END USER RESPONSE TO AN EVENT DETECTION AND ROUTE RECONSTRUCTION SECURITY SYSTEM PROTOTYPE FOR USE IN AIRPORTS AND PUBLIC TRANSPORT HUBS

Orla McCarthy
Centre for Transportation Research,
Department of Civil, Structural & Environmental Engineering
Trinity College Dublin
Dublin, Ireland
Tel: +353 1 8962084
Fax: +353 1 6773072
otmccart@tcd.ie

Margaret O'Mahony
Centre for Transportation Research,
Department of Civil, Structural & Environmental Engineering
Trinity College Dublin
Dublin, Ireland
Tel: +353 1 8962084
Fax: + 353 1 6773072
margaret.omahony@tcd.ie

Word count: 6221 + 3 tables/figures x 250 words (each) = 6971 + 26 references

Submission Date: 1st August 2015

ABSTRACT

Video surveillance is extensively used in many countries for security purposes, contributing to effective prevention, detection, and/or prosecution of crime and terrorism. Although its contribution to security is not under debate, its effect on the privacy rights of citizens has been the subject of much controversy. This paper reports the results of research which examined the potential use of new security technologies in an airport and a major public transport hub. The research aimed to consider both the security and privacy implications of new security technologies, specifically closed circuit television (CCTV) with automatic event detection, alerts, and route reconstruction (to determine the route taken by a suspicious person in advance of a detected incident). The system also allows for the deletion of any footage not associated with the detected events or reconstructed routes, when that footage was considered not relevant to security. Interviews and technology demonstrations were conducted with employees of two transport organisations, the airport operator of Linate and Malpensa Airports in Milan in Italy, SEA, and the Spanish railway operator, Renfe Operadora. The main findings are that, while facets of the system appeal to the transport organisations, changes would need to be made in order for it to be implementable. Particularly, the respondents pointed to the early deletion of the non-security relevant footage as an issue due to legal requirements placed on them.

Keywords: security, privacy, CCTV, end user response.

INTRODUCTION AND BACKGROUND

Security technology involving surveillance brings its own concerns. A study which conducted 592 hours of observation of CCTV control rooms between 3 sites and found that almost 40% of those targeted for surveillance were surveilled for no obvious reason *(1).* They also found that 90% of targets were male and that black people had a higher chance of being targeted for surveillance. Other research suggests that the proliferation of technologies is altering the way police agencies handle urban space and recommended that consideration be given to the impact of automation of these systems on people and cities *(2).* It was highlighted in other research that using data for a purpose other than the originally intended use is becoming common Coudert *(3).* She also comments on the presentation of privacy and security as being a zero-sum relationship, where more privacy means less security and more security means less privacy, and that shorter retention periods for footage is among measures introduced to minimise the impact on individuals' privacy *(4).* The Ontario Information and Privacy Commissioner's Office strongly rejected the use of the zero-sum concept in relation to privacy and security in the context of a complaint against the Toronto Transit Commission (TTC) and said that they should be allowed to collect personal information through the use of video surveillance as it was necessary to the proper administration of Toronto's mass transit system *(5).* However, they recommended, among other things, that the TTC reduce their retention period of footage to 72 hours from 7 days.

In an effort to mitigate the privacy intrusion of CCTV, other work proposed a system in which the video footage is encrypted and stored within the camera, from where it can be retrieved and decrypted and viewed only if a crime occurs *(6).* A trial was carried out with certain retailers in Kiryu City, Japan, where the images could only be viewed using special software installed in the computers at the police department. A further experiment in the city involved the installation of the cameras on lamp posts in a residential area (the image owners were a Parent-Teacher Association of a high school). The results of the experiment (which was running for at least 6 months), from the points-of-view of the camera owners and local residents, were that the system was effective from both safety and privacy perspectives, and the system was considered affordable.

