Harmonized Evaluation, Certification and Testing Of Security products

D6.1
Ethics and Human Rights Risks of Security Products

University of Warwick
Katerina Hadjimatheou

Date: 2015-05-13
Project No: 606861
FOI Designation No: FOI-2012-1271
Dissemination Level: PU
Total No of Pages: 29

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

D6.1
Ethics and Human Rights Risks of Security Products

Due date of deliverable:	2015-04-30
Actual submission date:	2015-05-13
Updated:	
Version:	1.0
FOI designation no:	FOI-2012-1271
Responsible:	Tom Sorell
Author(s):	Katerina Hadjimatheou
Number of pages:	29
Dissemination level:	PU
Start date of project:	Sep, 2014
Duration:	3 years

Summary

HECTOS is a European project focusing on harmonization of Evaluation and Certification schemes for physical security products. It will identify mechanisms to evaluate the performance of security products, as well as compliance with interoperability, regulatory, ethical, privacy and other requirements. The project will develop a roadmap for the development of new harmonised product evaluation and certification schemes.

This report builds on HECTOS Deliverable 1.1, the security product review, which provides a foundation for the work of HECTOS by categorizing and describing the principal attributes of the different physical security products that are used in the provision of physical security solutions. In this report, we identify and discuss the key ethical and human rights issues arising in connection with the design, packaging, instructions for use, and sale of the security products identified in HECTOS D1.1.

Products can be grouped into a number of broad categories by the security function they perform. HECTOS covers a wide range of product categories including:

- Barriers (fences, gates, vehicle barriers and other building components)
- Access Control (locks, safes, identity and access management, biometrics)
- Surveillance (CCTV, security lighting)
- Detection (intruder alarms, CBRN and E detection)

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

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

One aspect of the HECTOS project (www.hectos-fp7.eu) is to consider how standardisation and certification practices can better take into account the ethics and human rights aspects of security products. To that end, a distinct stream of the project's research, Work Package 6, analyses the ethics and legal issues, reviews how they have been treated in current standardisation and certification approaches, and considers how this might be improved in the future.

With this report we contribute to the first of these activities, by identifying and providing an overview of the ethics and human rights issues that arise in connection with security products. These issues are treated as risks, because they arise differently depending on the design and application of products. We do not attempt to evaluate the overall ethical acceptability of products, because to do so would require a consideration of the context in which and conditions under which they are used. We adopt the categorisation of security products established by our colleagues in Work Package 1. That categorisation is explained and presented in detail in Deliverable 1.1, HECTOS Physical Security Product Survey. This introductory report will be followed by a study in which we consider the ethics and human rights issues of security products in a range of detailed application scenarios. That report will be available online by the end of the summer, 2015.

1.2 Purpose and content of the document

In this report we introduce and provide an overview of the ethics and human rights issues that arise in connection with the use of security products. We begin, in Section 1 ‘Introduction to ethics and human rights’ by clarifying what we mean when we talk about ethics and human rights. In that Section we describe the distinctions and overlaps between ethics and human rights. And we explain why we take ethics as the primary guiding framework for the issues discussed. In Section 2 ‘Ethics and human rights issues discussed in this report’, we introduce each of the ethics and human rights issues that arise in the report. 9 broad issues are discussed: privacy; data protection; mission creep; discrimination; error; consent; dual use; freedom of movement, expression, and association; and health and safety concerns. In Section 3 ‘Ethics and human rights issues by security product category’, we examine how these issues arise in connection with each of the 4 product categories focused on by the HECTOS project: Barriers and Fences; Access Control; Surveillance; and Detection.

2 Introduction to Ethics and Human Rights

This report refers to ‘ethics and human rights issues’ in one breath, but while ethics and human rights are related, they are distinct. Ethics relates to the moral reasons that help us decide what is the right thing to do. Human rights are a specific set of legal entitlements people have in virtue of being human. Ethics overlaps with human rights, because it provides the moral reasons why people should have that specific set of legal entitlements. For example, ethics can explain why a private life is so important to human beings that they should be entitled to one even when protecting that entitlement is costly to others. But ethics can also give an explanation of when it is justified to invade people’s privacy. In this way, ethical considerations help us define the scope and limits of the human right to privacy.

Ethics is broader than human rights. Whereas human rights describe only those entitlements that are of vital importance to humans and enforceable by the law, ethics deals with all manner of rights and wrongs, even minor ones and ones that it would be wrong to enforce upon anyone. For example, human rights have nothing to say about the privacy intrusions involved in reading a friend’s diary without permission. But ethics says there are always moral reasons against reading someone’s private material without their consent, even when there are independent reasons for not using the arm of the law to enforce those reasons.

There is another way in which ethics is broader than human rights. Human rights are generally understood as describing the entitlements individuals have in relation to agents that wield significant power over them: typically the state, but also non-state actors such as the IMF or large multinational corporations. Ethics too describes these entitlements, but it does not stop there. Ethics also describes the duties individuals have *towards* the state, and indeed towards each other as individuals. It is also concerned with harms affecting groups of people, communities, and even society as a whole. What is more, it has a lot to say about the duties individuals might have towards other entities such as animals, future generations, and even the environment.

Human rights often track ethical values, but sometimes more than one human right is needed to protect a single ethical value. For example, the value of privacy is protected by both the right to privacy and the right to the protection of personal data. Roughly speaking, the former protects people from interferences in private zones, such as the home, whereas the latter protects people from losing control over personal information about themselves.

Ethics and human rights are often mutually reinforcing, but they can also depart. For example, in the ethics work for the FP7 SURVEILLE project, it was argued that there are good ethical reasons to permit police to place a bug in a person’s home, *if* the crime the person is suspected of is serious. The ethical reasons have to do with the seriousness of the harm averted by bugging relative to the seriousness of the harm bugging presents. In contrast, the human rights lawyers concluded that bugging of homes for crime-fighting purposes is always a violation of the fundamental right to privacy. The legal reasons appeal to EU legal interpretation and case-law.[i] In this case, we can conclude that bugging the homes of people suspected of serious crimes is ethically permissible but legally prohibited.

Finally, it is important to note that the issues discussed in this paper are intentionally framed as risks rather than inevitable outcomes. These risks can be greater or smaller depending on the design, manufacture, and application of products. The fact that a product is associated with an ethical risk such as, for example, privacy intrusion, does not imply that the product is ethically unacceptable. On the contrary, many risks can be and indeed are justified in practice. Whether they are or not depends on the likelihood of their occurrence and the severity of the harm they threaten, given the likely benefits of using the product in question. This report does not attempt to provide such an evaluation of the overall ethical acceptability of security products.

