact issues relating to the ADDPRIV technology, the results of the dialogue workshops will be presented. Subsequent to considering this data, a summary will be offered of both the interview and workshop data.
4.3.2 Workshops

The four dialogue workshops produced rich discussion of issues relevant to the development and potential implementation of the ADDPRIV technology. The following analysis focuses only on those results relevant to ADDPRIV end use. Gathering together and coding the data received from the four workshops, it was possible to draw together 11 themes that characterised the discussions of end use. These could be further grouped together into a simple scheme of positive, open and negative potential end use impacts. Below is an initial summary of this simple scheme, followed by a more in-depth analysis:

Positive themes

1. A reduction in trawling
2. A reduction in function creep
3. An ethical solution to other environments

Open themes

4. The system may not be adopted by police forces
5. The system may result in less clear accountability
6. There may not be high demand for the system

Negative themes

7. This will lead to a deskilling of operatives and a loss of jobs
8. This is too complex for end-users
9. This will reduce the possibility of identifying witnesses
10. This will increase function creep
11. Deletion will lead to a reduction in security

Positive themes: Although the positive feedback from the dialogue workshops is represented here by only three themes, the majority of the discussion in workshops was positive and the ADDPRIV technology was broadly welcomed by most participants.
as a move toward developing and taking seriously the possibility of an ethical surveillance system. Participants in two of the workshops discussed the positive impact on end use that would emerge from a reduction in operatives trawling through surveillance footage. This was deemed a positive step forward in terms of both making surveillance operations more efficient and also in terms of an ethical impact; only those connected to a relevant event would be seen. Participants in three of the workshops also suggested designing a system like ADDPRIV would cut down on function creep – that is, the use of a surveillance system for ends other than those it was designed for (although see the negative themes below). This was identified as a positive end use scenario as it might enable end user organisations to build a greater trust with those passing through end user sites. Also, participants in two of the workshops identified that ADDPRIV was an ethical system that could be rolled out into other end user environments creating a broad positive impact. In particular, settings such as museums and galleries were discussed as potential sites where the ADDPRIV technology could be used.

Open themes: Some of the feedback from participants was neither strongly negative nor positive. Instead it took the form of issues that participants introduced that they were uncertain about – particularly as ADDPRIV is still a technology under development. Participants at times felt uncomfortable trying to predict the future impact. We have termed these discussion themes ‘open’ issues. Many participants felt that the impact of ADDPRIV would be limited by the possibility that the technology might not be welcomed by police forces. Other participants went further and suggested that organisations that deploy surveillance systems in general might not welcome the ADDPRIV technology. For both sets of participants the concern here was with the limitation on visibility that ADDPRIV would impose and the limitation on data storage. A less common ‘open’ theme was the potential impact of ADDPRIV on organisational accountability. This was asked as a question rather than raised as a point of criticism. The question was: what would happen to organisational accountability with so much activity (event detection, auto-deletion) delegated to the technology?
Negative themes: Although the dialogue workshop discussions were broadly positive, there were a number of negative themes regarding ADDPRIV end use that emerged. Several participants across three of the workshops suggested ADDPRIV would lead to a deskilling of operatives (who would become nothing more than button pushers in response to the technology) and would result in a loss of jobs (as fewer operatives could be used to run the ADDPRIV system). Other participants focused instead on organisations rather than operatives specifically and felt that ADDPRIV would be a too complex system to install, operate and maintain. A small number of participants also argued that ADDPRIV’s reduction of visibility and data storage would make it harder to identify witnesses to events. In contrast to the positive themes that emerged, participants in one workshop argued that ADDPRIV would lead to an increase in function creep with, for example, the user interface or deletion system simply being switched off, leading to an enhancement of the surveillance capabilities of the organisation using the technology. Finally, participants in two dialogue workshops argued that auto-deletion would lead to a decrease in security in end user sites as data would no longer be available for historical searches.
5 Discussion and Conclusions

This section draws together the results of the interviews and demonstrations conducted with the end users in the consortium and draws conclusions based on the working practices and feedback received. The feedback of the potential end users is also summarised.

5.1 Summary of End User Organisations Feedback

This section contains summaries and discussions of the information gathered from SEA and Renfe during the course of the project. Conclusions are drawn regarding the potential impact of the system in the end user organisations and the requirements the end users would have for alterations to the system, if it was to be implemented.