In another discussion paper, it was suggested that the organisational need for evolved CCTV systems can be attributed to, among other things, the proliferation of CCTV systems *(7).* The paper highlights that there are also practical difficulties with operating a smart surveillance system and that there is a gap between users' expectations… and… the reality *(7).* Other research reports on a CCTV system which allows for searching video based on detected video objects. The authors mention the need to take the users into consideration in the design of such systems. Otherwise, a situation could arise whereby all the advanced and promising underlying technologies end up mismatching the end users' searching and browsing needs *(8).*

Dubbeld *(9)* investigated the impact technology has on CCTV surveillance practices. A case study was conducted of a central control room for CCTV for 15 stations, set up by a Dutch railway company, using observations, various interviews, a review of relevant documents (and articles) and attendance at company meetings. Among the results, it was found that technical objects steer operators' monitoring capacities and behaviours, thus affecting the levels of surveillance achieved in a system of CCTV *(9)*. The Urbaneye project incorporated studies completed in seven European countries; Austria, Hungary, Germany, Great Britain, Norway and in parts of Denmark and Spain. One method used for gathering information was to survey (using questionnaires) people involved with the CCTV systems, such as owners or managers *(10)*. Information sought included;

- The system's owners and operators
- Whether or not there was notification of the system
- The monitor-camera ratio of the system
- Whether or not observers could watch the system in real-time
- Whether or not the images were recorded.

Also studied were the control room routines and surveillance practices of some participants *(10)*. They find that house rules are often an essential part of this risk management regime, and CCTV is used to support the enforcement of these rules. They noted that the system relies on the CCTV operators targeting, interpreting and reacting to a scene from a distance according to a specific purpose. The sensory limitations imposed by this distance and the observation occurring through a video screen was found by the researchers to encourage the application of categorical suspicion based on narrow range of readily observable traits rather than the application of behavioural suspicion *(10)*.

Other research examined the issue of privacy in the development of ITS *(11)*. Two surveys were conducted: the first with state agencies responsible for commercial vehicle security and the second concerning both personal and commercial vehicle operators. One of the conclusions of the research was that future implementation of technologies would be influenced by public privacy concerns *(11)*. One of the perspectives which came out of this work, concerning civil rights, was that non-criminals could be forced to change their daily routines and modify their behaviour. Their recommendations included that CCTV managers must be professionally accredited and made legally responsible for compliance with human rights, data protection and associated codes and that systems should be subject to routine and random inspections and evaluations.

An EU funded project, entitled PACT (Public perception of security and privacy: Assessing knowledge, Collecting evidence, Translating research into action) presents the results of a pilot survey with a discrete choice design, but based on train or metro travel in Europe *(12)*. The attributes used in the discrete choice scenarios were recognition capabilities in CCTV cameras; time period for storing the CCTV information; who has access to CCTV information; type of security personnel at the station; security measures at the station; time to pass through security checks and related queues, and additional security surcharge (on top of ticket cost). Among the results, it was shown that advanced CCTV technologies were preferred to standard CCTV and that retention of CCTV footage was preferred to it not being recorded. The results regarding the level of access to the footage suggested that it was not an attribute to which the respondents were particularly sensitive *(12)*.

Other work looked at the purpose of CCTVs and their effectiveness in counter-terrorism security *(13)*. The authors determine that CCTV would be more effective for deterring street crime than terrorism, especially in the case of a suicide terrorist act, and that the footage could be used by the terrorist organisations. Another study mentions non-crime related uses for CCTV such as finding missing children and encouraging residents or visitors to visit an area, among others *(14)*. The authors conclude that too much must not be expected of CCTV. Other researchers have concentrated on the discourse on privacy and CCTV in society *(1, 15, 16)*; while others, *(17, 3, 4)* have studied the issues from the perspective of the law or its interpretation.