3 Ethics and Human Rights Issues Discussed in this Report

This section gives readers an introduction to the key topics in the range of ethics and human rights issues that arise in connection with security products. As explained in Section 1 above, the ethical issues overlap with but are broader and more numerous than the human rights concerns. For this reason, we take ethics issues as our guide to headings and starting point for discussion. Human rights issues are discussed separately only where they diverge from the ethical issues. More focused discussion of how the issues described here arise in relation to each of the four HECTOS product categories and the specific products within them will follow in Section 3. For each of the headings in this section we also provide a brief indication of some of the current measures by which developers and manufacturers of security products try to address the ethical risks. Most of these are privacy-by-design techniques, meaning measures taken at the design and manufacturing stage of product development.

3.1 Privacy Intrusion

The ability to exclude the unwanted gaze of others from one's thoughts, home, communications, private professional and intimate relationships, and body, is vital to people's ability to live a meaningful life. Privacy is one means by which we protect this ability. Security products interfere with privacy when they reveal or collect information about one's personal life or private sphere. This is why people generally agree that CCTV camera should not be placed in public bathrooms, hotel rooms, or pointing at the windows of people's houses. It is also why body scanners that reveal the naked image have met such strident opposition. Automatic concealment or deletion of personal information or images detected by security products is an example of a technical attempt to reduce their privacy intrusiveness.

3.2 Right to Protection of Personal Data

Personal data is information that can be linked to a particular person, e.g. name, birthdate, location, sexuality, gender, and so on. People have a (legal and moral) right to exercise some control of who can use their personal data and for what purposes. One reason for giving people control over their data is that it can be very revealing of their private lives and thus intrusive of privacy. Another is that data collected for use in one sphere can be used to quite different purposes if transferred to another. For example, the sharing of health data with medical staff can save lives. But it could deny basic opportunities if shared with, for example, prospective employers. Data protection regulations aim to ensure that personal data is processed in ways that are transparent and consented to by data subjects; that transactions involving data are fair; and that there are guarantees of the security of data and measures for redress if data is misused.[ii] In the EU, data protection is a fundamental right, and data protection law is more stringent than that of many other jurisdictions.

3.3 Error leading to unwarranted interference or suspicion

Security products used to identify identify suspicious people or things or to control access are subject to error, and error can result in inconvenience, privacy intrusion, mistaken suspicion, or other unpleasant outcomes for individuals. It is important that error rates are understood and taken into account when using security products in order to take measures to prevent these outcomes. Automation can filter out certain kinds of errors, namely those arising from flaws in human perception and reasoning, of which prejudicial assumptions is one example. But automation can also introduce errors. It is important that these are identifiable so that they can be rectified. This may require re-introducing a human into the security loop at an evaluation stage, who is able to verify the accuracy of the distinction made by the technology and is authorised to override automated decisions.

3.4 Discrimination and social exclusion

Security products can lead to discrimination if their use results in the imposition of unfair or disproportionate inconveniences, privacy-interferences, or suspicion on certain social or ethnic groups. In most cases, any discrimination that occurs in connection with the use of security products will be a result of the way the product is used, rather than any design feature of the product itself. For example, if people of certain ethnic backgrounds are disproportionately targeted for explosives detection checks at airports, this may count as discrimination. Here, the source of the discrimination is the decision about who to target, rather than anything about the explosives detection product. Better training of security guards is most probably the best solution.

But sometimes security products may be designed or programmed in ways that have discriminatory effects. For example, if facial biometrics products used for visas, passports, ID cards or other important access-control products consistently fail to register people who wear head-coverings for religious reasons, this may cause extra inconvenience, embarrassment, or even humiliation to such people, who would need to remove their headgear both in order to register and each time the system is used. In this case, the source of any discrimination lies primarily in the product design and not the way in which the product is deployed.[iii] Potential solutions to the problem might nevertheless be achieved by changing the conditions under which they are deployed, say by giving people the option of removing their headgear in closed cubicles.

The term ‘social exclusion’ refers to a kind of disadvantage that is a subset of discrimination. One useful definition describes it as “any unfair restriction or removal of access to the range of social goods and activities that other members of society do, or could, take for granted”.[iv] The term is often used in relation to the excluding effects standardized systems have for people who diverge from the standards, especially the disabled. In relation to security products, social exclusion of the disabled might occur if, for example, they cannot complete biometric registration for documents that provide important or essential access to services. For such cases, alternatives to biometric access management should be provided.

3.5 Consent

Generally speaking, the fact that people consent to being treated in a particular way makes that treatment less ethically suspect than it would otherwise be. Consent to the use of security products can only be given if people are aware that they are being used and have some understanding of how their use might affect them. Partial, tacit, and indirect consent are often the best we can hope for in relation to the use of security products that state agencies deploy on populations. Approval of the use of such products by legislatures provides indirect, democratic consent. More direct consent can be achieved by informing people about the use of security products. Signs telling people that they are being watched by CCTV cameras, or that they can expect biometric screening at airports, are examples of such attempts.

3.6 Dual Use

In ethics, dual use refers to the risk that a product designed for use for a legitimate purpose will be used for illegitimate purposes. For example, a security product used by police raises dual use issues if it could, if acquired by criminal gangs or terrorists, be put to harmful and illegal use. A risk of dual use also arises if a product is exported to illiberal regimes that may use it in human rights-violating ways. Password-dependent activation, disabling functions, technological back doors and export controls are all techniques for mitigating the risk of dual use.[v]

3.7 Mission or Function creep

Mission or function creep occurs when security products or the data they collect are used for a purpose other than that for which it was originally authorized, often via a gradual expansion of their application. For example, in the UK ANPR data was originally approved for collection for traffic offences; since then it has also been used to identify individuals attending political protests.[vi] Mission creep is unjustified when the new purpose to which the data is put has not been approved via a legitimate democratic process.

3.8 Mission or Freedom of movement, expression, and association

Democracy thrives when people are able to share, experiment with, express, and modify their ideas about how society should be organized. It is stunted when such activities are punished or met with official suspicion. Some security products might be used in ways that inhibit or obstruct freedom of expression and association. Fences and barriers that are used in ways that break up and disperse political rallies or protests, CCTV or ANPR cameras that are used to collect information about the identities of those who attend such events, all pose some risk to freedom of expression and association.

