Harmonized Evaluation, Certification and Testing Of Security products

# D6.2
# Report on ethical/human rights aspects of application scenarios

**University of Warwick**

Date: 2015-07-14
Project No: 606861
FOI Designation No: FOI-2012-1271
Dissemination Level: PU
Total No of Pages: 55

This project has received funding from the European Union's
Seventh Framework Programme for research, technological
development and demonstration under grant agreement no 606861.

# D6.2
# Report on ethical/human rights aspects of application scenarios

| | |
|---|---|
| Version: | 1.0 |
| FOI designation no: | FOI-2012-1271 |
| Responsible: | Dr Katerina Hadjimatheou, UW |
| Author(s): | Dr Jethro Butler, UW |
| Number of pages: | 55 |
| Dissemination level: | PU - *Public* |
| Start date of project: | Sep, 2014 |
| Duration: | 3 years |

# Document information

### Document revisions

| Version | Date | Author | Comments |
|---|---|---|---|
| v1.0 | 2015-07-14 | | First release of D6.2 |
| | | | |

## Summary

This report examines the ethics and human rights risks of the technology use described in the application scenarios specified in D1.2. In doing so, it builds on the work of D6.1, which identified ethics and human rights issues arising in connection with the security product categories developed in D1.1. The most commonly arising issues are: privacy, data protection, freedom of expression, association, and movement, health and safety concerns, proportionality, and issues around consent. Some of these issues can be addressed at the stage of product design and manufacture. Others can only be addressed by changes to the processes and procedures around technology use, such as training of staff, codes of conduct, protocols and standard operating procedures. The potential of privacy-by-design and ethics-by-design certification to address these issues will be examined in depth in a forthcoming deliverable.

# Contents

# 1 Introduction

## *1.1 Background*

HECTOS is a European project focusing on harmonization of evaluation, certification and testing of physical security products. Physical security equipment and systems are very diverse in technology, concept of operation, application area and performance, and similar security products are difficult to compare in terms of performance, accuracy, usage, trust and validation of functionality. Currently, there are very few test, evaluation and certification procedures in Europe that are mutually recognized by different Member States. This leads to fragmentation of the market, as identified in the recent EC Communication on Security Industrial Policy, with negative impacts on both suppliers and users.

The HECTOS project focuses on the evaluation and certification schemes for physical security products, and studies how existing schemes used in other areas could be applied, adapted or developed for products used for physical security of people, property and infrastructure. Developed evaluation and certification schemes will be validated by applying them to two different product groups as case studies; explosives detection systems (outside of aviation security) and biometric recognition.

The HECTOS project will learn from and work with other initiatives working in broader areas such as security systems and cyber security, as well as with other standardization and certification initiatives, including the EU research project CRISP.

HECTOS will result in elements for a roadmap for the development of harmonized European certification schemes for physical security products, and provide standardization bodies with proposals for new work items.

HECTOS focuses on the functional performance of physical security products, those used for the protection of (mainly) physical assets against physical attack, such as those by criminals or terrorists. Physical security products are used to provide solutions to many different security requirements in many different applications and market sectors. Often products from one or several categories are used in combination. The relationships are complex and it is not possible to produce a simple mapping between products, applications, market sectors and security requirements. Instead, this report describes a number of application scenarios which, whilst not exhaustive, are representative of security requirements and the way that security products are deployed to help fulfill these requirements.

D1.2 lists and describes application scenarios where physical security products may be used. They are intended to guide and support the research carried out during the HECTOS project. The scenarios do this in a number of ways. For example: as concrete examples to guide and illustrate the development of concepts; as examples for use during the case studies; and, as test cases to examine the breadth of applicability of the evaluation and certification schemes developed on the project.

This report adds analysis of the ethics and human rights dimensions of those applications to the scenarios.

## *1.2 Purpose and content of the Document*

This report examines the ethics and human rights risks of the technology use described in the application scenarios specified in D1.2. In doing so, it builds on the work of D6.1, which identified ethics and human rights issues arising in connection with the security product categories developed in D1.1. For the most part, the issues discussed in this paper should be understood as risks rather than implications or inevitable costs, because the extent to which they in fact arise depends on the particulars of the case at hand, and the application scenarios are more general than detailed.

Most of the issues discussed in this report were already identified in HECTOS D6.1. The most commonly arising remain: privacy, data protection, freedom of expression, association, and movement, health and safety concerns, and issues around consent. Where HECTOS D6.1 considered the ethics and human rights implications of some products that are not currently in use in the EU, this report only discusses products whose sale and use is already permitted under EU law. Some of the issues discussed here, namely those that arise in virtue of the specific characteristics of the context in which the technologies are used, are not covered in D6.1. Examples include concerns about the implications of certain technologies used at airports for the ability of border officers to fulfil their duties to vulnerable individuals such as potential victims of trafficking and those seeking asylum, and concerns about the potential of CCTV in schools to undermine some of their educational purposes.

Some of the issues highlighted in this report can be addressed at the stage of product design and manufacture. Others are better addressed by ensuring that products are used in practice by professionals who are bound by well-developed codes of conduct and/or in accordance with a standard operating procedures or protocols. All these ways of addressing ethics and human rights risks of security products are potential candidates for certification and so relevant to the aims of the HECTOS project. However, it is possible that some of the concerns raised in this report are so peculiar to the applications described in the scenarios that they are difficult to address through certification. This and other matters related to the potential of standardisation and certification to achieve ethics and human rights compatibility will be raised at a forthcoming experts meeting in the autumn of 2015, and reported on soon after in a deliverable (D6.3).

This report is structured as follows. Each of the application scenarios presented in HECTOS D1.2 is reproduced below, in a text-box. Commentary on the ethics and human rights implications of the application scenario follows each text-box. As far as possible, issues are distinguished and discussed under separate headings. This gives the reader a clear overview, at a glance, of the range of issues arising in connection with each application scenario.

# 2 Ethics and Human Rights Implications of Application Scenarios

***Scenario 1 – Biometric payment security***

**Summary:**

Biometric payment systems use biometric data (e.g. fingerprint or vein pattern) to confirm the identity of the user for a payment. These techniques are starting to be used, especially in the fast growing eCommerce area, as an alternative or supplement to traditional PIN code methods as a method of combatting fraud in personal financial transactions.The combination of biometrics (use of human characteristics) and financial transactions brings the individual into potential danger. (i.e. spoofing or direct attacks). Therefore the whole biometric payment process should be highly resistant to any kind of attacks.

**Description:**

Electronic payment systems are widely used both by individuals and businesses especially with the grown in internet use and eCommerce. Financial transactions are subject to fraud, through hacking, stolen payment cards and PIN numbers and other techniques. Biometrics represents an additional security measure that can be used.

Examples of current use of this scenario are low value payments and purchases using Apple Pay on iPhones and, in Japan, biometric fingerprint scanners are used to supplement PIN codes in some ATMs.

Today, knowledge-based authentication in the form of passwords and PINs are still the most widely used form of authentication. Cardholders must enter a secret PIN for confirming debit transactions. To prevent the illegal use of the card by unauthorized persons, in addition or as an alternative to the secret PIN, biometric characteristics of the cardholder can be used for cardholder verification provided that the biometric verification method achieves the required levels of attack resistance and usability. Biometric payment security systems should be resistant to any kind of attacks. For example in case of payment using fingerprints, the payment system should be able to differentiate between live fingers and lifeless dummies in order to resist presentation attacks (spoofing) using artefacts or chopped off fingers.

Standards and trusted evaluation and certification schemes are required in order for financial institutions to be able to assess the risks and implement appropriate systems.

Similar techniques can be used to verify a person’s identity for access to mobile phones and computers and for access to non-financial transactions – such as vehicle registration and licencing, and access to sensitive personal information.

## Scenario 1- Commentary on ethics and human rights issues

### *1.1 Social Exclusion*

If biometric payment technologies become the norm for basic goods and services, such as banking or payments, efforts must be made to reduce the numbers of those unable to register for their use and to establish easily available alternatives.

### *1.2 Data protection and mission creep*

A danger of mission creep leading to data protection regulation infringements or violations arises when biometric data collected for one purpose is used for another purpose. The purpose for which biometric data is collected should be clearly specified and clearly limited by the company collecting it.

### *Scenario 2 - Small business – office/shop – intruder detection alarms*

**Summary:**

Small businesses such as shops and offices face the risk of burglary and vandalism. They are often unoccupied in the evenings and at night. Physical barrier security measures such as secure doors and windows provide one layer of security. Another is provided by intruder alarms and possibly CCTV surveillance. These measures are usually designed and implemented by specialist companies, and operated on a day-to-day basis by relatively untrained staff in the business.

**Description:**

There are over a million shops and small offices in the EU. They often face the street and are not occupied in the evening or during the night. These businesses are at risk from break-ins, by intruder's intent on stealing stock, business equipment or cash and other valuables stored on the premises. Whilst the consequences of a break-in in absolute terms are lower than for scenarios involving serious crime or terrorism, they may still be very serious for a small business. In market terms, the scenario is important because the number of shops and offices is so large.

These businesses protect themselves using a number of physical security measures and products from different categories: physical barriers, access management, surveillance and intruder detection.

A typical scenario is a shop occupying its own building in the high street of a town. Typically, this will have doors and windows facing the public street, which will be well lit and have some passing pedestrians and traffic at all hours. The street may also be equipped with a video surveillance system operated by the municipal authorities. The shop also has doors and windows at the rear in an area which is generally hidden from public view. The shop has a range of stock, both on display and in a stock-room. It also has computers and other business equipment. Cash, up to 5,000€ is sometimes held on the premises overnight.

Typical physical security measures will include:

- Secure burglar resistant door sets and windows. The windows at the rear are protected by metal shutters. Doors are either equipped with mechanical, key operated locks or a small smart-card operated electronic access control system, linked to the intruder alarm.
- The building is further protected by an intruder alarm system which has a range of sensors. These include door and window opening sensors, break-glass sensors on windows, passive infra-red motion detectors. The alarm is connected to a bell and is also linked to an alarm monitoring centre provided by a private company, which will send security guards and/or alert the police in the case of a break-in.
- A CCTV system is also installed. This monitors and records the areas of the shop open to customers during the day, and can monitor the whole building at night. The system is linked to the alarm system, to ensure that cameras are activated in the event of a break-in.
- The final security measure is the installation of a safe which is rated to hold cash to the value of 5000€. This is used to store cash left on the premises overnight – either to provide a 'float' for the next day, or because it has not been possible to take the previous day's cash to the bank for some reason.

This application is not regulated by government. Insurance companies often set requirements on the security measures that need to be implemented in order for the business to obtain insurance cover.

These types of security system are typically designed and implemented by specialist companies. Advice can be obtained from these companies as well as from the police (Police Crime Prevention teams in the UK). There are certification schemes for companies that design and install electronic security systems (intruder alarms, video surveillance systems, access control systems) in some countries. For example in the UK, the National Security Inspectorate (NSI) operates such a scheme.