The EU funded project entitled Automatic Data relevancy Discrimination for a PRIVacy-sensitive video surveillance (ADDPRIV) *(18)* aimed to develop a system for CCTV which has event detection and route reconstruction functions. In this case, route reconstruction means the route an individual took prior to being identified as associated with a security event as determined by the network of cameras employed in the airport or public transport hub. The intention of the ADDPRIV system is that CCTV footage involved in the detection of an event or a route reconstruction will be retained, allowing footage that is not considered relevant to security to be deleted. The purpose of the research presented in this paper is to investigate the practical implications of implementing the ADDPRIV solution in transport end user organisations. The end users in the project consortium were 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 research conducted for this paper sought to analyse how the personnel in the end user organisations responded to the prototype, more detail of which is presented in the project deliverables *(19)*. 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. The paper first summarises the system interface and then focuses on the demonstrations conducted to collect end user feedback on the ADDPRIV system *(20)*. The feedback is analysed and its findings are discussed from which the resulting conclusions from the work are drawn.

METHOD

ADDPRIV´s approach is based in the principle that discrimination cannot be implemented at the level of a single camera but at the multi-camera network level as a whole. The suspicious behaviour of one individual generates an alert event in one of the network cameras. This alert triggers the instruction to other cameras in the network for automatic detection of that same individual (features recognition) by browsing scenes stored in certain time windows. The development of these solutions is based on implementing artificial intelligence for learning algorithms, so that they can be rapidly and effectively adapted to different infrastructures and changing situations.

The ADDPRIV System

This section provides a brief summary of the system architecture in order to provide context for the following discussion about the individual components *(21).* Figure 1 shows the main components and their interactions.

- A multi-camera network provides input video frames to the Media Proxy (MP) system. The MP has the main goal to enrich and synchronise video frames with a timestamp used later as a unique ID for all the video systems. Both event detection (ED) and route reconstruction (RR) systems process the frames received in real-time to generate internal metadata and tagging information for the respective goals: find and describe security relevant events (ED), prepare metadata (RR) to be used later when building route reconstruction trees.
- The ED is in charge of discovering security relevant events, such as unattended luggage. As a consequence it sends an event descriptor (red arrow) to the privacy enhancement (PE) system that stores it into the ADDPRIV system permanent storage.
- The PE sends the event descriptors received from ED to the RR system thus triggering the creation of a RR tree of video frames that are related to the event received (black arrow labelled Route Request).
- The RR provides the RR tree related to the route request received to the PE system that stores this information for later retrieval via the user interface (UI).
- In addition to storing events and routes, the PE also saves video streams received from the MP in order to provide videos about detected events when requested by the users. RR optionally can request specific video frames stored in PE as needed by RR internal algorithms. All data stored in the PE is deleted after a configurable time interval unless related to an event marked as relevant.
- The UI retrieves events, routes and videos from the PE in order to allow human operators to interact with the system. Users can give feedback to mark events as relevant or irrelevant *(21).*

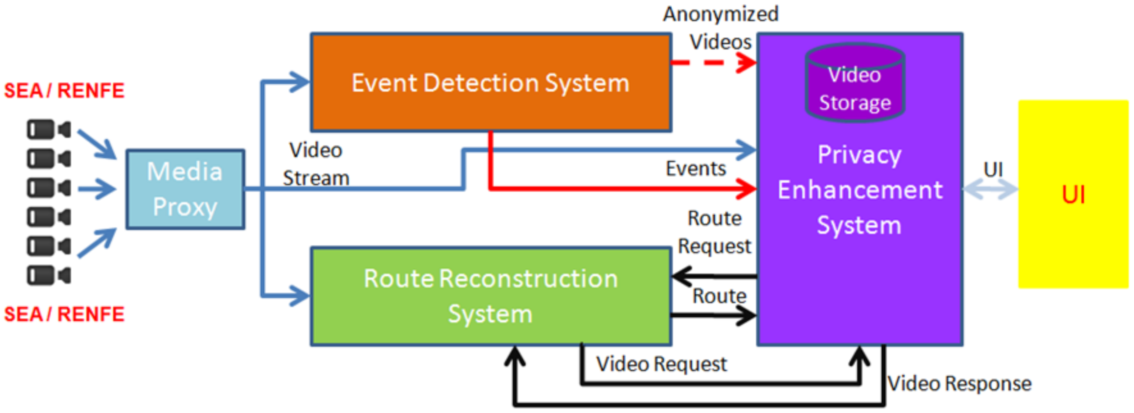

FIGURE 1. ADDPRIV High level Architecture *(21)*

Event Detection (ED)