3.9 Health and safety concerns

Security products can be used in ways that lead to accident or unwarranted injury of human beings, whether these are the users of those products or the targets of security measures. It is important that products are both designed and put to use in ways that minimise the risks to health and safety. Few of the products discussed in what follows do pose serious risks to health and safety. Of those discussed, locks and emergency doors raise greatest concern.

4 Ethics and Human Rights Issues by Product Category

In this section we consider the ethics and human rights issues that arise in relation to products within each of the 4 broad security product categories:

- Barriers and Fences
- Access Control: Locks and Safes
- Access Control: Biometrics
- Video Surveillance Systems: CCTV
- Detection: Explosives, Weapons, CBRN

In addition to the issues outlined in Section 3 above, we discuss some risks that arise in relation to specific product categories.

4.1 Barriers, fences and gates

The ethical issues that arise in connection with the use of fences and barriers relate mainly to the possibility that they are used to detain people unjustly, to prevent people accessing places they in fact have a right to be, or to prevent people gathering for peaceful political protest. Fences and barriers neither intrude on privacy nor collect data about people. And they raise few ethical concerns if they are used to prevent people or vehicles entering areas in which they have no right to be in the first place, i.e. if the category of those they keep out matches perfectly the category that has no right to enter. In this section we consider the ethical issues that arise in relation to the use of 3 kinds of fencing: portable fencing for political gatherings; electrified fencing; and vehicle barriers.

4.1.1 Uses of fencing in political gatherings

Fencing is often used by police in cases of planned political protest to corral protesters, separate them, protect buildings, and to guide the flow and direction of protests. All of these uses of fencing raise ethical issues. Political rallies and protests are important means by which people express collectively their political views. However, even peaceful protests can interfere with the flow of traffic and people in cities, causing inconvenience. Protests can also be volatile, leading to violence and disorder. For example, protesters can turn violent, and begin to attack police or damage property, and they can themselves become the targets of anti-protest violence. Some protests are more likely to remain peaceful than others, and the extent to which it is easy to predict which protests may tend to violence varies. Police have a duty to protect the rights of peaceful protesters to assemble and express their views. They also have a duty to prevent violence, protect property, and maintain public order.

The location of protests influences the likelihood they will become violent. For example, nationalist or anti-immigrant groups sometimes choose deliberately provocative locations for their activities, such as marching through immigrant areas, or rallying outside places of worship of religious minorities. Here, the target audience is the minority group in question and the message is a threatening one. Fencing and barriers are sometimes used to re-route or corral those involved in political actions of this kind, in order to protect the minority community from threats and violence. For example, in Northern Ireland, barriers have been used to prevent a group called the Orangemen from celebrating historical victories over Catholics by marching through Catholic residential areas.[1] Fencing has also been used to prevent the outbreak of violence between protesters and counter-protesters, as in the UK between the English Defence League and Unite Against Fascism.

Dual use of fences as weapons against police and protesters

The use of fencing to restrict the movements of political groups in order to prevent minorities being threatened and intimidated, or to reduce a high risk of violence, is justified. Even when the use of fencing is justified, ethical issues may still arise if the fencing can be easily transformed into a weapon in the hands of violent individuals, as past incidents demonstrate.[vii] In order to reduce the risk of fencing leading to serious physical harm or even death, fences procured for use in scenarios of violent protest should be designed in such a way as to be a) difficult to dissemble and b) difficult to use as a weapon (e.g. difficult to throw; without very sharp edges, etc).

The right to peaceful political expression

The location of protests influences their effectiveness as an exercise of peaceful political expression. For example, many protests start or end near the seat of the government, precisely because the target audience of protesters is the rulers of the day. For this reason, it is important for protesters to be guaranteed peaceful access to zones in which government buildings are located, even when this might cause traffic and inconvenience for local workers, residents, or tourists. Even in liberal democratic jurisdictions, police are often accused of unjustly prioritizing the reduction of inconvenience to traffic and tourism over the freedom of expression and movement of protesters. Their use of security fencing and barriers to control the route, access, and flow of peaceful protesters has been criticized on these grounds. For example, London's Mayor has recently been threatened with legal action after enclosing Parliament Square with fencing that would prevent the space being used for peaceful protests.[viii] For this reason those objecting to the fencing claim it is an infringement of their right to protest peacefully. In a separate incident in London, portable steel fencing was used by police to deny access to Parliament square and the surrounding area to peaceful protesters, but not tourists or workers.[ix] This, more targeted use of fencing, led again to accusations of police interference with the right to protest peacefully (ibid).

Freedom of movement and risk to health and safety

Fencing has been used by police to corral protesters into specific areas in order to ease traffic or access to public transport facilities. This practice is known in the UK as 'kettling'. If freedom of movement is restricted in this way for extended periods of time, it can become very uncomfortable for those thus restricted. Being prevented from accessing water, food, or toilet facilities, or from sitting down, can be worse than uncomfortable for some vulnerable groups, such as the elderly, disabled, very young, or sick.

Mission creep

Concerns about **mission creep** have arisen, for example, in relation to the use in protest contexts of portable steel barriers designed originally for use in CBRN incidents (ibid). CBRN incidents pose a potentially much greater threat to public security than peaceful protests. Therefore, at least in principle, they justify greater interferences with freedom of expression, association, and movement. Barriers and fences designed for use in CBRN incidents may be more suited to predictably violent protests and disorder than to political protests.

4.1.2 Electric fences

In Europe, electric fencing is used mainly for agricultural purposes, rather than for security. Nevertheless, it is also marketed as a tool for the protection of private property and for securing state institutions such as immigration detention centres, prisons, and high-security infrastructure sites.

Disproportionate infliction of physical discomfort or harm

Harming people intentionally is only justified when they themselves pose a credible threat of harm. Electric fencing inflicts at best discomfort and at worse severe burns or death on people or animals that touch it. The extent of the harm done depends on the voltage delivered. The harm done via electrocution should be both necessary and proportionate to the harm prevented. The 'UN Basic Principles on the Use of Force and Firearms' state that force should only be used as much as is necessary and that lethal force should not be used except when strictly unavoidable in order to protect life. For example, using electric fences with voltages high enough to deliver serious burns in order to protect property would present a disproportionate, and therefore unjustified use of force because the act of trespass is illegal, but does not threaten life. The same can be argued for other uses of lethal electric fencing, such as the reinforcement of borders. Lethal electric fencing for the protection of private property would be illegal to use in the UK and in the EU more widely, yet has been marketed in at least one security product fair in the UK.[1] Amnesty International published a press release criticizing the decision to permit the company to promote this product in the UK.