Event Detection

Two end users, participants in the Renfe demonstrations and a participant at the End Users’ Advisory Board, made mention of existing equipment which was supposed to automatically detect something, but which was not in use due to the false alarm rate being too high. The false alarm rate would need to be acceptably low if ADDPRIV is to provide a viable solution to the end users.

Events suggested by both end user organisations related to gatherings of people. SEA’s operators are monitoring the CCTV for growing queues, while Renfe participants suggested an event be defined to detect crowds. Intrusion was also considered by a Renfe participant as being potentially applicable in the areas where trains are stored overnight. The potential application of event detection will be further discussed in Deliverable 6.4. Involving employees in events that are detected was also raised by a SEA participant and a participant in the End Users’ Advisory Board and this would have to be taken into consideration in planning for any potential implementation of a system such as ADDPRIV.
**Route Reconstruction**

The route reconstruction component of the ADDPRIV system was interesting to the representatives from both organisations. Possible uses put forward were using it to improve responses to events in helping to find the individuals of interest and using it to reduce the amount of video to be watched in real time when conducting an investigation subsequent to an event. It would be necessary to ensure that this element of the system was reliable.

**Deletion**

As previously mentioned, issues have arisen with regard to the deletion of video footage in the system, if ADDPRIV were to be implemented as envisaged. The lengths of the retention periods at present are in accordance with national laws. Concern was expressed by both the end user organisations as they are required to hold on to all footage for a set length of time and they could be subject to a request for that footage by another authority, for example the police. The organisation may not necessarily be told why that footage is required by the other authority. Where a video segment for a certain time period is requested as opposed to requesting footage for a specific event, if ADDPRIV had not detected an event on the relevant camera at the right time that footage would not have been retained. Alternatively, even if an event was detected, if it was reviewed by an operator and they had not deemed the footage to be relevant, the footage would be deleted once the time threshold (currently 24 hours) had been reached. This issue would need to be addressed if the system were to be adopted.

During the End User’s Advisory board meeting, some suggestions about ways in which this system could be applied within the end users’ organisations were put forward. A representative for a public transport company proposed that such a technology could have applications during exceptional events, such as a football match, for example. However, he indicated that this would still require the involvement of Police officers as regards the decision of what footage could be deleted or not.
It is concluded from the feedback that, given the current requirements placed on the end users in terms of video storage and the necessity to produce it upon request, the current deletion component of the ADDPRIV solution is not suitable for implementation in these organisations for the purposes of security monitoring. It was put to those present that the ADDPRIV system could have applications to address the logistical or safety requirements of the end user organisations to which they agreed. Any change of application would require new events to be identified and defined within the system.

**Interface**

As outlined in the feedback from the participants in discussions at Renfe, several changes to the event list page would be desired if ADDPRIV were to be implemented. This would include changes to the filtering functions for sorting the events, and what information is provided about the detected events in the event list.

**Video Analysis**

The concern was raised by Renfe that for an organisation such as theirs, where they are remotely monitoring hundreds of stations, the practical consideration of where the video will be analysed needs to be addressed. This could be further developed in any future research into scaling the system to work on larger camera networks than the test area.

**Timing**

For some of the events which are currently detect by ADDPRIV, the response time to these incidents could be critical for end users, for example, the abandoned luggage in an airport. If the ADDPRIV system were to be implemented with a view to reacting to, and intervening in, incidents when they are detected, then the time taken by the system to relay the relevant information and footage could pose an issue for some of the end users. In addition to, participants for both end user organisations responded that it would be better if the video clips of the event itself were longer than is currently the case.
Operators

At present, it is the case in both end user organisations, SEA and Renfe that only specific employees have the authority to review recorded footage (as opposed to the live camera feeds), authorise the extraction of the footage or carry out the extraction of that footage. The operators themselves are not entitled to review the recorded footage. If the police make a request for footage from the archive, then a specific employee from the CECON will review it with them. Copies can be made for the police. If ADDPRIV were to be implemented, it would put the operators in the position of reviewing video associated with the trigger events. In the case of both end users, this could result in non-manager level employees reviewing recorded footage, where, previously, they would have been working solely with live footage. In addition to this, there would be the responsibility of deciding which events are relevant to security, and which are not. In the case of SEA, this would represent an extra task for the control room operators, who currently monitor fixed CCTV footage for crowd control purposes. In Renfe’s case, it was pointed out that this would represent a significant extra time burden on the operator, to the extent that it was suggested that a dedicated operator for reviewing the detected events would be required.