The ED component is devoted to finding three types of events in the video streams in real-time: left luggage, barrier crossing (intrusion in a forbidden area) and counter flow. The detection of all events is based on moving object detection. Then, the left luggage detection algorithm analyses pixel stabilities in regions denoting stopped objects, while barrier crossing and counter flow detection algorithms combine object tracking with optical flow in order to obtain object movement trajectories and short-term, pixel-level velocity vectors of all objects. The Event Detection component receives video streams from the Media Proxy module and reports events detected with advanced message queuing protocol (AMQP) messages *(21).*

Route Reconstruction

The RR module processes in real time (no local video frame storage) the input video frames to create tagging and metadata used later by the RR algorithms. It receives event descriptors from the PE module and provides as output a route reconstruction tree that collects all the video clips that could be related to the event descriptor received. In order to do this, the module contains a topology database in which to store the information about spatial dependencies between cameras and relevant surveyed sensitive areas. The RR can also request specific video frames from the PE system during the execution of the route reconstruction algorithm. The RR module provides the RR tree related to the route request received by the PE system that stores this information for later retrieval via the UI. The PE module deletes all the video frames that are older than 24 hours (or a configurable time interval) or that are not marked as events or part of a RR tree *(21).*

Privacy Enhancement

The PE system is the integration point of the elements of the ADDPRIV solution. Its main task is to implement the storage, indexing and deletion of the information (both privacy-sensitive - such as video footage - and anonymous data - such as security events being detected). It also orchestrates the interaction between the ED and the RR systems *(21)*

Queries on the collected information are also managed by the PE, which enforces the access levels for each role consulting the data. This way, normal users cannot access privacy-sensitive information that has not been informed as security relevant by the ED or the RR. A special access level is provided for special cases such as national law enforcement agencies requiring access to specific footage *(21).*

Events Tested

The system was developed using recorded video footage and then validated on live streams in a SEA controlled airport terminal. The algorithms were further tested using video footage from a commuter train station provided by Renfe Operadora. The project involved the development of algorithms to detect the events agreed by the end user organisations involved, SEA and Renfe Operadora. Those events were:

- Abandoned luggage
- Intrusion into a forbidden area / crossing a barrier

- Counter flow (a person moving against the direction people are supposed to move – for example in the security queue)

Once an event had been detected, the system compiled footage from across its CCTV network which the system estimated were most probably going to contain the person detected as being involved in the event, from before and after the event up to the point when the event was reviewed. This is shown in Figure 2 where a piece of luggage has been abandoned and the cameras taking footage of the individual who left it are highlighted in red. The intention was that all footage not related to any event or route reconstruction could be deleted, thus reducing the amount of footage of passers-by retained. This is shown in Figure 3 where the time period over which the luggage abandonment event took place is shown in red at the bottom of the figure, on the time axis, indicating that this period of footage would be retained but footage taken outside that time frame would be deleted.