Dual use leading to human rights violations

High voltage-emitting electric fencing may be used by undemocratic or oppressive regimes in ways that violate a range of human rights. For example, in Kenya the has been forcibly resettled outside of an area fenced off for the protection of Rhinos, but which contains the hundreds of forest beehives they depend on for their livelihood.[x] Lethal electric fencing has also been used for border control in South Africa, leading to numerous reported injuries and deaths.[xi] Export controls should prevent EU-based companies selling electric fences for use in ways that violate human rights abroad.

Risks to health of minor electrocution

Some people might suffer significant health consequences even from weak electric shocks of the kind that would cause mere discomfort to most. This, more vulnerable group might include people with heart difficulties, and those who suffer from anxiety or panic attacks. It is important that people are given the opportunity to stay away from such fences, and that means being informed on site of what might happen to them if they do not. In South Africa, uncertainty amongst irregular migrants about whether the voltage on electrified border fencing was switched to lethal or non-lethal settings has reportedly resulted in avoidable injuries.[xii]

Reducing risks to health by electrocution

People should be alerted to the presence of electrified fencing. This is especially important in relation to fences with lethal and non-lethal settings, where there may be uncertainty about the setting in use at any specific time. But it continues to be important even when the shock emitted is weak. This is partly because people should be given the opportunity to avoid even relatively minor physical discomfort. But, more importantly, it helps to protect the minority of people who may suffer serious consequences even from weak electric shocks. For this reason, users of such fencing are legally obliged to display signs at regular specified distances warning people of the voltage contained in the fence. In addition to the basic legal requirements, we suggest that, in order to ensure that this requirement is understood and consented to, manufacturers should display it in a way that is impossible for the consumer to overlook. Having the requirement included somewhere discreet in the instructions for installation will not be sufficient. Instead, for example, the legal requirement could be written on a sticker, also distinguished by an attention-grabbing warning sign that must be removed (and thus read) before the product is used.

4.1.3 Vehicle barriers

Few ethical issues arise in connection with vehicle barriers, as they tend to be placed in areas vehicles are legitimately prohibited from entering.

Health and safety

It is possible that vehicle barriers risk limiting people’s access to emergency assistance if they are placed in such as way as to also block emergency vehicles, such as fire engines or ambulances, from approaching a building.

Social exclusion

Vehicle barriers may result in social exclusion if they obstruct access to public buildings for people in wheelchairs, with prams, or with other mobility requirements.

4.2 Access management: locks and safes

Ethical issues arise in connection with locks when they keep people out of places that they have a right or pressing need to be or when they confine people in places in which it is dangerous for them to be. Poor security of locks also raises issues if it leads to greater risks of unauthorised and malicious access to places where vulnerable people are located or where dangerous materials are kept

Risks to health and safety of those confined

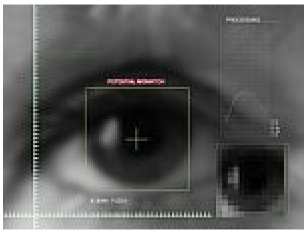
In 2014 in the USA a 16-year old died after being locked into a car in very high temperatures. The car doors could not be unlocked from the inside.[xiii] Emergency releases should be built into locks used in areas in which confinement of humans might lead to health risks and where large numbers of people may be confined leading to panic, such as hospitals or concert halls.

Unauthorised or ill-intentioned access to dangerous materials

Safes and locks that restrict access to places where dangerous materials such as weapons or chemical or biological agents are kept might be targets for ambush by criminals or terrorists. For this reason, they should be designed in such a way as to be particularly difficult to pick, break, or otherwise open maliciously. Misuse by those with authorized access can be prevented by embedding accountability measures into the access systems. These can be designed into the locks themselves. For example, a safe might be secured with a fixed number of combinations each of which is allocated to a single individual only and each of which is recorded each time the safe is opened.

4.3 Access management: biometrics

Biometric technology uses sensors to detect physical and physiological features of people. These features are used to identify people and, often via authentication of their identity, to determine whether or not they should gain access to a particular area, and monitor their movements. The ethical issues that arise in relation to use of biometrics for access management relate mainly to the risk of error, the risk of discrimination or social exclusion in registration for biometric access management facilities, privacy, mission creep, and the protection of personal data.



Privacy

Biometric data used in access management can be used to recognize and authenticate individuals, but is not typically revealing of aspects of a person’s private life. DNA data is an exception, because it can reveal information our biological relation to other human beings, and our racial ancestry, amongst other things. These are things about ourselves we have legitimate interests in deciding not to reveal, even to ourselves. Biometric access management products could result in unfair intrusions into privacy if the data is mined to reveal these aspects. The intrusion into privacy becomes especially problematic morally if this is done without the data subject’s consent.

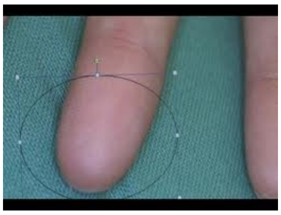
Biometric access management products can also be used to monitor people's movements and location in controlled areas to which they have been granted access. For example, some schools are using biometric identification and access management products to monitor the location and activities of pupils on school grounds. Location tracking of this sort is not tantamount to physically following an individual around, unless someone is in fact monitoring identifiable pupils' movements in real time. Even if devices are used only to set off alarms when pupils enter forbidden areas or leave school grounds, the question arises whether pupils should be thus monitored, or whether they should be given the freedom to choose not to break school rules. The age of pupils is relevant to how much freedom and trust they should be given. Location tracking is also subject to hacking and misuse by authorised staff. Therefore the general question arises whether, given the ethical risks associated with it, location monitoring is a proportionate response to the legitimate aims of school authorities to keep pupils safe and enforce school rules.

Discrimination

Biometric data used in access management systems could be used to discriminate unfairly against people, especially if it reveals ethnic traits or medical information. The possibility of unfair discrimination based on ethnicity is not a new concern: after all, faces reveal ethnic traits, and ethnic traits have historically been used as a basis to treat people pejoratively in all manner of contexts. Automating biometric access management can reduce significantly the risk of discrimination based on the ethnic prejudices of, say, border guards. However, were DNA matching to become a basis for access management, concerns might arise about the potential discrimination that could arise from the **dual-use** of that data to reveal racial ancestry, biological relations, gender, and other highly sensitive aspects of an individual's identity.