## Scenario 2- Commentary on Ethics and Human Rights Issues

### *2.1 Consent*

Just as with shopping centres (scenario 7) concerns about privacy with inward-facing CCTV systems are mitigated by the implicit consent of those people who continue into a shop where the use of CCTV is clearly advertised. Similarly, with the nighttime use of inward-facing CCTV systems for the purposes of intruder-detection; we can safely say that an intruder has implicitly consented to be filmed by means of the explicit action of breaking and entering. However, just as in scenario 7, even where persons have implicitly consented to be filmed by means of their express action of entering the shop or office where the use of CCTV is clearly advertised there are places within the shopping centre where the use of CCTV would be inappropriate; restrooms and changing rooms for example.[1]

### *2.2 Privacy*

Outward-facing CCTV cameras (cameras that face out of a shop or office and into public spaces) are more problematic. A camera that monitors an external door is not likely to raise any issues but cameras that continuously monitor a public street outside the building may raise issues. The owner or operator of a shop or office has a legitimate interest in securing their property (or the property for which they have responsibility) which may give them sufficient justification to make it permissible to install CCTV cameras inside that property. However, owners and operators lack an interest in or duty for securing the public street outside of that building sufficient to ground a right to collect camera data from the street. Whereas there may be a sufficient justification for the police to monitor a public street this justification is absent for a private owner of a shop or office. Such surveillance is not proportionate for the purposes of ensuring the security of the buildings, its goods and the people inside that building. Sufficient care may need to be taken to ensure that a camera that is attached to the shop or office does not illicitly monitor and collect data from areas that a proprietor has no right to observe. A camera that, for example, directly monitors someone's private dwelling is a definite violation of privacy even where this is a side-effect and the express purpose of the camera is to monitor an external door or something similar.[2] Given that these buildings are places of work, there are additional issues where CCTV is capable of being used by employers to covertly monitor the performance of employees.

### *2.3 Data protection*

Just as in scenario 7, storing images or footage for an excessive amount of time or distributing and exploiting the images or footage for other purposes is likely to violate the right to the protection of personal data and/or the right to privacy of the person filmed. Where CCTV

[1] Again, for useful guidance on the suitability of placing CCTV systems in sensitive areas see, See the Home Office Surveillance Camera Code of Practice, June 2013 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/204775/Surveillance_Camera_Code_of_Practice_WEB.pdf The authors of the code of practice suggest an exception in situations of emergency or of exceptionally high risk but emphasise that any such CCTV coverage must be well notified and not covert.

[2] See the U.K. Information Commissioner's Office publication, 'In The Picture: A Data Protection Code of Practice for Surveillance Cameras and Personal Information', https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf

cameras are connected to networked computers it is important to ensure that the data stored is secure. Also, insecure networked CCTV systems have dual use properties since illicit access to a networked CCTV system gives an attacker a considerable advantage in planning their attack.

### *2.4 Health and Safety*

Finally, technologies that are capable of trapping intruders inside a shop or office raise important health and safety risks; for example intruders may be trapped and unable to escape in the event of fire or they may be rendered inaccessible in the case of a medical emergency. There are also risks associated with criminals taking employees hostage and forcing them to open safes or other locked areas. If safes and door locks leading to areas which are tempting to thieves lock automatically between certain hours with the access codes only being accessible only via an alarm operating company or some other reliable agency the incentive for hostage-taking would be diminished.

### *Scenario 3 - Bank – safes/vault – storage of cash and valuables*

**Summary:**

Banks and other organisations dealing with high value goods use safes and strongrooms to store cash and other valuable items. These objects need to be protected against theft, usually by forced attack. Safes and strongrooms are used as an element in an overall layered set of physical security measures to provide appropriate security.

**Description:**

Banks and other organisations dealing with high value goods such as precious stones and metals, jewellery and artworks use safes and strongrooms to store cash and other valuable items. These may include safety deposit boxes, held for individual customers within a larger secure store. There are also specialist providers of these services. These items are subject to attempted theft, often by well organised criminal gangs using specialist equipment.

Material needs to be protected against both forced attack and against attempts to access the valuables by manipulating the locks and by threatening staff to force them to provide access.

Safes and strongrooms are used to provide secure storage of these items. They are not used alone, but as part of an overall set of physical security measures to deter, detect, impede and delay a potential attacker. These will include perimeter security, access management, surveillance and intruder detection alarms.

Safes and strongrooms provide both a physical barrier and access control through high-security locks. Special mechanisms are also used to provide time delays, require multiple keys/persons to open the safe, and other measures to mitigate against attempts to coerce staff.

A typical example of this scenario is a bank branch in a small city. The bank stores cash to meet the needs of personal and business customers, as well as providing a safety deposit box facility, again for personal and business customers.

There are well established EN standards for safes and strongrooms and for high security locks. Conformity test methods are included within the standards and in other standards produced by evaluation and certification bodies.

### Scenario 3 - Commentary on Ethics and Human Rights Issues

*Balancing wealth security benefits of individualised authorisation against risk of threats and violence to employees*

As noted in the description of this scenario, attempts to break into bank vaults and jewellery stores often involve threats to life as well as to material wealth. A brief review of recent bank and jewellery heists in the EU reveal that employees continue to be threatened by robbers regularly for goods on display, but that goods in safes and vaults tend to be targeted directly, that is, without going via the individuals with authorised access. Design of safes and vaults but also of the security systems into which these are incorporated must seek a balance between the aim of ensuring that only those authorised can gain access to safes and vaults and the aim of protecting those authorised from becoming obvious targets for criminals. For example, using biometric access control systems for safes and vaults is likely to involve too great a risk of harm to those with authorised access. By linking access so directly to specified individuals it converts risks to the security of material wealth into risks to the life and physical wellbeing of the employee.

### *Scenario 4 - Security screening – large public event (permanent venue)*

**Summary:**

Events at large sporting and entertainments venues are high profile targets at risk from terrorist attack by explosives and weapons. There are also risks of lower-level crime such as fights leading to knife or gun attacks on individuals. Patrons are screened to mitigate this risk. A major challenge is that many thousands of people have to be channeled into and out of the venue within a short period of time. This requires careful planning and efficient controls.

**Description:**

Large sports and entertainment events – football games and pop concerts for example – are typically held in purpose-built venues such as stadia and concert halls. A typical example of the scenario is a football stadium holding 10,000-50,000 spectators.

The risks include terrorist attacks by a single or group of attackers using weapons or explosives. The effect of such an attack can be magnified by the panic it creates amongst the crowds. These events are also at risk from disorder, for example resulting from rivalry between supporters, which can lead to fights including, potentially, gun and knife crime. Operators of these events often wish to prevent other (non-security related) items being brought into the venue for commercial, safety and other reasons. Prohibited items might include fireworks, banners, horns, recording equipment, food and drink.

Protecting arenas, stadiums, large public venues and special events needs to be specific to the venue, location, and event, time of day, crowd demeanor and even international and terrorist situations. The right balance has to be found between security, efficiency and freedom of movement. The number of people that need to be screened in a short period of time is a critical factor in designing any screening operation.

Typical screening solutions involve a combination of explosives and weapons detection products and manual search. The design of a screening operation can be greatly simplified if the items carried by patrons can be managed. For example, pre-event communication can be used to limit the (benign) items and the number and size of bags that patrons carry with them.

Explosives and weapons detection products that can be used include walk-though and hand-held metal detectors and x-ray systems for bag screening. Other techniques such as explosives trace detection could be used, but the operator skills needed and time taken for their routine use is an issue. Manual search and other detection techniques such as detection dogs may also be effective. Careful design is needed to make sure that screening does not cause undue delays and that it does not in itself create secondary targets.

Other security measures that need to be considered include: mitigation of vehicle-borne threats; access management and perimeter security to prevent attackers avoiding security screening; appropriate measures to prevent insider-threats by staff; and, area and building search to ensure that explosives or other devices are not hidden in advance of an event.

Security screening is this scenario is generally not regulated, although local police may offer guidance and many organisations have their own policies. For example, the international football organisation FIFA has the following rules:

”FIFA events are exposed to greater threats than may normally be present in the host nation and this includes acts of terrorism. The stadium safety and security management team must implement basic countermeasures as part of their daily “housekeeping”. As a minimum, stadiums (including areas within the outer perimeter) must be searched by trained personnel prior to it being handed over for event use. Once a stadium has been searched, it must be suitably guarded by security to prevent unauthorised access. Furthermore, all vehicles and personnel entering a secured stadium must be searched” ”Security checks shall be carried out on persons and vehicles at the entry points of the outer and inner perimeters, as well as at entry points to areas that are not open to the general public” [FIFA Safety Regulations - http://www.fifa.com/mm/document/tournament/competition/51/53/98/fifa_safety_regulations_en.pdf ]

## Scenario 4- Commentary on Ethics and Human Rights Issues

Much like the airport search, searches at large public events in permanent venues can feel intrusive to the individuals who are being searched.

### *4.1 Consent*

Much like the airport search, just so long as the patron is well informed in advance that they will (or could) be searched as a condition of entry, the patron can be deemed to have consented to the search by agreeing to enter the venue. Similarly, the confiscation of property deemed to be harmful can be said to have been consented to just so long as the patron was supplied with a clear list of prohibited items in advance (on their ticket or confirmation email for example). Just so long as the patron was adequately informed of the list they have no reasonable complaint. That said, the consent given by a patron extends only to procedures that are reasonable for the purposes of detecting security-relevant wrongdoing.

### *4.2 Proportionality*

In addition to a plausible case for informed consent to security searches of bags and persons for weapons are proportionate. The threat posed by knives, guns, explosives, poisons or other substances that can cause harm to others at the venue is sufficient to outweigh the intrusiveness of the search procedures. The proportionality of security checking contributes to the case for presumed consent to these searches insofar as we can say that most reasonable and rational people would submit to their bags being searched for knives/guns/explosives if this is necessary to prevent them being the victim of an attack.

### *4.3 Privacy*

The filming with CCTV cameras of patrons in order to prevent disorder and harm is proportionate and therefore not an unfair intrusion into privacy just so long as attendees are well informed (e.g. by notices outside of the temporary venue and/or a notification on their ticket or confirmation email) then they can be said to have consented to a proportionate level of surveillance.

### *4.4 Misuse (voyeurism) and discriminatory profiling*

There is a risk that issues of privacy may arise if the event involves people dancing, flirting, kissing and so on, as may well be the case at a concert, and CCTV operators have the opportunity to voyeuristically watch these activities in real time. This risk may be greater if CCTV can be directed so as to follow specific people around a venue (a feature that delivers enhanced security potential too).

Racial or other forms of profiling, for the purposes of enhanced search or surveillance (e.g. being followed by CCTV cameras) raise issues of unfair discrimination. Additionally, such profiling – where profiled persons are denied entry or subject to enhanced observation when inside – raises issues of social exclusion. Risks of unfair profiling and of misuse of camera feeds for voyeuristic purposes can be addressed via guidelines and training for operators.

### *4.5 Health and safety*

Directing the flow of people and vehicles in order to minimise security threats is not in itself problematic when it comes to people who have agreed to submit to direction as a condition of attending an event. It is more of a problem for those who are not attending where they are affected directly or indirectly by those security measures. These people have not consented to be directed by, for instance, private security guards. Those effects might be fairly minor (e.g. traffic delays) or major (e.g. delayed medical treatment).

Health and safety issues are raised by the funneling of large number of people into security checking areas. Older people should not be forced to stand for excessive amounts of time and young children may need access to food and water. Public events present a greater problem in this regard than airports, there are likely to be many more people and the physical environment prior to the checking area is likely to be less controlled. For these reasons it is important that the security measures are speedy, efficient and proportionate.