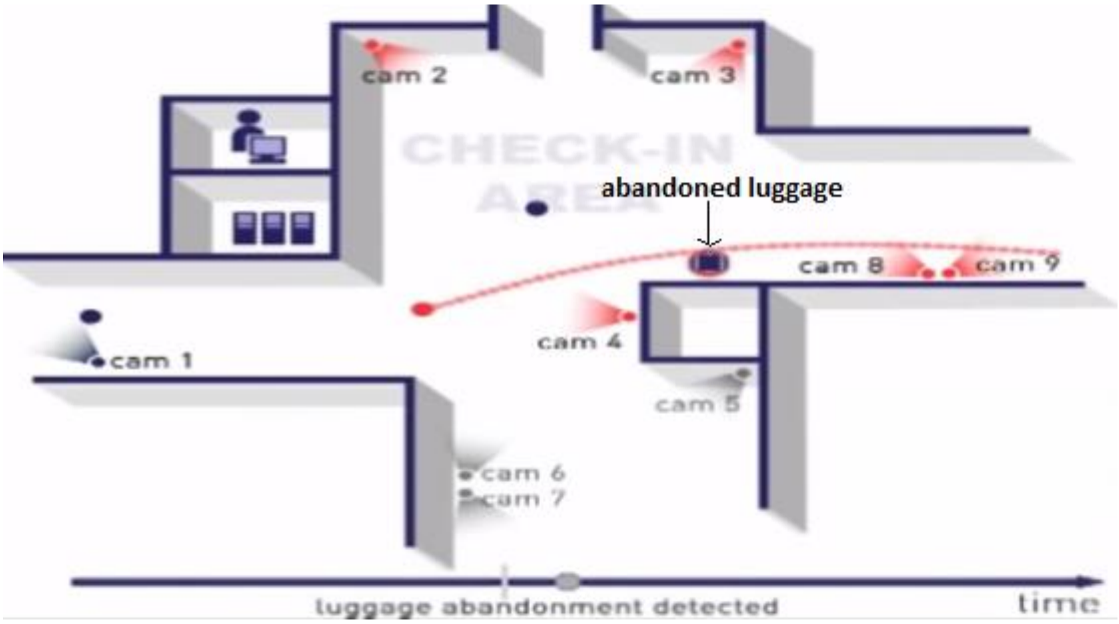

FIGURE 2 Example of abandoned luggage event *(22)*

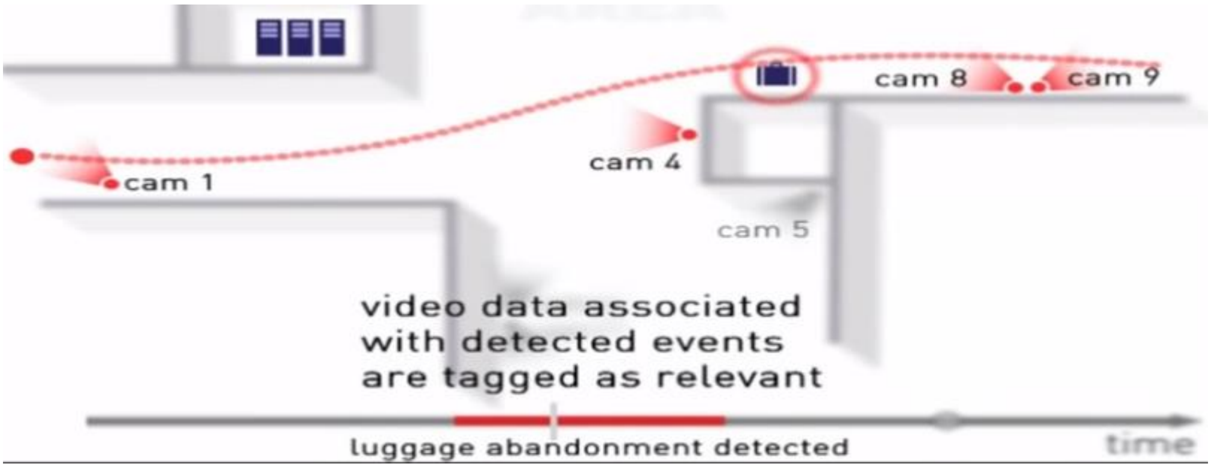

FIGURE 3 Time period during which event took place highlighted for retention *(22)*