Social exclusion of those who cannot complete biometric registration

If biometrics are integrated into access management tools that enable people to access basic or important social goods and services, those who cannot register may be unfairly disadvantaged. People potentially affected include those whose fingers do not 'print well', those with diseases or conditions affecting the readability of prints, and those who lack fingers, all estimated at causing the fingerprint rejection rate of between 1-2%.[xiv] For such cases, alternatives to biometric access management should be provided.[xv] Failure to do so risks excluding such people from access (or at least relatively easy access) to social goods and services to which they are entitled.



Data protection weaknesses increasing risk of, e.g. identity theft

Insufficient protection against hacking or other unauthorised access of biometric data may enable malicious acts such as identity theft. For example, EU passports often include an RFID-chip containing photographs and fingerprints of both the passport holders' index fingers. RFID technology involves the quick transmission of information over a wireless connection, by holding the chip close to a reader. RFID readers are easily obtainable. It is therefore possible that someone other than passport control personnel could *covertly* read passports.[xvi] Despite in-built protections against unauthorised access, independent research has demonstrated that remote detection of both the presence and nationality of a passport can be achieved relatively easily.[xvii] Identity theft can incur significant financial costs, can facilitate crime, and can result in criminal suspicion or worse for innocent individuals whose identities have been stolen. This is a privacy-by-design issue that can be addressed by increasing the security of such devices.

Forgery leading to security threats

Perhaps contrary to popular belief, some biometric data can be faked. Artificial fingerprints, for example, can be created with material bought from a supermarket.[xviii] Artificial faces can be produced with the use of masks (Ibid). Vulnerabilities with a finger vein recognition device were recently revealed by an EU-funded research team with the help of a fingerprint on paper and some sellotape.[xix] Researchers on that project also highlight spoofing vulnerabilities of palm-vein recognition technologies.[xx] Biometric spoofing could be used to produce false identities for criminal or other illegal purposes. The greater the reliance on biometrics and the greater the ease of forgery, the poorer the protection offered against security threats presented by unauthorised access.

Mission creep

There are three ways in which mission creep arises in relation to biometrics for access management. The first relates to the capacity of systems used to store biometric data and the possibilities large storage poses for supplementing biometric with other forms of data. For example, RFID chips used in passports have capacity to store much more data than they currently do. This creates a technical possibility to include other potentially sensitive information alongside biometrics, thus increasing the vulnerability of individuals to hacking. This could be addressed via privacy-by-design by limiting the storage capacity of current chips. Or it could be addressed through regulatory constraints by introducing mandatory legislative action for any decision to increase the quantity and variety of sensitive data stored. The second way in which mission creep arises relates to the gradual increase in the use of biometric data for purposes other than those for which it was originally collected. This risk is higher for some kinds of biometric data than others. For example, not much other than identity can be determined from a fingerprint. A photograph is far more revealing, as it typically shows gender, age, and ethnic appearance. DNA is even more revealing, as discussed above. The risk that such data will be used for purposes beyond access management is more easily addressed by regulation of the kind just described than any privacy-by-design approach. Finally, the more data that is stored in different systems for different purposes, the more data can be cross-referenced to reveal new relationships or features of people. Government agencies commissioning new biometric systems should consider the potential of cross-referencing them with existing and planned databases and what this might mean for the design of the new systems.

Error

All biometric systems are subject to error. Error in biometric systems can lead to people being wrongly denied access or wrongly permitted access. People wrongly denied access can suffer inconvenience or more intrusive suspicion, for example, surveillance or registration in a no-fly list. Some people wrongly permitted access may pose little or no threat-- say, if they are illegal migrants looking to work. Others may pose a significant threat-- say, if they are criminals or terrorists intent on using access to commit offences. There are a range of ways to reduce the risks of error, including making careful use of automation (see the discussion of error in the introduction to ethics issues, p.8 above). Error rates should be in any case continually assessed and made as transparent as possible to procurers and users of the technology. Clear procedures should be in place for people to challenge apparent errors and to achieve redress if and when errors are revealed.

Increased risk of violent crime

Biometric solutions often promise greater security from violations of property rights, or theft, because it is harder for a person to spoof or otherwise breach a biometric system than one that relies on documents, keys, or passwords that can be transferred easily between individuals. But some biometric systems can be breached by harming people physically or otherwise coercing them. The case in 2005 of a man whose finger was severed by car thieves wanting to gain access to his biometrically-activated ignition has been much cited in this respect.[xxi] Fortunately, however, it has not as yet been much repeated. Nevertheless, concerns have recently been raised about the possibility that vulnerable people, such as children in care, could be abused by those wanting to sell their biometric data.[xxii]

4.4 Video Surveillance Systems: CCTV

A range of well-rehearsed ethics and human rights issues arise in connection with the use of CCTV. Traditionally, CCTV has been connected with intrusions into the privacy of citizens. As CCTV technology develops and becomes easier to integrate with other forms of highly identifying technology, such as facial recognition, the risks to privacy increase dramatically. But ethics and human rights concerns with CCTV go beyond privacy, raising issues of unfair suspicion, misuse and dual use, mission creep and discrimination. Issues of consent arise because the technology is developing so fast that public understandings and expectations of how CCTV is used cannot keep up.

Privacy

The privacy-intrusiveness of CCTV depends in part on the context in which it is used. For example, CCTV can intrude on privacy when it is used in areas in which people live out aspects of their private lives, such as bathrooms, changing rooms, hotel bedrooms, residential areas, places of worship, and so on. It can also be intrusive when it is covert, i.e. when its use is not declared openly via signs or other kinds of warnings, as this creates false expectations amongst those recorded about whether their actions may be monitored. Covert CCTV use is sometimes justified, especially when instigated by police in serious crime investigations. But both law and ethics require any interference with right to be no more harmful than the crime it helps to prevent or prosecute.