### *Scenario 5 - Security screening – large event (temporary venue)*

**Summary:**

Some events where there is a risk of attack are held at temporary venues, or at venues where the risk is usually much lower. An example is the visit of important statesmen to a public building, conference etc. Explosives and weapons attacks are the most serious threat, although there is also a risk of politically motivated disturbances to the event. Temporary security measures need to be set up and operated during the preparation for and during the event itself. These include perimeter security, access management and screening of attendees for explosives and weapons.

**Description:**

A typical example of this scenario is the official visit of an important statesman. Official visits are popular targets for terrorists and mentally disturbed persons due to their high visibility, economic, political and psychological impact. Conceivable are direct attack to persons with weapons or explosives carried by offenders or an attack to vehicles or persons by planting bombs. The procedures for official visits may be defined in national regulations, e.g. [4.2].

The extent and types of security measures deployed vary greatly dependent on the risk and include:

- Cordoning off of restricted areas with temporary fences and barriers
- Surveillance of area by CCTV and security personal
- Search of area prior to event
- Access to restricted areas only with entry authorization
- Person screening for weapons and explosives by manual search or metal detectors (WTMD or HHMD)
- Screening of belongings by manual search, metal detectors and x-ray imaging, supplemented by explosives trace detection

Temporary events of this kind may be of different size. Small events may only have a hundred people or so, but large ones could have tens of thousands.

Equipment is operated by trained personnel but the operation of the systems and processes is not heavily regulated. Guidance is available from police and counter-terrorism organizations. Local policies and procedures often exist. There are usually special government police, military or security organizations who implement and operate security measures at the most sensitive events.

### Scenario 5- Commentary on Ethics and Human Rights Issues

All of the comments applicable to scenario 4 are also applicable to scenario 5. There are some additional features of temporary venues that are worth noting:

*5.1 Data protection and mobile equipment*

Mobile equipment is inherently less secure than equipment that has been permanently installed. Unlike permanently installed equipment, mobile equipment can be stolen or mislaid, also it is harder to ensure that mobile equipment is only accessed by authorised persons and there are additional opportunities for misuse, for example, during transit. Where mobile equipment capable of collecting sensitive personal information is in operation it is important that the data collected by this equipment is secure.

*5.2 Freedom of speech and association*

Being filmed by CCTV cameras for the purposes of security-relevant surveillance, can be said to have been consented to just so long as attendees are well informed (e.g. by notices outside of the temporary venue and/or a notification on their ticket or confirmation email). On the other hand, there are events, e.g. political rallies, where the use of CCTV may interfere with freedom of expression and association and here it important that the use of CCTV not exceed the stated purpose of securing the immediate safety of the event. The long-term storage of CCTV images for the tracking of individuals and the recording of their associations or political allegiances is deeply problematic. The tracking of a person's political interests, associations or allegiances might be problematic for a number of reasons: for one thing, if an individual person can be associated with a political party for whom they wish to vote in an election without their having consented to be so identified this could violate their right to participate in a secret ballot. Also, individuals are under no legal or moral obligation to reveal their membership of political parties and the acquisition of data concerning an individual's political beliefs is regulated by data protection regulations throughout the EU.

There is also an ethical concern about collecting and storing information about identifying the individuals who attend political events and storing that information. Citizens in democratic societies ought to be free to develop and deliberate with a view to forming their views and attitudes. This requires the freedom for individuals to consider views which others may find offensive and which those people might not wish to be publically identified with. For example, someone might attend a political event and be identified by means of CCTV or other surveillance. After deliberation, they might subsequently reject the ideas expressed at that event, yet they have been identified and associated with those views. The ability to consider ideas without attracting public opprobrium or official scrutiny is an important democratic value.

Where politicians, for example, are present at these events – or the event is implicated in some kind of public controversy – there is the strong likelihood of some kind of public protest. It is important that security measures properly balance the public interest in exercising the rights of lawful protest with the need to ensure the safety and security of the event.[3]

[3] Article 11 of the European Convention on Human Rights recognises a right to peaceful assembly and a right to freedom of expression. Article 9 recognises a right to free thought, conscience and religion.

### *5.7 Collateral effects and health and safety*

As in scenario 4 there is problem of security measures adversely impacting persons who are not attending the event. However, with temporary venues the problem is somewhat greater. Unlike the people who have expressly chosen to attend the event, those people who are not attending the event cannot be said to have consented to the intrusive measures associated with the event's security. It is important that those responsible for the security of a temporary event are mindful of the potential for the disruption to the lives and wellbeing of those people who, in the everyday movements of their lives, pass through the area in which the temporary event is being held. Low levels of inconvenience, minor traffic delays for example, are not ethically problematic. However, to take another example, where access to a hospital for disabled persons or for those seeking medical treatment is severely disrupted, this is more problematic.

### *5.8 Authority and the accountability of private sector security agents*

The use of private security guards to police protest can be problematic because: (i) private security guards may lack adequate knowledge and training in dealing with lawful protest; (ii) private security guards are not authorised agents of the state. Private security guards are generally less knowledgeable about the parameters of legally acceptable force and are therefore more often subjects of criminal prosecution and civil litigation. At the same time, the nature of private security organisations makes them less open to democratic oversight and less accountable when things go wrong. Finally, the commands of private security guards may lack the authoritative status of police officers and members of the public may react to those commands with less respect or more aggression, relatively speaking. Similar concerns have been raised about the U.K. operations of the private security company G4S who are responsible for running private prisons and for the deportation of people who have been refused U.K. residency. [4]

[4] http://www.theguardian.com/commentisfree/2014/dec/22/g4s-convictions-deaths-employees-racial-overtones

### *Scenario 6 - Security screening & surveillance – open crowded place*

**Summary:**

Open crowded places pose a target for terrorist actions involving explosives or firearms, but can also include CBRN materials. Measures that help to deter, detect and delay a terrorist attack include: traffic management and hostile vehicle mitigation measures; CCTV oversight; and, for buildings, blast resistance and building management.

**Description:**

Open crowded places – i.e. places with no natural control over people passing – will be found in a wide range of locations, including commercial centres, transport hubs such as railway stations in large cities, and high street visitor attractions. Crowded places can also include the public realm – open spaces such as parks and squares. Crowd densities may vary during the day/night and may be temporary, as in the case of sporting events or open air festivals (shopping centres and large events being treated in separate scenarios).

Crowded places are an attractive target for terrorist actions since they are easily accessible, regularly available and offer an impact beyond the loss of life alone, but also psychological and economic/political impact. The threat may be to people in the crowded place or to surrounding buildings and property. Attacks on these kinds of targets are likely to involve the use of firearms or improvised explosive devices (IEDs), of which the three main types are person-borne (PBIED), vehicle-borne (VBIED) or leave behind (LBIED).

Security measures to mitigate against a terrorist attack, include the adoption of security-oriented urban design principles [4.3] as well as counter-terrorism protective security measures.

Typical urban design measures that help to deter, detect and delay a terrorist attack include:

- Hostile vehicle mitigation measures such as controlling vehicle access and speed, vehicle security barriers
- Better oversight through clear lines of sight around buildings, uncluttered street furniture’ video surveillance (CCTV) monitoring and potentially security guarding

Protective measures can be applied to sensitive buildings other assets in the area, such as barriers, access management and video surveillance.

In the case of increased threat level to the crowded place, security screening measures can be implemented. This might include increase levels of surveillance, possibly including video analytics and biometric techniques to identify suspicious persons or activities. Security screening for explosives and weapons can also be considered. This might include random inspections or checks on suspicious persons. Screening and biometric checks may be done by exploiting existing or specially created chokepoints to provide some level of control on person movement and visibility. For screening of freely moving persons, some non-cooperative stand-off screening technologies are available for weapons and explosives, but they are not really yet at a maturity level where they can be used on freely moving crowds.

## Scenario 6- Commentary on Ethics and Human Rights Issues

Several different types of place are mentioned in the scenario, each of which raises different sorts of issues. We propose to focus on train stations and public parks since this aids clarity, avoids unnecessary repetition and covers all of the significant ethical issues.

The scenario also envisages two kinds of threat level: everyday threat and heightened threat level. We deal with these two levels of threat in talking about train stations and public parks. What grounds the difference between train stations and public parks? Public parks and train stations are treated by people both as destinations and places to pass through, they are both essentially public spaces. In these respects they are very similar. However, public parks and train stations differ in their function as public spaces. In what follows we discuss these differences and their implications for the proportionality of different kinds of CCTV monitoring.

### *6.1 Public parks*

A public park has the purpose of being a space for recreation, free expression, play, family time, and limited romantic displays of affection. Part of what makes public parks so desirable is the opportunity that they allow people to relax and engage in types of behaviour that would be inappropriate in other kinds of public space. CCTV may represent a significant intrusion on the activities for which public parks were designed. For this reason the security and crime-prevention considerations that speak in favour of CCTV surveillance in parks has to be balanced against the extent to which these measures cut against the value of the park as a public space.

#### 6.1.1 Privacy and public parks

Extensive use of CCTV might have the potential to adversely affect perfectly lawful behaviour. For example, quiet and remote areas of some public parks are often used by adults to meet other consenting adults for the purposes of arranging casual sexual encounters. Assuming that the actual sex happens somewhere appropriate there is nothing unlawful about these assignations. Yet the people involved may wish to remain anonymous and for there to be no record of their comings and goings; they may well find CCTV surveillance highly intrusive. At any rate, the use of CCTV ought to be carefully targeted and proportionate – as the authors of the Campbell Systematic Review ‘Effects of Closed Circuit Television Camera Surveillance on Crime’ put it when comparing the significant effect of CCTV on vehicle crime in car parks but its negligible effect on the prevention of violent crime in public spaces:

> “CCTV has a modest but significant desirable effect on crime… We conclude that CCTV surveillance should continue to be used to prevent crime in public space, but that it be more narrowly targeted than its present use would indicate. Future CCTV schemes should employ high-quality evaluation designs with long follow-up periods.”[5]

#### 6.1.2 Proportionality and public parks

Reasonable expectations of privacy are not only about opportunities to consent, they are also about recognition of reasonable grounds for intrusion, which means necessity and proportionality to a legitimate purpose. So, even if notices are present in a park informing

[5] Welsh BP, Farrington DC. ‘Effects of Closed Circuit Television Surveillance on Crime.’ Campbell Systematic Reviews 2008, p.3. www.campbellcollaboration.org/lib/download/243/

people that CCTV cameras are in operation (giving them opportunity for consent) the presence of an extensive CCTV camera system, especially if that CCTV system involves real-time monitoring, may still be excessively intrusive. In situations of heightened threat, it may be permissible to increase the level of surveillance in a public park. But it is important that the level of CCTV coverage is proportionate to a reasonable assessment of the level of threat and that the level of coverage is reduced to pre-threat levels once the threat has passed.

### *6.2 Train stations*

Unlike parks, train stations are not spaces designated and used for intimate or quasi-intimate activities. This is reflected in the extent and depth of the privacy concerns identified below.

#### 6.2.1 Privacy and consent in train stations

If a person proceeds to enter a railway station and CCTV notifications are present and clear, then that person can be said to have consented to being filmed if they continue, informed, into the station (with the usual proviso that the level of filming is proportionate).