Determining Feedback from End Users

The work presented in this paper focuses on the evaluation of the ADDPRIV system’s operation in the transport organisations. Alternative methodologies were considered for gathering feedback, including focus groups and demonstrations of the prototype ADDPRIV system to gauge response. Focus groups involve unstructured interviews or discussion with several respondents at a time, on the topic of interest. This method could have provided rich data in terms of exploring, in-depth, the respondents opinions on a tightly defined topic due to respondents’ discussion and challenging of each other’s views *(23)*. However, it was decided that the topic being researched (privacy and security, and the new security technologies in transport) was too broad to garner useful information from focus groups. There was a risk that while the information collected may be rich, it could also be too nebulous to draw robust conclusions, or identify trends, in the absence of restrictions on the discussion *(20).* In addition, the ADDPRIV system was, at that time, still in its design stage and so it would not be possible to include any respondents in the focus group who had experience of this technology. It was considered that interviewing relevant personnel in the end user companies during demonstrations of the technology would be a better way to proceed.

Site visits were conducted to the airport and the train management companies’ CCTV control rooms. Interviews were carried out with relevant members of the organisation to identify what were the normal operating practices of the organisations, prior to this new technology system being introduced. At the same time, a list of technical questions was sent to the companies involved (SEA and Renfe) to gather information on the technology currently used. The organisations were also asked to identify job roles which could be involved in the management or operation of the ADDPRIV system. The interviewees were provided with an information sheet about the project in either Spanish or Italian and asked to sign an informed consent form (also in Spanish or Italian) *(20).*

The main standards and documents on which the interview questions were based were the Data Protection Audit Resource of the Irish DPC *(24)*, the Closed Circuit Television (CCTV) Management and Operation Code of practice of the British Standards Institution *(25)* and the International Standards on the Protection of Personal Data and Privacy - The Madrid Resolution *(26)*. 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 *(20).*

RESULTS

Feedback from Airport Security Personnel

The first demonstration of the ADDPRIV system to end users took place in the Linate airport offices in Milan. In attendance at this demonstration were airport police officers, head of the airport police, the security personnel of airport operator and CCTV operators. The demonstration began with the playing of the ADDPRIV video accompanied by an explanation of the system, followed by discussion and interviews. The discussion was recorded in Italian and a summary provided in English. The feedback from the end users was broadly positive. Specific feedback on timing, alerts, the user interface, route reconstruction, event detection, event deletion, operator training and future developments are summarised here.

Timing

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 (research stage) was not acceptable. 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.

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 an 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. An abandoned bag would be a priority (it could be a bomb), whereas a counterflow event would be a lower level 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. They 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, would 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.

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.

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.

Another issue noted was 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.

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. The concern was 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. This pointed to a potential loss of flexibility' for the security department.

Future Developments

In terms of possible future implementation of ADDPRIV, it was also suggested 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.

Feedback from Railway Security Personnel

The second demonstration of the ADDPRIV system took place in one of Renfe's control centres in Madrid. A presentation of the system was given 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 technicians, engineers and CCTV operators. The system was demonstrated in the form in which was set up in Linate Airport. The issues raised in feedback concerned integration, video analysis, one-off events, automatic deletion, timing and logistical issues, as follows:

Integration

The attendees at the demonstration felt that the ADDPRIV system would complement the existing systems in the control centre. In the course of the subsequent discussions, the importance of ADDPRIV's integration with the existing framework was highlighted. It was suggested that 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.

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, it would necessitate all feeds, from all cameras, being transferred from the stations to the control centre. Those involved in the discussion felt that this was not viable, not only was the quantity of footage to be communicated to a control centre 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 control centre 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-off Events

A discussion was prompted on the possibility 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 but the attendees did not think that this would be appropriate for the Renfe stations on busy days. The Renfe personnel responded that, were ADDPRIV to be implemented, there would need to be a function which would allow unusual events to be marked for exemption, so that the entirety of the footage for such events or days would be retained.