The privacy-intrusiveness of CCTV also depends in part on the technical specifications of the product in question. The more revealing the images are of people's identities, actions, and intentions, the more privacy-intrusive they are. High-definition and pan-tilt-zoom (PTZ) CCTV is more intrusive of privacy than low-definition CCTV. CCTV equipped with high-functioning facial recognition technology is not yet a technical reality but when it is,[xxiii] it will be far more privacy intrusive than most current systems. CCTV that also captures audio is more intrusive of privacy than CCTV that does not. Privacy-by-design techniques in use to address these issues include automatic blurring of faces that can only be reversed by a viewer with sufficient levels of authorization.[xxiv] Smart CCTV systems programmed to flag up for human attention only the kinds of behaviour the system aims to detect are also privacy-protecting, because they limit observation to what is necessary. However, as discussed below, some of the more experimental of these smart CCTV systems, might cast suspicion on innocent people.

The privacy-intrusiveness of CCTV also increases with its ability to be cross-referenced or integrated with data from other sources, such as person location tracking. A comprehensive, audio-enabled, PTZ CCTV camera network that can be integrated with ANPR and location tracking can enable police or local authorities to literally follow people around. Combine this with high-function facial recognition and voice recognition technology and we can start to imagine a scenario in which surveillance of potential criminal suspects becomes much easier and far cheaper than it is at present. It is important that such technological developments are debated publicly and that people are given meaningful opportunities to **consent** and object to this kind of tracking.

Finally, the privacy-intrusiveness of CCTV increases with the numbers of people with access to the footage.

Misuse

CCTV can be misused by those authorized to view it. For example, police and transport or local authority officials sometimes leak CCTV footage to the media in ways that could prejudice a criminal investigation, thus infringing the presumption of innocence. Leaks may also harm people's reputations. These kinds of misuse can be addressed via accountability-by-design techniques, which establish an electronic record of who has accessed the images. They can also be addressed by establishing a need-to-know policy for access to CCTV footage.

Hacking

Some CCTV systems are connected to the Internet (Internet Protocol cameras) and are therefore more vulnerable to hacking than traditional analogue systems. Remote access to CCTV feeds, often explicitly for purpose of viewing on mobile devices, is now a very widespread feature of digital video recorders.The more privacy-intrusive the CCTV system, the better protected against hackers it should be.

Dual Use

CCTV products can be purchased by criminals or governments on the open market and used in ways that violate people's human rights. CCTV cameras are increasingly discreet and this can make them more attractive to ill-intentioned agents. The more identifying CCTV becomes, for example, with the likely increased effectiveness of facial recognition add-ons, the more useful they will be to regimes intent on controlling their populations. It is difficult to control the private sale of CCTV as it is, understandably, legal for use in private areas. Export controls for security products could help to prevent the sale of intrusive CCTV to regimes posing the highest risks of human rights violations.

Mission creep

CCTV systems in urban areas are increasingly being integrated with other kinds of sensors. For example, in the UK they are integrated with ANPR cameras, and the FP7 SMART project[xxv] explores ways in which they can be integrated with audio and other sensors in an approach known as massively integrated multiple sensors installations (MIMSI). CCTV products that are designed in such a way as to be open to integration with a range of other systems may contribute to the facilitation of mission creep as new surveillance functions are incrementally added to the system. Local authorities, police, and elected politicians should have the choice to procure products that are not easily integrated with other sensors.

Erroneous suspicion

Some forms of what is known as 'smart CCTV' are programmed to search automatically through footage to detect certain kinds of behavior, both retrospectively and in real time. Running, fighting, overcrowding, and abandoning luggage are all examples of suspicious or otherwise problematic activities that smart CCTV researchers are trying to programme cameras to detect. When the suspicious activity is relatively easy to isolate and detect accurately, these systems can be both more protective of privacy and more efficient than CCTV viewed only by human observers. For example, CCTV that is programmed to sound an alarm every time a human figure approaches a prohibited area or perimeter or every time the number of humans in a given area exceeds a certain health and safety threshold is relatively easy to programme and effective to use. In contrast, CCTV that utilizes algorithms that attempt to detect broad categories of, for example, 'abnormal behaviour' at transport hubs, is more likely to result in high numbers of false positives, potentially casting suspicion on innocent individuals. Algorithms whose operation is obscure can produce false positives and negatives that are hard to detect immediately by a human examiner. The more investigation needed by a human examiner, the more inconvenience and intrusion visited on those wrongly singled out.

Discrimination

In a famous study of open-street CCTV use, Norris and Armstrong concluded that decisions to monitor people were based on race, gender, and age rather than engagement in suspicious behaviour. Teenagers, black people, and men were targeted by CCTV operators disproportionately for surveillance, and thus the discriminatory use of CCTV was demonstrated.[xxvi] Of course, non-CCTV police patrol decisions on who to monitor may well have been just as discriminatory. CCTV systems that blur out faces, thus disguising race and, to some extent, age, could reduce the extent to which discrimination occurs. Smart CCTV that detects and highlights suspicious behaviour reliably could also reduce discrimination.

False sense of security

When CCTV in public or quasi-public areas like shopping centres is clearly signposted, it may create a false sense of security in members of the public that it can and will be used to investigate any crime perpetrated against them that falls within its range of vision. In the UK at least, much signposted CCTV is either not functional or of very poor quality, thereby making it useless in criminal investigations. Even when good quality footage of a crime is available, police are not obliged by law to access and use it in criminal investigations. Both victims of crime and people wrongly accused may receive a false sense of security that the presence of CCTV increases significantly the likelihood that injustices against them will be corrected by the criminal justice system.

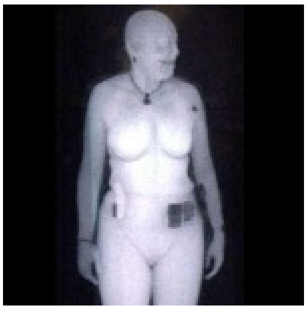
4.5 *Detection: Explosives, Weapons, CBRN*

Comparatively few human rights issues arise in connection with detection technologies *when they target objects rather than human beings*. This is because, as described in the introduction above, human rights are entitlements that can be claimed only by individuals, rather than by communities of society as a whole. For this reason, most human rights issues arising in this category relate to weapons and explosives detection products, because these target specific individuals or their property for scrutiny. The ethics issues that arise in relation to explosives and CBRN detection relate both to the impact on individual rights and wellbeing but also on the potential impact of false positives and negatives on large groups of people. For example, reliance on a product that does not work as well as its manufacturers claim can put the safety, and even the lives of humans at risk. Similarly, products with high false-positive rates can lead to unnecessary fear, restriction of liberties, and mobilization of resources.