#### 6.2.2 Privacy and proportionality in train stations

In terms of privacy intrusions related to CCTV, a greater concentration of cameras with fewer blind spots for instance, is more appropriate in a train station than in a public park. Train stations are public spaces but they are not designed with relaxation, play, and socialising in mind. To this extent, an extensive CCTV system may be rather less intrusive in a train station than it would be in a public park. Moreover, CCTV systems are useful for the everyday secure operation of the train station, for instance, to make sure that there is not overcrowding on train platforms leading to people risking getting pushed onto tracks or enabling the police to quickly intervene if a fight on the platform occurs. The presence of cameras has a clear rationale and the nature of a station as a particular kind of public space makes the presence of those cameras less intrusive. The non-intrusive nature of the filming suffices for its permissibility and the various risks associated with its everyday operation suffices to justify the kind of real-time monitoring of CCTV that would be inappropriate, in ordinary circumstances, in a public park.

### *6.3 Data protection and dual use*

It is important to ensure that the data collected by the CCTV system in both parks and train stations is only accessed by authorised persons. Where equipment is capable of collecting sensitive personal information it is important that the data collected by this equipment is secure. Additionally, the security of CCTV systems, where these systems are networked, is of paramount importance given their dual use possibilities. Gaining illicit access to the CCTV system of a railway station considerably enhances an attacker's ability to do harm.

### *6.4 Function creep*

CCTV systems are generally not capable, on their own, of tracking the movements of individuals – although CCTV footage can be used by the police to establish the movements of individuals after an event. However, real-time tracking of individuals is possible CCTV systems are used in conjunction with other location and tracking technologies (e.g. mobile phone geo-location data):

> "It is possible for data collected by a range of surveillance systems to be integrated into broader 'big data' processing systems operated by organisations. This has implications in terms of profiling, what can be learnt about individuals and how decisions are made about them."[6]

Real-time tracking of individuals is more intrusive and may constitute surveillance that runs considerably further than anything to which individuals have consented. Technologies that are capable of identifying individuals are capable (if that data is stored and searchable) of tracking the movements of those persons. Emergency situations of the sort contemplated in the scenario provide a justification for this tracking but, outside of an emergency, such tracking would be morally problematic. Hard and fast information about the actual incorporation of CCTV footage into data fusion technologies for tracking purposes is hard to come by. However it is clear that there is potential for the technology to be used in this way. In light of the data fusion possibilities opened up by data of this sort, and the serious privacy issues raised by data fusion, the networked systems that store CCTV information need to be secure.

### *6.5 Discrimination and social exclusion*

Similar to previous scenarios, racial or other forms of profiling, for the purposes of enhanced search or surveillance raises issues of unfair discrimination. Additionally, such profiling, where profiled persons are denied the possibility of travel raises issues of social exclusion.[7] Denial of access to public spaces or to travel for lawful purposes based on membership of a group serves to indicate a symbolically lesser or unequal status for members of that group. Where this occurs in a public space this symbolic indication of lesser status is additionally humiliating.[8]

[6] 'In the picture: A data protection code of practice for surveillance cameras and personal information', Office of the Information Commissioner, p.25, https://ico.org.uk/media/for-organisations/documents/1542/cctv-code-of-practice.pdf

[7] See, Kevin Macnish 'Unblinking Eyes: The Ethics of Automating Surveillance' *Ethics and Information Technology*, 2012, Volume 14, Issue 2, pp 151-167.

[8] Smart CCTV technologies which automatically blur faces so that the race of filmed persons is not visible are being developed for use by police in public places. The faces can be subsequently un-blurred by a senior authorised officer once an incident has occurred. See, C. Pantoja, V. Arguedas and E. Izquierdo, 'Anonymization and De-identification of Personal Surveillance Visual Information: A Review' http://www.advise-project.eu/sites/default/files/content/LACNEM-CP-VF-EI-v6.pdf . It may be the case that this sort of technology is more appropriate for use in a public park than it is for use in a train station where it may impede the ability of transport police to respond quickly to real-time threats.

### *Scenario 7 - Shopping centre –video surveillance (CCTV)*

**Summary:**

Video-**s**urveillance is the monitoring of enclosed or open rooms from a distance by means of video cameras. It is widely used for security and safety surveillance of public and commercial buildings and open spaces

**Description:**

Video-surveillance systems may be installed in shopping centres for purposes of crime prevention and detection and for facility management. Because surveillance is an intrusion into the privacy of the persons monitored, video-surveillance should be limited to circumstances where public safety and security are at risk. Other areas where similar video surveillance techniques are used include transport such as rail stations and airports, sports venues, etc.

A typical example of this scenario is the deployment of a CCTV camera network with approximately 100 cameras in a large department store or shopping centre.

Most video surveillance is either for post-event analysis by human operators or has human operators to spot situations of interest and then to use pan-tilt-zoom etc. to focus on them.

Unlike the individuals trying to be accepted by access control systems (scenarios 7 and 9) or automatic border control systems (scenario 10), the individuals in the field of view of video-surveillance systems are in general not cooperative.

Furthermore, the environment of video-surveillance systems is in general not designed for the collection of uniformly illuminated and optimally posed face images. The environment may be far from optimal for capturing face images. The inferior face recognition performance in less-controlled environments necessitates the involvement of trained personnel in video surveillance.

Video-surveillance systems may make also use of object detection and scene recognition techniques. Such technologies can be used for incident verification and detection of suspicious actions like leaving unattended bags, fighting and crowding of people.

## Scenario 7 - Commentary on Ethics and Human Rights Issues

### *7.1 Consent and proportionality*

CCTV surveillance of customers in a shopping centre raises the prospect of privacy intrusion. However, since shopping centres are commercial spaces, this worry is mitigated by the fact that, just so long as persons have the genuine option of avoiding the shopping centre, and the surveillance is well signposted, customers can be said to have consented to the CCTV surveillance. It is, however, implausible to think that this consent to be filmed extends beyond the time period necessary to maintain the security of the shopping centre or for surveillance that is disproportionate to the purpose of detecting or investigating genuine wrongdoing. Storing images or footage for an excessive amount of time or distributing and exploiting the images or footage for other purposes is likely to violate the privacy rights of the filmed customers.[9]

### *7.2 Appropriate siting and use*

Even where customers have implicitly consented to be filmed by means of their express action of entering the shopping centre where the use of CCTV is clearly advertised there are places within the shopping centre where the use of CCTV would be inappropriate; restrooms and changing rooms for example. In these areas there is a heightened risk of inappropriate voyeurism on the part of the private agencies responsible for operating the CCTV systems and the personal data collected is much more vulnerable to misuse. Also, given that a shopping centre is a workplace there are additional issues where CCTV is capable of being used by employers to covertly monitor the performance of employees.[10]

### *7.3 Dual use*

Additionally, the security of CCTV systems, where these systems are networked, is of paramount importance given their dual use possibilities. Gaining illicit access to the CCTV system of a shopping centre considerably enhances an attacker's ability to do harm.

### *7.4 Profiling and discrimination*

Similar to other scenarios, racial or other forms of profiling, for the purposes enhanced search or surveillance raises issues of unfair discrimination. Additionally, where profiling effectively denies an identified group the possibility of using a shopping centre, it raises issues of social exclusion. An incident involving the use of CCTV to exclude youths wearing 'hoodies' in the Bluewater Shopping Centre in the U.K. in 2005 raised just this sort of issue.[11]In the Bluewater incident, coordinated CCTV and private security was used to exclude youths wearing hooded sweatshirts from the Bluewater shopping centre. The management of the shopping centre decided on this policy as they felt they had sufficient anecdotal evidence that youths wearing

[9] For specific U.K. guidance on the use of CCTV systems see, See the Home Office Surveillance Camera Code of Practice, June 2013 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/204775/Surveillance_Camera_Code_of_Practice_WEB.pdf

[10] In the U.K. where an employer wishes to use CCTV to monitor their staff at work they have to apply, giving their reasons for wishing to record their staff, to the Office of the Information Commissioner. Employees also have a right to see any footage that has been taken of them. See: https://www.gov.uk/data-protection-register-notify-ico-personal-data

[11] See: http://news.bbc.co.uk/1/hi/england/kent/4534903.stm

this item of clothing responsible were responsible for anti-social behaviour and committing a disproportionate number of thefts at Bluewater. The hoods also make the wearers of this particular piece of clothing harder to identify using CCTV cameras. This kind of profiling, where the risk of a person’s behaviour is pre-judged and distinctive treatment meted out based on their membership of a group with statistical properties, is inherently discriminatory. There is an obvious trade-off insofar as these items of clothing may make it harder to identify people thereby lessening the effectiveness of CCTV surveillance. On the other hand, there are items of clothing of religious significance that also make it harder to identify persons that it would be wholly discriminatory to exclude from commercial spaces and, under ordinary circumstances, highly inappropriate to require persons to remove. Some head or face coverings are an obvious problem in a shopping centre – e.g. a motorcycle helmets or various kinds of masks that are often used to disguise a person’s identity during a robbery and, to be sure, perfectly licit head or face coverings can be converted for illicit purposes. Distinguishing licit from illicit uses of head or face coverings is a matter of fine judgement and careful training. Generally speaking, members of the police forces are more likely to have good training in this regard than private security personnel.

### *Scenario 8 - First responder application – suspected CBRNE incident*

**Summary:**

When a there has been a suspected CBRNE incident, first responders are the personnel securing the crime scene at an early stage. After forces such as bomb squads has cleared the area from people and dangerous items, forensic personnel investigates the scene to find traces or visible amounts of residues from the incident which could be used as evidence in the following forensic investigation or in further security measures around the scene directly after the attack.

**Description:**

After a suspected CBRNE incident, one important measure is to collect information in order to understand the sequence of events that have occurred and the possible threat substances used in the attack. The scenario can vary significantly depending on weather C, B, RN and/or E threat substances have been used in the attack. The choice security products will also be dependent on the situation.

First, the area is secured by the first responders (police, firemen, medical personnel) who set up suitable barriers or cordons, care and evaluate people, and extinguish eventual fires. The crime scene is typically divided into risk zones; cold, warm and hot zones. In hot zones forces e.g. bomb squad may use remotely controlled equipment for investigating the scene. These could be small mobile x-ray detectors, which screen suspected threat objects such as bags and operated at a safe distance. Neutralization of additional threats might be necessary before entering into the hot zones.

Forensic investigators are then investigating the crime scene, primarily to get an overview of the scene in order to undertake the correct measures. This is often time critical and portable and/or hand-held instruments for easy operation is used. Besides this, forensic sampling is performed which is less time critical and does not require immediate results. The investigators are primarily looking for traces or visible amounts which could originate from e.g. post-blast traces, undetonated explosives etc. The environment can vary significantly, from controlled indoor environments to outdoor urban environments where also weather conditions have to be taken into account. Hence, the investigated items, prints and surfaces can in principle be of all different types.