As the system would require alterations to its original specification, as it was originally intended, it is difficult to be explicit in outlining the expected user profiles for the organisations. There follows an outline of some of the main user roles which could be required by an end user organisation if the ADDPRIV system were to be implemented. Not every job profile would be feasible, with the size of a given organisation’s camera network and its responsibilities being a guiding factor.

IT / administrator role: This user profile would allow the user to access only the User Management functions of the ADDPRIV system. User Management would be the only tab to appear in the interface when they log in. Users in this role would be responsible for creating user profiles, assigning access levels and allowing for the resetting of passwords when necessary (this would be done without the administrator seeing the password of another user).
Security operator (reacting to events): This user profile would allow the user access to the event detection list and to view the event. If this same user is to be the user who reviews and reclassifies an event as relevant or not, then it introduces a new responsibility to the operator’s role, as currently operators are generally not the ones who review video footage (taking into account only the commercial end users, not police forces). The operator would be reacting to events and putting in train the correct procedure for responding to the event.

Security personnel (reviewing events): This user profile would allow the user to access the event list and change the status of events. This user could also search past events and review sections of video based on a time period (if the function is added), such as described during the discussions with Renfe personnel.

**Training**

Currently, operator training relates to the technical operation of the technology in the control room and to response procedures to the different alarms / alerts that are raised. The ADDPRIV system would introduce several new aspects into the tasks of operators, for which new training would need to be developed if the system were to be implemented in its current format.

As part of the ADDPRIV system, operators would be put in the position of deciding which events count as security relevant and which do not. In the case of SEA, this would introduce a new task to the role of the security operators, whose primary use of the CCTV in the control room at present is crowd management. In the case of Renfe, while security is a responsibility of the CECON, as one member of security personnel pointed out, the designation of “relevant” or “irrelevant” to security would be based on the point of view of the operator, or Renfe. If the operators were to decide the relevance of an event to security, i.e. more than simply indicating if the event was correctly detected or not, then their training will need to incorporate more than merely the operation of the technology. One attendant at the End User’s advisory board felt that no operator should be in a position where they are pre-empting the courts in deciding what video footage counts as security relevant and what not.
As in both SEA and Renfe, operators are tasked with initiating the correct response procedure to intervene in whatever alarms they receive in the control room, new response procedures for the “events” defined within the system would also have to be developed. The issue of introducing different level alerts was raised during the course of the interviews to which it was suggested that each type of event could require a different type of response.

**Movable cameras**

For one of the end users the ability to track was described as “critical” and an attendee at the second set of demonstrations asked how ADDPRIV would cope with detecting events on a moving camera. This would require further research and details on ideas for future research and development will be provided in Deliverable 6.4.

**Additional Functions and Further Developments**

During the course of the first set of tests in Linate, an additional option was discussed for inclusion in the tab menu at the top of the interface. This option was nominally called “View Segment”. Various functions were considered for inclusion under this heading, including the possibility to view live footage and of allowing those operators who were appropriately authorised to retrieve sections of video, which they would specify based on a time or date range. Feedback from the Renfe operators suggests that, for their organisation, this function would be desirable.

In SEA, some of the end users involved in the discussions suggested that being able to classify events may aid in reacting to them. Where the introduction of a scale for the alerts was first suggested by an interviewee, they gave the example that a piece of abandoned luggage could be perceived to be more dangerous than a counter flow alert. Further to that, the respondents felt that the alerts should be more than simply another line of text appearing in the list. Respondents suggested that visual and audible elements could be added to the alerts to help bring it to the attention of the operator and, assuming different alerts for different “levels” of event, identify the urgency or type of event which has been detected. Renfe participants suggested all of
these options should be configurable when the system is being set up. Developing a function that allows operators to receive alerts to hand held devices was mentioned, by one of the end users in SEA, as a possible future enhancement of the system, if the alerts were developed.