4.5.1 Weapons and explosives detection

Privacy

Weapons detectors which, like some body scanner products, reveal images of the naked human body, are intrusive of privacy. Indeed, since 2012 their use for aviation security has been outlawed in the EU. Even when public opinion is broadly accepting of such products, as it appears to be in the USA, procurement should take into account the legitimate objections of the minority. Body scanners that are as effective at revealing weapons but do so without revealing the human body are now widely available.



Some explosives detectors are used on the contents of people's luggage at airports. Though people are generally speaking aware that their luggage may be searched at border crossings, it is unreasonable for them to be expected to remove from luggage items they do not wish to be exposed to a search. Despite expectations, luggage may still legitimately contain very personal items that are revealing of intimate or deeply private aspects of a person's life, such as medicines, prosthetics, or items that reveal sexual preferences. For this reason, if explosives detectors cannot be designed to work from a distance, searches should take place in screened-off areas.

Error leading to intrusion and false suspicion

Explosives and weapons detection products with high rates of false positives will inevitably cause inconvenience, privacy intrusion, and embarrassment for innocent people. It is important for manufacturers to communicate false positives and negatives rates to their customers clearly and in a way that enables procurers to compare different products and approaches available to them. It is also necessary to enable security officers to design reactions to a false positive in such a way as to inflict only proportionate intrusions and restrictions on those flagged as suspicious (e.g. further searches versus immediate detainment and questioning).

Error or intentional misrepresentation of effectiveness leading to risk to human life

In 2013 James McCormick was jailed for 10 years in the UK for fraud after selling more than 7,000 fake bomb detectors to police, border guards, the military and other security officers. His products (picture above) were used at checkpoints in Iraq. Reliance on them almost certainly caused civilian deaths. Reporting on the case, the Guardian Newspaper wrote: "McCormick claimed the gadgets could detect explosives at long range, deep underground, through lead-lined rooms and multiple buildings. In fact, their antennae, which appeared to be like car radio aerials, were not connected to any electronics and had no power source."[xxvii]
Even where there is no question of fraud, the clear communication of honest and scientifically verified detection rates should be given by manufacturers marketing such products. Poorly understood error rates can lead to over-reliance on technologies and unwarranted risk to human life.

4.5.2 CBRN detection

Error leading to risk to health or life

As discussed immediately above, technologies that provide false reassurance of the safety of areas, objects, or people, pose a risk to people's safety and even life. Clarity around the rates of false negatives of CBRN products and of their relation to thresholds between safety and danger is vitally important.

Error or uncertainty leading to fear, stress, panic, use of force, and unnecessary quarantine

Some detection technologies are designed to test whether individuals have been exposed to dangerous agents and can be used to determine whether they need treatment and/or quarantine. The impact of such tests on people can be temporarily detrimental to their emotional wellbeing and mental and physical health. Some people may refuse to be tested, and this might justify the use of force to prevent them putting other people at risk.
While the need to contain and treat the use of such agents justifies quite severe restrictions of people's rights in principle, the more accurate and speedily delivered the results are, the less stress, fear, panic, use of force, and unnecessary restriction on people's movements via, for example, quarantine or isolation. More generally, reports of chemical, biological or nuclear

threats can trigger panic in members of the public. This in itself may put people’s health and safety at risk. It is important that authorities gain the trust of members of the public in order to increase cooperation and reduce panic. Trust is increased by clear and well-informed communication. Accurate representation of error rates and thresholds by manufacturers to clients is therefore vital.

5 Conclusion

This report identifies ethics and human rights issues arising in connection with a range of security products. It has focused primarily on those issues that have some bearing on the design of the products, their instructions for use, and the conditions of their sale, because these are most relevant for manufacturers and vendors of such products. The report has not discussed in any depth ethics and human rights issues that can only be addressed at the stage of application. Those issues will be addressed in a forthcoming report, which considers the ethical and human rights concerns that arise in the context of a range of carefully-described typical application scenarios. That report, entitled D6.2, will be published on the HECTOS project website in the summer of 2015.

6 References

[i] Analysis and discussion of these competing accounts of the right to privacy appear in SURVEILLE deliverable D2.6 ‘Matrix of Surveillance Technologies’. http://www.surveille.eu/PDFs/D2.6%20Matrix%20of%20Surveillance%20Technologies.pdf

[ii] For excellent work on the state of the right to the protection of personal data and to redress for violations see the EU’s Fundamental Rights Agency programme of publications in this field: http://fra.europa.eu/en/publication/2014/access-data-protection-remedies-eu-member-states

[iii] Wickins (2007), ‘The ethics of biometrics: the risk of social exclusion from the widespread use of electronic identification’ *Science and Engineering Ethics*. 13(1) p.51

[iv] Burchardt, T., Le Grand, J., & Piachaud, D. (2002) Introduction in Pichauds (Eds) Understanding Social Exclusion, (pp. 1-3_ Oxford University Press.

[v] This understanding of ‘dual use’ differs from that used in EU trade to refer to products designed for civilian purposes but which may have military applications, see http://ec.europa.eu/trade/import-and-export-rules/export-from-eu/dual-use-controls/.

[vi] Guardian Newspaper, 2012 Protester sues police over surveillance database
http://www.guardian.co.uk/uk/2012/feb/09/protester-sues-police-surveillance-database
http://www.guardian.co.uk/uk/2012/feb/09/protester-sues-police-surveillance-database

[vii] ‘Who are the Orangemen?’ BBC News, 11 July, 2012. http://www.bbc.com/news/uk-northern-ireland-18769781

[vii] For example, in 2010 English Defence League members tore down fencing and threw it at police at protest in being prevented from marching through the town. ‘Violent Clashes at Mosque Protest’, *The Telegraph* Newspaper. Alastair Jaimeson, 03 April 2010. http://www.telegraph.co.uk/news/uknews/immigration/7549964/Violent-clashes-at-mosque-protest.html.

[viii] Parliament Square Fence Crushes Protest Rights, Mark Townsend, 03 Jan 2015. http://www.theguardian.com/uk-news/2015/jan/03/boris-johnson-occupy-democracy-london-protest-fence

[ix] https://www.opendemocracy.net/ourkingdom/dan-hancox/britains-policing-kettling-20-and-olympic-state-of-exception ‘Britain's policing: Kettling 2.0 and the Olympic State of Exception’ OpenDemocracy website,
DAN HANCOX 11 December 2011

[x] ‘Kenya's electrified route to human-wildlife harmony’ in New Scientist, 25 February 2015 by Fred Pearce. http://www.newscientist.com/article/mg22530104.200-kenyas-electrified-route-to-humanwildlife-harmony.html#.VTTlJ0L8RUQ

[xi] *Prohibited Persons: Abuse of Undocumented Migrants, Asylum-seekers, and Refugees in South Africa*. Human Rights Watch, New York, 1998. p.45-7.