A combination of detectors can be used and techniques based on surface sampling are often utilized in first responder application scenarios. Examples are colorimetric test kits or immunoassay technologies, which provide relatively fast results. Investigators can also use dosimeters for their personal safety and to undertake immediate actions (such as cordoning or evacuation) in case of elevated R levels. In addition, samples can be brought to a laboratory for a more detailed analysis using conventional methods (e.g. with GC/MS, CL) which then takes longer time but provides a result with high material specificity. In order to achieve a forensic quality of results that can be used in a court of law the requirements for on-site portable equipment is very large. In the case that the use is for early warning that provides input to the tactical and practical investigation less demands can be put on the techniques. Such example is in-situ surface detectors, which are typically laser based and short-range hand-held instruments. However, these are most reliable on bulk amounts.

The operators are skilled but the process varies from country to country and relies also on best practices. There are no international operational and/or educational practices for the staff. As an example, the result can depend on how the sampling of surfaces is performed and factors such as surface material, particle size and operator experience are important. These factors also have influence on the choice of detection equipment.

Some of the trace explosives detection equipment that may be used in first responder applications have been tested and approved by ECAC for aviation security. This does not mean that they have the same performance at a possible CBRNE incident scene.

The number of incidents/suspected incidents in Europe is likely in the order of a few thousand, and many of them are certainly referred to insufficient safety rather than security related.

## Scenario 8 - Commentary on Ethics and Human Rights Issues

### *8.1 Consent and proportionality*

All the same issues around accurate, reliable, and comprehensible outputs of detection technologies raised in connection with scenario 18 below arise again here. However, additional issues around consent and proportionality arise if readings are taken from individuals covertly; if people are forced to stay in a specific area until readings have been taken from them; and/or if readings are taken forcibly from people's skin or clothes via swabs.

Only some technologies lend themselves to covert use. For example, optical (infrared/raman) devices could theoretically be targeted at people without their knowledge. Covert, targeted use of detection technologies is only proportionate if evidence exists of potential serious criminal activity, which the scan aims to detect. Otherwise, individuals should be informed that they are subject to scans.

It may be reasonable, especially in a post-incident crisis scenario, to compel people to stay in specific areas until they have been scanned. Those responsible for scanning should be well-trained to deal with such eventualities. Efforts should be made to persuade individuals to comply voluntarily with scans and to ensure their health and safety while they are confines. While it may be reasonable to prevent potentially contaminated people leaving certain areas, it may not be reasonable to prevent people entering such areas, as long as they understand are prepared to take the risks. This may be especially the case with parents who wish to gain access to their quarantined children.[12] Staff should explore the possibilities for dealing with such ethical dilemmas as part of their training.

Finally, compelling people to submit to readings of their skin and/or clothes can be justified in crisis scenarios where public health is at risk, but should be approached with great caution. Efforts should be made to gain voluntary consent and even when consent is denied, efforts should be made to inform individuals about what is happening to them, why, and what the health and other consequences might be. Use of force should be strictly limited and exerted only by authorised professionals e.g. police or the military.

### *8.2 Erroneous interpretation leading to unjustified restrictions of liberty*

It is possible that some people who are not contaminated or bearing illegal and dangerous substances test positive to CBRN and similar scans. For example, some heart drugs are based on explosive substances. Patients who are prescribed them may therefore find themselves triggering an alarm where there is in fact no cause for suspicion or concern. Staff operating detection devices should be aware of these possibilities and explore them before taking rights-restricting measures.

### *8.3 Data protection*

Products considered in this scenario raise issues of data protection if they store or transmit identifiable readings from individuals. In such cases the processing of data should meet data protection standards. In the case of emergencies data protection restrictions may be loosened

[12] See discussion in Rebera and Rafelowski 'On the spot ethical decision-making in CBRN (chemical, biological, radiological or nuclear event) response: approaches to on the spot ethical decision-making for first responders to large-scale chemical incidents.' *Science and Engineering Ethics*, 2014 20(3).

as fluid and flexible sharing of information may be vital to protecting public health and even human life.

### *8.4 Balancing security/public health and protection of staff*

It is important that staff are protected while they do their job of protecting others. Therefore it is also important that devices should be able to be operated and read by staff wearing protective gear.

### *Scenario 9 - Urban area – air monitoring for CB attack*

**Summary:**

At increased threat level, there can be a need for air monitoring for a chemical or biological attacks. Installations are typically performed in urban environments in which an attack has significant impact. The cost and impact of responding to an alarm (e.g. evacuation of an area and the danger of panic in the population, means that false alarm rates need to be minimized and response procedures to alarms need to be considered very carefully.

**Description:**

Crowded places in cities are potential targets for terrorist attacks with chemical and biological threat substances due to their high visibility and significant impact to the society. Both stationary and portable equipment are available but for long-term use stationary installations without operators are preferable.

There are detectors for monitoring increased threat levels in the vapor phase (typically for C) as well as particle monitors (typically for B). Installations should be located at strategic positions taking external conditions into account, and should preferably not interfere with people. Available instruments are often developed for military use but are also applicable in civil environments. Air monitoring detectors sample the surrounding air continuously and work in real time. When threshold values are exceeded, the detector alarms which is followed by further measures such as evacuation and/or alarm resolution steps.

The threat object could for example be carried by a person, left behind (in bag, vehicle etc), executed through ventilation system etc. It is important that the background levels are well known for each specific environment and that the settings/thresholds are carefully adjusted in order to minimize false alarms. Stand-off monitors are under development but are not mature for this scenario at the moment.

Examples of urban environments in which air monitors can be used are in open crowded areas, transportation (metro stations etc) or in critical infrastructures. However, the number of installations in Europe is until now relatively few because the threat level has been considered as low.

The scenario is not regulated but there is an ASTM standard covering specification for stationary point chemical detectors for homeland security applications. There is a corresponding standard for hand-held point detectors

### Scenario 9- Commentary on Ethics and Human Rights Issues

*Error and proportionality*

Few ethics and human rights issues arise in connection with air monitoring devices because they are not targeted at specific individuals or groups and do not in and of themselves interfere with liberty of people. The issues that do arise relate to the possibility of false positives and the need to ensure proportionate and effective responses to alerts.

### *Scenario 10 - School/Hospital – low security, open building – protection from attack*

**Summary:**

Schools are hospitals are semi-open buildings with large numbers of people entering and leaving each day. They are subject to a low, but not negligible risk of attack by an individual or terrorist group. Weapons attacks are the most likely. They are also subject to other lower level crime, including theft and anti-social behaviour. High levels of (intrusive) security are usually deemed inappropriate. Perimeter security, access management, intruder detection, surveillance and threat detection may all be deployed.

**Description:**

Schools and hospitals are semi-open buildings where users generally expect not to be subject to intrusive security measures. There is a risk of terrorist attack, since they are regarded as soft targets with high impact in terms of publicity and threat to society. Attacks by lone individuals and terrorist groups have occurred in a number of countries. These have usually involved weapons, sometimes with a group of attackers. Explosives and other threats are also possible. Other semi-open building such as large hotels, museums, shopping centres share a number of similar characteristics.

Schools and hospitals are also subject to the risk of lower level crime, such as theft and anti-social behaviour. Hospitals also use materials which could be used for a CBRN attack, so protection of these is also important.

General physical security measures can be used to secure the site and buildings, both during and outside, normal working hours. These include perimeter security, access management, intruder detection and video surveillance systems. These can be used to control access to different parts of the facility.

If the threat level is high enough, then it is possible to deploy detection measures to screen users of the site for explosives and, particularly, weapons threats. The use of WTMD and bag searches is routine in schools in some parts of the USA to combat gun and knife crime. It is not common in Europe. Screening could be deployed on an occasional basis or on (randomly or otherwise) selected individuals as a security measure with a deterrent effect. This type of approach could also be used to keep the overall level of intrusion, cost and delays within acceptable bounds.

### Scenario 10 - Commentary on Ethics and Human Rights Issues

Schools and hospitals differ from museums and shopping centres in a number of ethically-significant ways. The relevant distinctions and their implications for the ethics and human rights implications of security technology use are considered below.

#### *10.1 Vulnerability in schools and hospitals*

A large proportion of those populating schools and hospitals are vulnerable. Children are vulnerable because they are highly sensitive to stress, fear, and other negative impacts of security threats and, more importantly, because they cannot defend or care for themselves yet, but instead rely on responsible adults to make decisions on their behalf and to look after and protect them. Many people in hospitals are vulnerable because they are physically or mentally dependent on hospital care; they may also be in a great deal of pain or emotional distress.

As is discussed in more detail below, the vulnerability of people in schools and hospitals provides both reasons for and reasons against security measures, such as CCTV monitoring or access control.

#### *10.2 Choice in schools and hospitals*

Patients and schoolchildren have less choice about being in hospital or school than people attending museums or shopping centres. Many patients' health (even their life) is dependent on being able to stay in or access hospital. Some patients lack capacity both to give consent even where it might be sought and even to be informed of the use of CCTV. Children are required by law to be in school during certain hours of the day. The relative lack of genuinely free choice about whether to submit to security measures in hospitals and schools makes it more important to provide clear justifications for their use.

#### *10.3 CCTV in hospitals: privacy and consent*

CCTV in hospitals is used to address at least the following three kinds of security threats: threats of violence or abuse by disturbed or aggressive patients or their associates against staff and other patients; threats by terrorists and other criminals; risks of infection and complications in patients arising from a failure of staff to comply with hygiene procedures and pre-op checklists. Each of these threats invites different kinds of security measures, and each carry different risks of privacy intrusion.

##### 10. 3.1 CCTV in accident and emergency wards

Violence and abuse of staff and patients by other patients and their associates is a serious problem for hospitals, especially in accident and emergency wards and at entrances to the hospital. Such areas are open, public places, but they do often host people who are in physical and/or emotional distress, for whom monitoring would be a privacy intrusion. Fitting such areas with CCTV systems is likely to provide limited preventive benefits, especially in relation to available alternatives.[13] CCTV is more likely to be useful as a means of investigating incidents after they have occurred. But even then, the fact that cameras have to cover a relatively large space means CCTV may only provide a sketchy or rough account of events. Recent efforts to

[13] A recent study shows that design techniques have the potential to be cost-effective ways of preventing conflict in hospitals without intruding on privacy..

equip security staff with body-worn CCTV that can be activated in response to an incident seem both more promising both in terms of effectiveness and in terms of privacy.[14] Body-worn cameras can be targeted more closely at the incident in question, thus simultaneously providing a potentially more accurate account of events and excluding data that is irrelevant and potentially intrusive of privacy. The very act of announcing that one is turning on a CCTV camera may also provide an opportunity to prompt hesitation in the offender and a de-escalation of conflict.

### 10.3.2 CCTV to monitor staff hygiene

Insufficient hygiene amongst staff is a major source of infection in patients. CCTV is increasingly used as a means of monitoring hygiene procedures, such as hand-washing rates, and reporting back to staff to increase compliance. [15] Initial studies suggest the method increases significantly hygiene compliance.[16] Such use of CCTV does not raise issues of patient privacy if it is targeted only at areas where hygiene procedures are carried out, such as, for example, staff sinks.