It should also be noted that both end user control rooms have some form of log for the actions carried out in the control room, or in the video recording area, and that, at present, no log exists within ADDPRIV for the actions carried out within the system. In this light, given that certain actions within the ADDPRIV system could lead to the deletion of video footage were the system to be implemented in its current form, it may be prudent to incorporate a log in the system to track actions carried out within ADDPRIV. As logs already exist in both organisations, the authority to review the logs has already been assigned to certain employee roles. The permission to review the logs would need to be added to the user profiles of these employees, or a new role which incorporated reviewing the logs (such as a Security Manager level) would need to be defined.
### 5.2 Summary of Potential End Users Feedback

The preceding analysis of end use impacts derived from interviews and dialogue workshops has introduced a number of themes of discussion. In the analysis, many of these themes have produced both positive and negative questions of ADDPRIV end use impact. In the following table, the 6 themes from the interview analysis are used to organise a summary of these negative and positive questions:

<table>
<thead>
<tr>
<th>Theme</th>
<th>Positive</th>
<th>Negative</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business case</td>
<td>• No new surveillance infrastructure required</td>
<td>• Staffing costs</td>
</tr>
<tr>
<td></td>
<td>• Help build a market for ethical surveillance technology</td>
<td>• Questions of efficiency</td>
</tr>
<tr>
<td></td>
<td>• An ethical solution to be used in other locations</td>
<td>• Questions of effectiveness</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• There may not be high demand for the system</td>
</tr>
<tr>
<td>Technical sophistication</td>
<td>• Straightforward system (no face recognition)</td>
<td>• Does the technology work?</td>
</tr>
<tr>
<td></td>
<td>• Enables proactive intervention</td>
<td>• Is too much data deleted?</td>
</tr>
<tr>
<td></td>
<td>• Reduces trawling</td>
<td>• Is it proportionate?</td>
</tr>
<tr>
<td></td>
<td>• Reduces function creep (?)</td>
<td>• Will it increase function creep?</td>
</tr>
<tr>
<td>Evidence handling</td>
<td>• Reducing police work in preparing evidence</td>
<td>• Admissibility of evidence</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Deletion of surrounding data</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Ability to identify witnesses?</td>
</tr>
<tr>
<td>Operator role</td>
<td>• Reduce operative bias</td>
<td>• Lose operative skills and status</td>
</tr>
<tr>
<td></td>
<td>• Enhance operative skills and training opportunities</td>
<td>• Lose unique operative knowledge</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Loss of jobs</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Too complex for end user organisations to install</td>
</tr>
<tr>
<td>Technology shaping end user</td>
<td>• A new standard for ethical surveillance technology</td>
<td>• How to make design decisions accountable?</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• How to make the system accountable?</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Deletion will lead to less secure end user settings</td>
</tr>
<tr>
<td>Ethics/law and end use</td>
<td></td>
<td>• Digital treatments impact evidence</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Who are the end users?</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• May not be adopted by police forces</td>
</tr>
</tbody>
</table>
5.3 Concluding remarks

Overall, the response to the concepts and solutions proposed by the ADDPRIV project to those who would be using the system in the consortium’s end user organisations, Renfe and SEA were generally positive. The participants from both organisations saw different potential for the application of the Route Reconstruction and Event Detection components to their work. However, the reliability of both would have to be assured if the system is to be implemented successfully. There were considerable concerns expressed about the deletion of “irrelevant” footage before the limit set by the law was reached. In addition to this, doubt was expressed about the feasibility of installing this system on so broad a station network as that monitored by Renfe.

It is clear from the feedback of end users that the current specification of the system would not be suitable for implementation as a security monitoring system for these organisations, without significant alteration. Correspondingly, one of the negative points raised by the potential end users was a query as to whether police forces would adopt the system. However, allowing for the adjustments that would need to be made, each end user could identify potential uses for the system, such as investigation of events subsequent to an incident or for use as an aid on occasions when dealing with unusually large numbers of people. The potential end users in the workshops also saw potential in the system, as the research project represents progress towards ethical surveillance.

The adaptation requirements and suggestions mentioned by the end users will be discussed in more detail in the section covering future research and design considerations in the ADDPRIV Deliverable 6.4 (forthcoming).
6 References