Automatic Deletion

In addition to the comments about retaining footage from one-off events, another concern 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 more than 30 days old, cannot be fulfilled due to the 30 day retention period legal requirement in Spain. However, if 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. 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

As the control centre deals with footage from so many cameras, a concern was expressed that it may not be possible to review all of the events which would be detected in 24 hours. It was concluded 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 Issues

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 too many false alarms in a system's video analysis functions would result in their being disabled. 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 it would be useful for dealing with aggressive behaviour of people in the stations and with incidents such as 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 are expensive to repair. People crossing the rails was also been mentioned and on further discussion the point was made that some 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.

DISCUSSION AND CONCLUSIONS

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.

The lengths of the footage retention periods at present are in accordance with national laws and can be as high as 180+days in some countries. 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. 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. If non-tagged video has been discarded then it will be impossible to build a case against the perpetrators or perhaps determine what methods, and supporting personnel which were involved in a criminal/terrorist event. Given that both the transport organisations can be subject to requests from external authorities e.g. Interpol, research could be conducted into the legal requirements around Europe for such systems and potentially developing a Europe wide legal framework for the operation of these systems, so that all countries in Europe are subject to the same standards, and companies that wish to innovate their security systems, to enhance privacy protection, are provided with clear guidelines as to what is and is not permissible.

At present, it is the case in both end user organisations 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 control centre 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. 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.

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. The intrusion event was considered as possibly having an application when people cross the rails or to reduce vandalism of train carriages when parked overnight.

ACKNOWLEDGEMENTS

The authors would like to thank SEA and Renfe employees for their valuable contribution.
This research has been carried out as part of the ADDPRIV research project, funded by the European Commission under the 7th Framework Programme, grant agreement n. 261653.
The ADDPRIV project consortium is composed of: 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 (RENFE) and The Provost Fellows & Scholars Of The College Of The Holy And Undivided Trinity Of Queen Elizabeth Near Dublin (TCD).

REFERENCES

1. Norris, C. and G. Armstrong, *The Maximum Surveillance Society: The Rise of CCTV*, Oxford, Berg. 1999.
2. Nunn, S. Police technology in cities: changes and challenges. *Technology in Society*, 23, 11-27. 2001.
3. Coudert, F. Towards a new generation of CCTV networks: Erosion of data protection safeguards? *Computer Law & Security Review*, Vol. 25, 2009. pp. 145-154.
4. Coudert, F. *When video cameras watch and screen:* Privacy implications of pattern recognition technologies. *Computer Law & Security Review*, Vol. 26, 2010 pp. 377-384
5. Cavoukian, A. *Privacy and video surveillance in mass transit systems: A special investigation report. Privacy Investigation report MC07-68.* Information and Privacy Commissioner of Ontario. [Available at: https://www.ipc.on.ca/english/Resources/Reports-and-Submissions/Reports-and-Submissions-Summary/?id=739]. 2008.