### 10.3.3 CCTV in areas of hospitals where medical care is administered

CCTV currently used for monitoring of staff hygiene may be similarly beneficial in monitoring compliance with medical procedures, such as pre-operative check lists and routine changing of intravenous equipment (Ibid.). Cameras trained on patient beds are, however, far more privacy-intrusive than those aimed at staff hand-washing facilities. Medical care is by nature intrusive of privacy, involving, as it does, scrutiny and physical interference with the body, as well as personal questions, and intimate discussions. Receiving medical care can make people feel humiliated, ashamed or embarrassed even when the care is of the highest quality and even when it is delivered in the best interests of and with the full consent of the patient. Patients may reasonably find it humiliating, embarrassing, or just overly intrusive to be watched by security staff while receiving medical treatment, discussing their health with staff, engaging in intimate conversations with visiting family, and/or eating, sleeping and doing all the other personal activities one does while in a hospital bed. Patients are the primary recipients of both privacy intrusions and benefits to health; their views about where the proper balance between privacy and health lies determine the fairness of any particular measure to a significant extent. For this reason, hospitals considering implementing such systems should seek the views of patients in advance.

Privacy-by-design techniques such as automatic blurring of faces and muting of sound may go some way towards reducing the intrusiveness of such CCTV. Seeking consent of patients as a prior condition of turning on the cameras may also be a way of respecting patients, although this may reduce the effectiveness of the measure and will in any case not be possible in cases where the patient lacks capacity.

[14] See the following report of a trial of body-worn cameras for hospital security staff in Wales, UK. http://www.itv.com/news/wales/update/2015-02-16/security-staff-at-hospitals-to-trial-body-worn-cameras/

[15] http://www.theguardian.com/society/2012/may/08/cameras-monitor-hospital-staff

[16] Armellino et al. *Using High-Technology to Enforce Low-Technology Safety Measures: The Use of Third-party Remote Video Auditing and Real-time Feedback in Healthcare* in Clinical Infectious Diseases, Nov. 2011. Abstract available at: http://cid.oxfordjournals.org/content/early/2011/11/18/cid.cir773.short?rss=1

### *10.4 CCTV in hospitals: data protection*

Material concerning patient care that is recorded by CCTV systems is highly sensitive and requires the strictest level of data protection. Any data recording patients in beds and/or receiving or discussing their medical care must be deleted as soon as the purpose of monitoring staff gas been achieved and preferably immediately.

### *10.5 CCTV in schools*

The use of CCTV in hospitals and its use in schools raise different issues. Privacy concerns are less serious in schools because of the many and real threats to the security of schoolchildren. On the other hand, concerns arise about the potential for surveillance to interfere with important educational aims.

#### 10.5.1 CCTV for perimeter monitoring in schools: proportionality

In schools, the use of CCTV for perimeter security is relatively unproblematic ethically, even if it involves real-time monitoring by individuals. Schools are secured areas, open access to which is controlled legitimately to specific times of the day. The vulnerability of children to harm means that anyone attempting to enter or exit the school grounds via points that are not designated for entry is fair game for intrusive surveillance. Real-time monitoring of the perimeter may also be justified to identify threats to children in the form of drug-dealing, bullying by older children, or approaches by dangerous adults. However, in such cases, evidence of reason for concern should precede monitoring; monitoring should persist only as long as the concern persists; and carers and anyone approaching the school perimeter should be informed about the presence of CCTV.

Schools are often located in residential areas and as a result perimeter monitoring may involve monitoring of people's houses or the street directly outside their house. In the UK, covert monitoring of such areas is only legal if proportionate and necessary to the prevention or prosecution of serious crime.[17] If used to prevent non-serious crimes such as bullying, it may infringe the right to privacy under Article 8 of the ECHR. Schools in the UK that wish to install overt CCTV must inform the Information Commissioner and renew the notification annually. Even in countries where this is not a legal obligation school authorities should take steps to ensure their use of CCTV is compatible with privacy and data protection law.

#### 10.5.2 CCTV for internal monitoring in schools: questionable benefits and educational opportunity costs

CCTV for internal monitoring is used primarily for reactive investigation once an incident has occurred. Explicit and routine use of CCTV to resolve conflicts between pupils or establish the 'truth' of what happened in cases of rule-breaking should be approached with particular care. Unless CCTV offers blanket coverage, without blind spots, it cannot guarantee access to an uninterrupted sequence of events. More often, it provides a snapshot or series of snapshots. At the same time, the more school authorities rely on CCTV footage to identify bad behaviour, the more pupils will seek out and use blind spots as a place to break rules. Finally, the educational aims of schools are better served by human surveillance than automated systems such as CCTV. Unlike CCTV, a person pacing the corridors or wandering the playground can be a place to run to for protection or emotional support. Unlike CCTV, a person can identify incidents in real-

[17] See the Regulation of Investigatory Powers Act

time and intervene in them to protect those in need, defuse hostilities, and help to facilitate negotiation and resolution in ways that fulfil important educational aims. For these reasons, CCTV should not be used as a substitute for human surveillance in schools.

### *10.6 Access control in schools and hospitals: health and safety*

Access control in schools raises few ethical issues because it is relatively easy to distinguish in advance between those who have a legitimate reason to enter or exit school grounds at certain predetermined times and those who do not. Access control in hospitals is more complicated because it is less easy to distinguish between people who have legitimate reasons for entering hospitals and those who do not. Also, strict access control measures risk hampering the hospital's ability to respond to emergency situations in a flexible and timely manner.

### *Scenario 11 - Perimeter security – critical infrastructure (open site)*

**Summary:**

For a power station sited on the countryside, perimeter security aims to prevent malicious acts and sabotage, e.g. by illicit entry of weapons and explosives. The measures include access control with search/screening of vehicles, persons and packages, and physical barriers to prevent illicit access from VBIEDs. Attention should also be given to providing protection measures against any stand-off or airborne threat.

**Description:**

This perimeter Security scenario is particularly considering a power station sited on the countryside. Such facilities are potential targets for malicious acts and sabotage due to their economic, infrastructural, societal and political impact.

The facility is secured to different extents, depending on type of facility. The objective is to deter, detect and minimize the impact from an intruder, by means of physical barriers, access control, intrusion detection, and hostile vehicle mitigation measures (VBIED) and blast resistance. The highest security level is regarded for nuclear power plants, for which the publication INFCIRC/225 provides a set of recommended requirements to achieve the physical protection objectives.

If possible, vehicle barriers should be installed at an appropriate distance from the so called inner area to prevent the penetration of land and waterborne vehicles that could be used by an intruder for committing a malicious act. Attention should also be given to providing protection measures against any stand-off or airborne threat, such as drones.

Vehicles, persons and packages should be subject to search on entering inner areas for detection and prevention of unauthorized access and of introduction of prohibited items. Instruments for the detection of nuclear material, metals, and explosives could be used for such searches.

## Scenario 11 - Commentary on Ethics and Human Rights Issues

This scenario carries a fairly low risk of privacy intrusion. Nor does it engage concerns about the right to the protection of personal data to any great degree.

### *11.1 Freedom of movement*

Physical barriers restrict movement but they do not engage concerns about freedom of movement since, for example, power stations are not the kind of public or commercial space over which citizens generally have rightful freedom of movement. Freedom of movement concerns are, however, motivated where new barriers and checkpoints severely encroach upon formerly public space and especially where these barriers serve to make movement, for example around a city, difficult or impossible.

### *11.2 Profiling*

If profiling is used where barriers and checkpoints mark out extensive areas, making them essentially no-go areas for marked-out groups, then concerns about discrimination and social exclusion are brought into play.

### *11.3 Collateral damage (civilian injuries and deaths)*

Where measures, for example blast resistance, that are designed to deflect an attack are employed due consideration ought to be given to the proportionality of the expected damage to persons in the area towards whom an attack is likely to be deflected. Where the critical infrastructure is a military facility due consideration ought to be given to the fact that it is not generally permissible to merely trade off the lives of innocent and uninvolved civilians in order to protect military personnel. At the very least, where an attack-deflecting measure alters the risk of harm faced by persons towards whom the attack would be deflected, these persons should be informed and measures taken to mitigate their risk.

### *Scenario 12 - Perimeter security & access control - government or critical infrastructure building (urban)*

**Summary:**

Government buildings or critical national infrastructure are possible targets for terrorist attacks. A physical attack is likely to involve a form of improvised explosive device (IED), which can be person borne, vehicle borne or delivered as parcel or mail.

Access control to government buildings shall prevent illicit entry of weapons and explosives. Visitors and their belongings are screened as they enter the area. The perimeter has to be shielded by fences and barriers to prevent illicit access of VBIEDs. When sufficiently far from a building, effective perimeter security measures can significantly reduce explosive blast effects.
Access to the building will be controlled by means of identification check and by screening visitors and their belongings and vehicles for IEDs.  In some applications it may also be necessary to screen staff entering or leaving parts of the facility to ensure they are not carrying any unauthorised objects.

**Description:**

Government buildings in urban areas like parliament buildings, ministries, foreign embassies and the like or critical national infrastructure like power stations, freshwater supply etc. are popular targets for terrorists and mentally disturbed persons due to their high visibility, economic, political and psychological impact.  Therefore the access and perimeter to buildings is guarded commonly by the police.

People entering the building have to pass a security check (at the German Bundestag for example by identification check, WTMD and checking belongings by x-ray examination, [4.7]. Furthermore the access to the building by vehicles is guarded and fenced off by barriers to prevent attack through VBIED. Examining every vehicle coming into a parking lot, especially underground should be standard practice. The use of explosive detection devices - both ETD and canine explosive detection is recommended.

## Scenario 12 - Commentary on Ethics and Human Rights Issues

### *12.1 Proportionality*

Where measures, for example blast resistance, that are designed to deflect an attack are employed due consideration ought to be given to the proportionality of the expected damage to persons in the area towards which an attack is likely to be deflected. At the very least, where an attack-deflecting measure alters the risk of harm faced by persons towards whom the attack would be deflected, these persons should be informed and measures taken to mitigate their risk. Concerns about the risk to the public from deflected attacks apply to a higher degree in this case than they do with a power station in a remote location.

### *12.2 Freedom of movement*

Freedom of movement concerns are motivated where new barriers and checkpoints severely encroach upon formerly public space and especially where these barriers serve to make movement, for example around a city, difficult or impossible. Since government buildings are usually situated in densely populated cities the concerns about freedom of movement apply to a higher degree in this case than they do, for example, with a power station in a remote location.

### *12.3 Freedom of association (lawful protest)*

Government buildings are likely targets of lawful protest and it is important that lawful protest and the prevention of unlawful attack are clearly distinguished in the design of security features for such buildings. It is the case that lawful protest can degenerate into a threat and it is perfectly licit to defend against these threats but, on occasion, genuine threat and mere inconvenience are not well distinguished. The methods employed ought to enable lawful protest and unlawful threat to be clearly distinguished. Sometimes a method of defence infringes the right to protest in a certain area, for example, the police may decide that the use of a particular public square adjacent to a government building that is often used for protest can no longer be used for this purpose. For example, in the U.K., specific provisions were inserted into the Police Reform and Social Responsibility Act 2011 in order to curtail protest activity in Parliament Square. This may be permissible as a side-effect of the defensive methods employed just so long as these methods are both necessary and proportionate. However, methods that infringe rights of protest are illicit if they are designed with the express purpose of stifling the lawful expression of dissent. Such measures are likely to be incompatible with Article 11 of the European Convention on Human Rights.

### *Scenario 13 - Access control to secure location*

**Summary:**

In the fields of physical security, access control is the selective restriction of access to enclosed rooms. These are mechanisms that are designed to minimize the risk of the intrusion by unauthorized persons.