[xii] Ibid. p.46

[xiii] ‘No Escape: California Family Sues BMW After Teen Dies in Locked Car’. *NBC News*, May 9th, 2014, by Mike Brunker. http://www.nbcnews.com/news/us-news/no-escape-california-family-sues-bmw-after-teen-dies-locked-n100881

[xiv] For a discussion of the causes of fingerprint rejection, see ‘Can You Lose Your Fingerprints?’ Katherine Harmon in *Scientific American*, Mar 29, 2009. http://www.scientificamerican.com/article/lose-your-fingerprints/

[xv] The provision of alternatives was also recommended by an EU-funded study into biometric passports: *Biometrics at the frontiers: assessing the impact on Society*, February 2005, Institute for Prospective Technological Studies, DG Joint Research Centre, European Commission.

[xvi] For an extended discussion of this issue, see

[xvii] Although in all passports the same international standards are implemented, experiments with passports from ten different countries show that characteristics of each implementation provide a fingerprint that is unique to passports of a particular country. This would mean that, with RFID readers, the nationality of everyone carrying a passport can easily be detected at a distance. H. Richter, W. Mostowski and E. Poll, *Fingerprinting passports*, published on http://www.cs.ru.nl/~erikpoll/papers/nluug.pdf.

[xviii] Research done by the EU-funded TABULA RASA investigates methods to detect artificial fingerprints. See http://ec.europa.eu/research/infocentre/article_en.cfm?id=/research/star/index_en.cfm?p=sf-20140828-biometrics&calledby=infocentre&item=Infocentre&artid=32659

[xix] See the FP7 BEAT project for a video showing how Swiss researchers achieved this https://www.beat-eu.org/news/swiss-researchers-from-the-idiap-research-institute-succeeded-to-spoof-a-commercial-finger-vein-device.

[xx] 'On the Vulnerability of Palm-Vein Recognition Technologies to Spoofing Attacks'. Pedro Tome and Sebastian Marcel, 2015. http://publications.idiap.ch/downloads/papers/2015/Tome_ICB2015-SpoofingPalmvein.pdf

[xxi] 'Malaysia car thieves steal finger', Jonathan Kent, BBC News, Thursday 31 March 2005. http://news.bbc.co.uk/1/hi/world/asia-pacific/4396831.stm

[xxii] "No difference between stealing car keys and severing fingers", Liat Clark, Wired Magazine, 26 March 2014 http://www.wired.co.uk/news/archive/2014-03/26/biometrics-stealing-body-parts

[xxiii] As Alessandro Acquisti of Carnegie Mellon University puts it: "Within a few years, real-time, automated, mass-scale facial recognition will be technologically feasible and economically efficient'. 'Facial recognition is rocketing ahead of laws that can control it', Ars Technica, 19 July 2012. http://arstechnica.com/business/2012/07/facial-regonition-tech-is-rocketing-ahead-of-laws-that-can-control-it/

[xxiv] See EU FP7 ADVISE project for an example of such techniques in the context of CCTV for urban police authorities. www.advise-project.eu.

[xxv] www.smartfp7.eu

[xxvi] Norris and Armstrong, *The Maximum Surveillance Society: The Rise of CCTV*, Berg. Oxford, 1999. The findings published in that 1999 study have reportedly been repeated in more recent studies across Europe. See Dubbeld, The Regulation of the Observing Gaze: Privacy Implications of Camera Surveillance, Printpartners, Ipskamp, Enschede, 2004 cited in IRISS Report 'Surveillance, Fighting Crime and Violence' p.181. http://irissproject.eu/wp-content/uploads/2013/04/Surveillance-fighting-crime-and-violence-report-D1.1-IRISS.pdf

[xxvii] 'Fake Bomb Detector Conman Jailed for 10 Years", *The Guardian Newspaper*. Robert Booth, Thursday 2nd May, 2013. http://www.theguardian.com/uk/2013/may/02/fake-bomb-detector-conman-jailed

Images:

Scales image courtesy of: *Image courtesy of Kittisak at FreeDigitalPhotos.net*
Facial recognition image courtesy of:
https://teknonuz.files.wordpress.com/2012/09/fbi_face_recognition_image2.png
CCTV warning sign courtesy of: http://www.amazon.co.uk/CCTV-Window-Sticker-Security-Warning/dp/B00C97JMUG
ANPR image courtesy of: http://www.automaticnumberplaterecognition.co.uk/anpr-products
Police barricade image courtesy of: *Getty Images*
Riot officers image courtesy of: *AP Photo/Matt Dunham*
Kettling image courtesy of: https://militantz.files.wordpress.com/2012/05/g20-kettle.jpg
Electric fence image courtesy of: http://www.vottle.com/home-and-garden-home-security-electric-fence-installation_v1307491#.VUjFTiFVhBc
Immigrants on fence image courtesy of: *Reuters*
Warning high voltage image courtesy of: *PinkBlue. At FreeDigitalPhotos.net*
Vehicle barrier image courtesy of: http://www.oztec.co.il/scripts/ImgView.asp?MediaID=83551
Door lock: *Image courtesy of mapichai at FreeDigitalPhotos.net*
Eye recognition software *Image courtesy of Chris Sharp at FreeDigitalPhotos.net*
Faces Image courtesy of stockimages at FreeDigitalPhotos.net
Fingerprints Image courtesy of Michael Ash http://www.ntd.tv/en/news/world/middle-east-/-africa/20111011/66841-people-without-fingerprints-israeli-researchers-explain.html
DNA *Image courtesy of sheelamohan at FreeDigitalPhotos.net*
CCTV warning courtesy of: https://aseasyasridingabike.wordpress.com/about/
Infrared surveillance warning courtesy of: http://www.mysecuritysign.com/infrared-wireless-surveillance-osha-notice-sign/sku-s-5885
CCTV control courtesy of: REUTERS/DAVID MOIR
Body scanners courtesy of: http://empowerednews.net/passengers-reassured-by-federal-officials-that-body-scanners-are-safe/183916/
Quarantine image courtesy of: http://emergencypublichealth.net/2014/10/31/quarantine/

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 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 author.