6. Prashyanusorn, V., P. Prashyanusorn, S. Kaviya, Y. Fujii, and P.P Yupapin. The Use of Security Cameras with Privacy Protecting Ability. *Procedia Engineering*, Vol 8, 2011. pp. 301-307.
7. Li-Qun, X. Issues in video analytics and surveillance systems: research/prototyping vs. applications/user requirements. 2007 *IEEE Conference on Advanced Video and Signal Based Surveillance*, AVSS 2007, 5-7 Sept. 2007 Piscataway, NJ, USA. IEEE, pp. 10-14.
8. Lee, H., A.F. Smeaton, N. O'Connor and N. Murphy. User-interface to a CCTV video search system. *IEE International Symposium on Imaging for Crime Detection and Prevention* (ICDP 2005), 7-8 June 2005, London, UK. IEE, pp 39-43.
9. Dubbeld, L. The role of technology in shaping CCTV surveillance practices. *Information, Communication & Society*, 8, 2005. pp 84-100.
10. Hempel, L. & Töpfer, E. *CCTV in Europe - Final report - Working Paper No.15. Urbaneye, 5th framework programme of the European Commission*. Available at: www.urbaneye.net. 2004. Accessed July 31, 2015.
11. Fries, R. N., M. R. Gahrooei, M. Chowdhury & A. J. Conway, Meeting privacy challenges while advancing intelligent transportation systems. *Transportation Research Part C: Emerging Technologies*, Vol. 25, 2012. pp 34-45.
12. Patil, S., D. Potoglou, H. Lu, N. Robinson, & P. Burge. Trade-off across privacy, security and surveillance in the case of metro travel in Europe. *Transportation Research Procedia* 1(1), 2014. pp. 121-132. (10.1016/j.trpro.2014.07.013)
13. Stutzer, A. and M. Zehnder. Is camera surveillance an effective measure of counterterrorism? *Defence and Peace Economics* 24 (1), 2014. pp 1-14.
14. Gill, M. and A. Spriggs. *Assessing the impact of CCTV*. London: Home Office Research, Development and Statistics Directorate. 2005.
15. Norris, C. & G. Armstrong. CCTV and the rise of mass surveillance society. In: Carlen, P. & Morgan, R. (eds.) *Crime Unlimited? Questions for the 21st Century*. London: Macmillan Press Ltd. 1999.
16. Neyland, D. *Privacy, Surveillance and Public Trust,* Basingstoke, Palgrave Macmillan. 2006.
17. Agustina, J. R. & Galdon Clavell, G. The impact of CCTV on fundamental rights and crime prevention strategies: The case of the Catalan Control Commission of Video surveillance Devices. *Computer Law & Security Review*, Vol. 27, 2011. Pp 168-174.
18. Anova IT Consulting, Trinity College Dublin, Politechnika Gdanska University, Goldsmiths, University of London, Hewlett Packard Italiana Srl, Societá Per Azioni Esercizi Aeroportuali SEA SPA, Avanzit Technologies S.L., Renfe Operadora and Kingston University. 2013. *Deliverable 6.4.* ADDPRIV project, www.addpriv.eu. Accessed July 31, 2015.
19. Hewlett Packard. *Deliverable 5.4: Report on performance test results, in the application context, and improvements required in the different solutions*. ADDPRIV Project, 2013. www.addpriv.eu Accessed July 31, 2015.
20. McCarthy, O. *Public transport, security technology and privacy: an analysis of operator organisation and public response.* PhD thesis. University of Dublin, Trinity College. 2015
21. Anova IT Consulting, Trinity College Dublin, Politechnika Gdanska University, Goldsmiths, University of London, Hewlett Packard Italiana Srl, Societá Per Azioni

Esercizi Aeroportuali SEA SPA, Avanzit Technologies S.L., Renfe Operadora and Kingston University (2013). *Deliverable 6.4. Conclusions on Future Work for Adoption of ADDPRIV Solutions*, ADDPRIV consortium, www.addpriv.eu 2013. Accessed July 31, 2015.

22. Anova IT Consulting, Trinity College Dublin, Politechnika Gdanska University, Goldsmiths, University of London, Hewlett Packard Italiana Srl, Societá Per Azioni Esercizi Aeroportuali SEA SPA, Avanzit Technologies S.L., Renfe Operadora and Kingston University (2013). *ADDPRIV website*, www.addpriv.eu. Accessed July 31, 2015.

23. Bryman, A. *Social Research Methods*. Oxford University Press. 4th ed.2012.

24. Data Protection Commissioner (Ireland). *Data Protection Audit Resource*. [Online] Available at: http://www.dataprotection.ie/documents/ enforcement/AuditResource.pdf. 2009. Accessed July 31, 2015.

25. British Standards Institution. *BS 7958: Closed Circuit Television (CCTV). Management and Operation. Code of practice*: 2009. BSI.

26. Spanish Data Protection Agency (Coordinators) & Working Group. *International Conference of Data Protection and Privacy Commissioners- The Madrid Solution*. Madrid. 5 November 2009: Available at: http://www.agpd.es/portalwebAGPD/canaldocumentacion/conferencias/common/pdfs/31_conferencia_internacional/estandares_resolucion_madrid_en.pdf [Accessed July 31, 2015].