**Description:**

Secure locations include the whole and/or selected parts of government buildings, commercial buildings, critical infrastructure, transport, financial institutions, residential houses and blocks of flats, and many others. Secure locations of all kinds are subject to risks which may include theft, state or industrial espionage, invasion of privacy, disruption or attack of unauthorised access.

A typical example is a company that works with sensitive material or documents. Staff have access privileges to different parts of the building (and to the various sites where the company has operations) depending on the department they work in, their role and seniority in the organisation.

The aim of physical access control measures is to control and determine who, where and when persons are allowed to enter or to exit the buildings and/or parts of buildings. So, each entering person must be authenticated and controlled by the access control point. Usually there are two main groups of persons who need access to the buildings: Persons who are "known" to the system (e.g. staff members) and "unknown" persons (e.g. visitors). Different groups of staff and visitors may have different rights of access to each part of the location.

To avoid circumventing the access control, physical access control to secure locations must always be accompanied by other security measures such as barriers (e.g. walls or fences) and lockable gates. The gates can be unlocked by authorised people after authentication using different types of credentials:

- Possession-based authentication: Using e.g. mechanical keys or cryptographic security tokens (such as contact-based or contactless smart cards or key fobs),
- Knowledge-based authentication: Using PINs (Personal Identification Numbers) or passwords to be entered through a keypad,
- Biometric authentication: Using biometric characteristics such as fingerprint, iris, or vein patterns for the verification of the identity or the identification of authorised persons.

For stronger authentication, more than one authentication factor should be used. (e.g. combination of a smart card and a PIN number). Access control depends on secure credential management.

Typically, electronic access control systems maintain an audit log of successful and unsuccessful attempts to access different parts of the facility. This can be used to identify unusual activity and attempts to gain unauthorised access. It can also be used as a forensic tool after a security breach has occurred.

Electronic access control systems are increasingly being linked to intruder detection systems and to surveillance systems to provide a 'so called' integrated security system.

### Scenario 13 - Commentary on Ethics and Human Rights Issues

Electronic access control systems raise ethics and human rights issues when they deny access or exit to people who have a right or need to enter or exit an area, or when they permit access to individuals who have no right or need to enter. None of the three types of electronic access control technologies described above raise particular issues in principle.

#### *13.1 Mission creep: from access control to location tracking*

However, all could potentially be used to identify people and track their movements or location (either by inference via records at entry/exit points or directly via the fob or key). This has implications for both trust relations between employers and employees and the right to privacy. Data protection regulations may also be breached if records of movements or location of employees are not processed properly. Employees should always be informed if information about their movements and/or location is being collected and processed, and the purpose for which the data is collected should be explicitly specified. And finally, there is a risk of discrimination if certain individuals are unfairly singled out for monitoring.

#### *13.2 Health and safety*

Access control systems must be designed in such a way so as to be disabled in the event that ambulance staff and firefighters need to gain emergency access to premises, or in the event that individuals on the premises need to be able to exit them quickly.

## *Scenario 14 - Government building – safes - storage of sensitive documents*

**Summary:**

Many government buildings hold sensitive documents with a government security classification. These documents need to be protected against unauthorised access, including by forced attack and covert access. Safes and security cabinets are used as an element in an overall layered set of physical security measures to provide appropriate security.

**Description:**

Government and other organisations hold sensitive documents. These are typically secret documents with a government security classification held by government or other organisations with a, so called, Facility Security Clearance. They may also include commercially sensitive documents, trade secrets and the like, held by commercial organisations.

These documents are subject to attack in the form of unauthorised access, both from external attackers and persons within the organisation (the, so called, ‘insider threat’). Documents and other material, such as electronic storage media, have varying levels of sensitivity. In the case of government classified material, there are formal sets of graded requirements for the handling and storage of this material at the level of individual Member States. In terms of material with an EU security classification, there are also formal requirements and defined rules for how material should be graded in terms of the security requirements of individual Member States.

Material needs to be protected against both forced attack and against covert attempts to access the material (for example by manipulation of locks or unauthorised access and use of keys, codes and other access credentials. Covert attacks can be mitigated both by security measures to prevent their success and by measures to detect unauthorised access once it has occurred.

Safes and security cabinets are used to provide secure storage of these materials. They are not used alone, but as part of an overall set of physical security measures to deter, detect, impede and delay a potential attacker. These will include perimeter security, access management, surveillance and intruder detection alarms.

Safes (providing high security against forced and cover attack) and security cabinets providing a lower level of security against forced attack but equally high levels of protection against covert attack are typically used as the innermost layer of security. These will have strong construction, may be physically secured to prevent them being removed and have secure locks. Locks will typically be mechanical or electronic combination locks- designed to provide high security and may also be designed to detect covert attempts to open the safe.

There are well established EN standards for safes and security containers and for high security locks. Government security agencies have additional requirements which are typically not made public. They may also have their own formal evaluation and certification procedures.

## Scenario 14- Commentary on Ethics and Human Rights Issues

### *14.1 Threats of physical violence*

Unauthorised access to highly sensitive government or security and defence industry documents can result in actions that put people's lives at risk. Yet at the same time, regular access to such documents by authorised officials may be necessary for the efficient operation of government or industry business. Manufacturers of such products as well officials responsible for designing the security systems where they are located may be faced with the challenge of keeping the unwanted out but allowing relatively unhindered access to those authorised.

One approach to balancing these apparently conflicting objectives is to link biometric access keys (such as 'staff cards' or even in-built biometric readers) to safes, so that only those who are authorised can open the safe. This does not, however, protect against insider threats. Traceability of access and accountability can be used as protections against these, but when documents are kept en masse and in paper form, it is difficult to log which have been accessed and by whom. The risk remains that ill-intentioned insiders could copy, remove, photograph, and share documents they have legitimate access to. As the case of the US National Security Agency whistleblower Edward Snowden suggests, it may be very difficult in practice for security products alone to protect against insider threats. A failure in the security system in one place (e.g. to address the concerns of staff about the ethical acceptability of government/industry practices) can lead to breaches in others.

### *Scenario 16 - Cargo/ Large volume freight screening*

**Summary:**

Lorries and shipping containers can be used to carry IEDs, precursor material and other threats. These are a threat to transport; threats can also be carried across borders. Whilst finding the smaller threats in cargo is very difficult, screening techniques can be used to help mitigate these threats.

**Description:**

Various types of threat can be concealed amongst other items in cargo and other large volume shipments. These are a threat to transport systems such as road and rail (especially tunnels) and to shipping. Threats can also be carried across borders. These may be explosive devices, precursors or other threat materials.

It is generally prohibitively slow and costly to unpack items in order to screen all the items in a container. Bulk screening techniques are therefore used to help mitigate the threat.

The leading presently available, non-intrusive inspection systems for large volume freight and for containers specifically, are based on radiographic imaging systems. These include two main types- Gamma ray and X-ray. These systems allow imaging the container's content, and the signal processing applications help the operator perform a threat analysis (threats covered include persons, weapons, organic material such as explosives, and more). The main disadvantages of these systems are their high cost, relatively low screening rate and their physical dimensions. An additional important disadvantage is that the systems must be operated by a trained operator, whose capacity to analyse a complex image is nevertheless limited, and who cannot operate effectively for a lengthy period of time.

Radioactive materials are usually detected using passive Gamma radiation detectors that are installed in a portal configuration or on-board cranes. These systems are intended to detect radioactive material that is not Naturally Occurring Radioactive Materials (NORMs), and which is suspected of being an IRD (Improvised Radiological Device).

Other threat detection solutions, whether based on trace or vapour, through implementation of IMS (Ion Mobility Spectrometry), MS (Mass Spectrometry) or GC (Gas Chromatography) technologies, or the use of canines, etc., are based on portable/hand held equipment that is used to inspect and analyse a sample of the freight or vehicle in a wide range of scenarios, and whose concept of operation (CONOP) is adapted to screen containers at seaports, trains and vehicles. These systems require opening the container, sampling material or air, and analysing it either on-site or off-site to detect a threat. Therefore, the use of these technologies to inspect freight is very slow, very labour intensive, and is conducted on a relatively small number of samples.

Selective manual searching and the use of explosives detection dogs are also used in this scenario. As well as screening techniques, secure supply chain approaches can also be used to mitigate the threat of devices being hidden in cargo.

A typical example of this scenario would be the screening of shipping containers at a port. The same screening techniques have additional applications in detecting smuggling of contraband such as illicit drugs, tobacco, etc.

A related scenario is air cargo screening. This area is regulated in terms of the procedure and equipment that are used.

## Scenario 16- Commentary on Ethics and Human Rights Issues

### *16.1 Potential health risks to stowaways*

Screening raises ethical issues if it has health implications for individuals who might be screened. Even those designing screening systems without humans in mind should take the implications of human screening into account in the design process, because humans regularly stow away in containers and cargo and therefore may inadvertently be screened. While individuals choosing to stow away may well decide to take the health risks associated with screening voluntarily, this does not absolve the developers or operators of the technologies entirely from moral responsibility for the foreseeable harm that might ensue.

### *16.2 Duties to protect people found in containers or cargo who are unwell or vulnerable (victims of trafficking and people seeking asylum) and to support staff to deal with such situations*

Some technologies are designed to detect human beings. Human beings intending to migrate illegally are likely to attempt to take any measures possible to avoid being detected. Detectors should be designed with this in mind, i.e. with the aim of avoiding creating obvious ways to avoid detection that are dangerous to human life. Only border officers trained in immigration control should process any individuals found within cargo or containers at borders. Customs officers typically lack the training to be able to identify and deal with vulnerable people. If screening is done by private companies, protocols must be put in place to ensure staff are able to protect any individuals identified. Basic medical equipment, such as first aid kits, water and so on, should be available nearby. Staff should be trained and supported to deal with potentially distressing situations, such as finding people who have died in containers and cargo.

### *Scenario 17 - Automated border control*

**Summary:**

Automatic border control systems can be used to increase the speed and reduce the cost of border control operations, whilst maintaining or increasing the level of security. An automated border control (ABC) system supports automation of border crossing checks procedures for arriving and departing travellers. The ABC system checks the authenticity of an electronic machine-readable travel document (eMRTD), establishes that the traveller is the rightful holder of the eMRTD, queries border control records, and then determines the eligibility of the traveller to cross the border according to predefined rules.

**Description:**

Border control systems are costly to operate in terms of manpower and can cause frustrating delays to travellers, especially to citizens leaving or returning to their own country. Automated systems using electronically readable passports containing encrypted biometric information are typically used as a security measure.

ABC systems can be implemented as one-stop process, integrated two-step process (mantrap), or segregated two-step process. Different types of eMRTDs may be used such as electronic passports, electronic national identity cards, or electronic visas. ABC systems can establish that the traveller is the rightful holder of the eMRTD by biometric verification using face, fingers, or irises. The environment of ABC systems is designed for the collection of uniformly illuminated and optimally posed biometric samples. Unlike the individuals in the field of view of video-surveillance systems, the individuals trying to be accepted by ABC systems are cooperative.

The basic workflow operation of a two-step ABC gate is as follows: The traveller places his/her ePassport on a document reader (scanner) at the gate entrance; a first door opens; the traveller enters the kiosk and his/her face and/or fingerprint (or iris) is captured by a dedicated sensor or camera. The captured data is compared with the biometric data stored in the ePassport or a database. On a successful check, the second door opens and the traveller can continue his way. In case of negative check, depending on the infrastructure, either the passenger needs to turn back and go to manual check (which may be difficult because of other passengers queuing in front of the gate), or a side door opens so that the passenger can eventually go to manual check.

The ABC gate should be able to detect attempts of crossing the gate illegally. So for example it must be able to differentiate between real and fake passports. Similarly the biometric capture process should ensure that the presented biometric characteristics (e.g. fingerprint) is not a fake one (e.g. a silicone dummy in case of fingerprint).

### Scenario 17- Commentary on Ethics and Human Rights Issues

Two sets of ethical issues arise in relation to the use of Automatic Border Control gates. The first relates to the risks and benefits of automating border checks and the second relates to data protection concerns.

*17.1 Benefits and risks arising from automation of border control*

17.1.1 Greater security against illegal border crossing

ABC gates are better at verifying identity than border officers and this increases the protection against, for example, illegal entry via impersonation.

17.1.2 Lower risk of intimidating or frustrating interaction with border officials

People who have a legal right of free movement across a specific border may be intimidated[18] by the interaction with border officials and may feel frustration at having to prove to a border official their genuine entitlement. These feelings can be expressed in ways that make the interaction at the border check stressful for both border officers and travellers. Automated gates do involve human oversight, but this is hands-off and at a distance.

17.1.3 Lower risk of discriminatory processing of passengers

The risk of border officers' using their discretion in ways that discriminate against individuals, at border control points is reduced by the process of automation. Assuming that automatic gates are designed only to confirm the identity of the traveller, the validity of their documents, and their right to cross the border, they are not able to detect racial, ethnic, gender or other differences and act on them in ways that are prejudicial or otherwise unfair.

17.1.4 Higher risk of failure to spot and act on: children in need of protection; vulnerable individuals including victims of trafficking; non identity-related indicators of suspiciousness.

FRONTEX guidance suggests that ABC gates must always be operated in a system including both a human operator with CCTV oversight and an assistant operator to act on any problems flagged by the system or encountered by the traveller.[19] This layer of human oversight is intended to enable identification of special groups needing extra assistance and/or protection, including: children using the ABC gates;[20] vulnerable individuals such as, for example, elderly people with dementia; people with learning disabilities; or people who display indicators of being victims of trafficking. It is also intended to enable the identification of and intervention

[18] The intimidating effect of the uniforms and demeanor of border officials has led FRONTEX to recommend that border staff whose role is to help travellers operate ABC gates should wear civilian uniform (FRONTEX, 2012). Research carried out by a company called IXP Visa also revealed widespread discomfort, intimidation and fear at borders. See the Guardian Newspaper's report on the findings at http://www.theguardian.com/travel/2013/oct/10/country-most-intimidating-border-control-officials.

[19] *Best Practice Technical Guidelines for Automated Border Control Systems* Frontex Research and Development Unit, 2012. http://frontex.europa.eu/assets/Publications/Research/Best_Practice_Technical_Guidelines_for_Automated_Border_Control_Systems.pdf

[20] EU member state practice diverges on the question of whether children can use ABC gates. The question arises whether design of systems could prevent children using ABC gates. For example, systems could be programmed to reject passports with a birth date indicating childhood. This would force children to pass through manual controls and benefit from the extra scrutiny and opportunity for protection provided there.

with suspicious travellers and people who might try to undermine the system by, for example, carrying surreptitiously a baby through the border in a body-worn sling. The quality of this human oversight will be determined by the training and skills of the operator but also the demands made on their attention. A maximum of 30 minute shifts for ABC operator staff is recommended by FRONTEX guidelines. This could be enforced via access control systems to the operator viewing deck that set off an alert if it detected the same officer doing more than one consecutive shift.

### *17.2 Data protection*

While it is useful for ABC systems to collect data that will enable quality control oversight to analyse their efficiency, the principle of data minimization should guide all such measures. If stored at all, identifying data, such as images, and should be deleted as soon as possible once it has served its purpose. Effective democratic oversight of such measures requires that data collection practices should be publicly known or at least revealed annually for scrutiny to an independent body such as, for example, the UK's Independent Chief Inspector of Borders and Immigration.[21]

Like other, manual border control systems, ABC gates grant access only once a check of relevant databases has been carried out and is clear. Inaccurate or outdated data that remains on such databases can lead to unjustified interferences with traveller privacy and freedom of movement. They might also lead to the visiting of unfair suspicion on the traveller by police. It is important therefore that measures exist both to prevent inaccurate entries and to enable travellers to be informed about, contest, and request removal or revision of the information on such databases. This requires a number of privacy-by-design and accountability-by design measures, such as an automatically generated record of all inputs and revisions to the databases.

[21] http://icinspector.independent.gov.uk

### *Scenario 18 - Border crossing point – RN screening of vehicles*

**Summary:**

Border controls need to prevent the entry of illicit threat substances into a country or union. One measure is RN screening of vehicles in order to find radiological and nuclear substances.

**Description:**

EU Member States are subject to the risk of attacks by state or terrorist actors using radiological and nuclear (RN) materials. This could be in the form of a nuclear weapon, but is more likely to be some kind of ‘dirty bomb’, which spreads radioactive material over a wide area.

In Europe, the abolition of the internal borders have resulted in joint forces between EU Member States in order to attain the dual objective of improving security through more efficient external border controls. While much effort today is focused on person identification, screening of vehicles for radiological and nuclear threat substances is not covered within EU legislations.

Due to the relatively short transmission range for α and β particles, it is primarily detection of γ-radiation that is of importance when screening vehicles at border controls. Stationary vehicle portals are typically based on plastic or NaI(Tl) scintillator technology but also HPGe technology is used today. For neutron detectors, typically gas ($^{3}$He) detectors are available, often in combination with gamma detector portals. In general, neutron detector portals are more rarely used compared to gamma detectors.

The border checkpoint has skilled staff responsible for managing the security operation. Typically it is the border police that are responsible. Staff experience is of importance and the thoroughness of the screening could be adapted, depending on e.g. nationality and behaviour. Commuters and government personnel, e.g. diplomats, may be processed faster in separate lanes.

The border control is sometimes integrated with the customs, thereby facilitating a close cooperation. However, while the border police focus on the prevention of an attack, the customs objective is only to focus on hindering illegal smuggling.

Thousands of vehicles are screened for RN threat substances each year, from cars to busses and trucks/cargo. Vehicle portals are not installed at internal EU borders, they are used at external borders. In a checkpoint, not all checkpoint lanes may have RN portal screening capabilities. Hand held detectors may be used as well or for complementary measurements.

Dosimeters can be used by the security personnel for RN threat indication. The dosimeters are however primarily in use for staff safety.

The screening process is not regulated and there are no harmonized testing procedures in the EU for RN detector equipment used for vehicle screening.

**Scenario 18- Commentary on Ethics and Human Rights Issues**

RN screening of vehicles for radiological and nuclear substances does not raise many distinctive ethical issues. Those it does raise come about in connection with the use of evidence-based and targeted screening, such as profiling, and the quality of and responses to the output of the detector. Only the second of these can be addressed at the stage of product design. Each is now addressed in turn:

*18.1 Relative risks of targeted and untargeted screening*

Those designing screening policies should take into account the relative costs and benefits of blanket screening, random screening, and targeted or evidence-based screening. The more targeted the screening, the less inconvenience experienced by passengers in general. Yet the more targeted the screening, the greater the suspicion visited on those singled out. And the more discretion given to border officials to choose whom to target, the greater the risk of prejudicial or otherwise unfair discrimination.

*18.2 Risks of disproportionate response*

Exposure to radiological and nuclear substances presents great potential danger to human health. The prevention of such exposure justifies in principle measures that cause significant inconvenience to travellers and involve significant interferences with people's liberty, especially the liberty of those who are suspected of intending an attack, but including those who are not. Panic and disorder are a risk of such measures. So is disproportionate use of force in relation to a suspected terrorist. In order to make sure that security measures taken in response to readings produced by such technologies are both necessary and proportionate, they must be sufficiently accurate to avoid either unnecessary measures or a failure to prevent harm. They must also be user-friendly enough to support a rational response by border police. This is partly a question of product design. Products should communicate readings that are clearly understandable to staff, but not to travellers (e.g. loud alarms that could potentially trigger panic should be avoided). For example, a reading should be accompanied by clearly understandable indication of threat level and the location of the threat. Ideally, the product would also give some indication of what steps should be taken to reduce the risk (e.g. evacuate up to X number of metres). But it is also a matter of training of operating staff. Border police must be trained to be able to interpret the readings produced by the technology effectively and respond calmly and proportionately. Clear protocols must be developed around responses to identified threats.

*18.3 Risks to safety of border police*

Border police are required to continue their professional duties even when readings from detection technology indicate that their own health may be at risk. Fairness requires that recognition of this extra duty or sacrifice is acknowledged. Measures should be put in place to enable officers to protect themselves. For example, protective clothing and de-contamination kits should be readily available to border staff responsible for overseeing responses to threats.

*18.4 Risks of malicious interference eg. hacking*

There is a risk that products at a particular border crossing could be hacked or even interfered with manually in ways that disable them and allow highly dangerous materials to pass unnoticed. Products should be designed in such a way as to make it difficult for this to occur.

Preventive design measures should be implemented with both external and insider threats in mind. Individual border officers should not be able to flip a switch that turns the scanner off, for example. Connected scanners should be protected against cyberattack. The functioning of the scanner should be monitored automatically and on an ongoing basis.

# 3 Conclusion

As is revealed by the discussion above, ethics and human rights risks posed by use of a single technology vary dramatically according to the context in which they are used. For example, whereas real-time CCTV monitoring is largely unproblematic in train stations, it is highly problematic in hospitals. Certification aimed at CCTV products coming to market cannot address the full range of privacy and data protection issues that arise with their use in these different contexts. To be able to address these issues, additional certification would need to be sought for the use of the technology in context. The CRISP project's legal analysis[22] suggests that codes of conduct for CCTV use produced by, for example, hospitals, local authorities, and schools are forms of certification in themselves. At the same time, there is a growing market for privacy-by-design certification not only for products but for companies, services and organisational processes too.[23] The potential of privacy-by-design certification and ethics-by-design certification to address ethics and human rights risks of security products will be examined in depth in a forthcoming expert meeting, and reported on in deliverable D6.3 for HECTOS in Autumn 2015.

[22] See CRISP, Evaluation and Certification Schemes for Security Products, D.4.1. Legal Analysis of Existing Schemes, p.99. http://crispproject.eu/wp-content/uploads/2015/05/CRISP_WP4_D.4.1._Legal-analysis-of-schemes-30-April_.compressed.pdf

[23] See, for example, Canada's Ryerson University's new partnership with Deloitte Canada, http://www.ryerson.ca/pbdi/certification.html, as well as more established providers such as ePrivacy, which offers privacy seals to products and companies

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 606861.

The research leading to these results has received funding from the European Union Seventh Framework Programme FP7/2007-2013 under grant agreement n° 606861.

The content of this report does not reflect the official opinion of the European Union. Responsibility for the information and views expressed herein lies entirely with the authors.