SIAM

Security Impact Assessment Measures

D4.6

Case study Report on Freedom Infringements

Yoel Raban

Shlomo Rosenberg

Yair Sharan

Work package 4

Case Study Report on freedom Infringements

Project number
261826

Call (part) identifier
FP7-Security-2010-1

Funding scheme
Collaborative Project

Content

1. Introduction

The overall aim of this work package is two-fold:

1) to generate knowledge about potential infringements associated with the technologies in our typology, and

2) to generate knowledge about measures to mitigate these infringements.

Infringements can be understood broadly as the legal, social, or cultural norms that may be intruded upon by a security measure, while counter-infringement measures refer to technologies, rules, or procedures that reduce, mitigate, and minimize those intrusions.

Infringements can be understood quite broadly as any action that an individual must accept in order to pass through a security measure. Some examples of these actions that have been discussed in previous project reports include:

- relinquishing personal property
- providing sensitive information, for example credit card information
- lifting a face covering
- submitting to a canine 'sniff search'
- altering planned movements and activities
- having information about them stored in a central database

Infringements may be better explained by the following terms:

- ***Scope*** refers to the spatial and temporal extent of the influence of a security measure upon a subject. Scope can have both physical and non-physical apsects. Physically, some security measures will be distinct in terms of both time and space. Physical barriers, gates, or fences, for example, are quite distinct on both space and time; they are physically identifiable structures that define borders between zones, and they cease to exert any influence over persons once they have been passed through. On the other hand, the use of surveillance camears across city centres reflects a much higher degree of scope insofar as it may be difficult to physically remove oneself from the reach of this security. Scope also refers to how information gathered as part of the operation of a security measure is shared with others ('spatial' scope) or retained for future use ('temporal' scope). The long data is kept or the greater the number of individuals/agencies that have access to this data the greater the scope of the measure.

- ***Normativity*** describes the degree of compulsion associated with a particular measure/technology, or in other words how much agency an individual may exert over being

monitored by a security measure/technology. Higher levels of compulsion to submit to a security measure/technology translates into means higher normativity, while lower levels of compulsion means low normativity. An example of a highly normative security practice is airport mag-and-bag checks, which are highly compulsory and offer little room for passengers to exercise any agency. This security measure is highly normative, but it is worth noting that this normativity is loosening as many airports in Europe and North America move to institute 'trusted traveler' programs wherein frequent travelers with trusted profiles are rewarded with less stringent security measures while others are subject to greater scrutiny.

- ***Intrusiveness*** refers to the kind and amount of damage a measure incures for the subject. This includes direct physical contact or even penetration of the body to subjectively perceived infringement of social norms. In general, the less intrusive a security measure/technology is the less potential for infringement. However, this rule is subject to the provision that subjects must also be **aware** that they are subject to the security measure/technology. In other words, security measures cannot be so un-intrusive that subjects are not aware they are subject to them; there should be no secret security measures.

2. Method

As recommended in the workshop guideline, the brainstorming workshop followed the 3 steps including 1) listing of potential infringements of security technologies, 2) compiling questions, that should be asked during technologies acquisition, and 3) recommending possible solutions (technologies, rules, regulations, procedures) for mitigating the impacts of the infringements.

The experts were asked to imagine a virtual departure from BGIA, where a passenger goes through the usual routine of surveillance, identification, luggage scanning, etc. In each phase the experts were asked to identify possible infringements and suggest means for mitigation.

The experts that took place in the brainstorming workshop are:

- Legal academic and an expert on human rights and technology usage
- A Ministry of Justice representative from ILITA (the Israeli Law, Information and Technology Authority)
- An expert on technologies of transportation control

3. Surveillance technologies

In this section we address surveillance cameras technology used in BGIA.

3.1 Infringements

Surveillance cameras are different than other security technologies in the sense that they operate from afar. When someone gives his fingerprints, he is aware of the action performed and may reject or accept it at will. People are generally less aware of surveillance cameras and sometimes have no idea about the possible consequences of their images being stored in video servers. There is no alternative that does not include privacy infringement. The right for privacy is based on informed consent, but is a person does not know what will become of his images then there is no consent.

LPR cameras are no different in the sense that they operate from afar and require proper notification, as well as privacy codes of conduct that will define how personal data is treated.

Taking photos in the public space is legal; however publicizing the photos may sometimes be illegal. It is forbidden to publicize photos in a manner that may embarrass persons in the photos.

3.2 Questions

- How can we make surveillance cameras more visible and noticeable to the public?
- How can we increase the awareness of people to the possible infringements of surveillance cameras?
- How can we guard passenger's privacy from surveillance cameras?
- How can we provide a non-intrusive surveillance option to passengers?

3.3 Counter infringements

Scope

Reducing the scope of surveillance cameras by:

- Limiting their coverage to areas that are more critical.
- Limiting the temporal extent of the surveillance cameras.
- Limiting the usage of the data (retention, forwarding, etc.)

Normativity

Reducing the normativity of surveillance cameras by:

- Offering an alternative where surveillance cameras are not part of the security system
- Requiring signage notifying passengers about the cameras

Intrusiveness

Reducing the intrusiveness of surveillance cameras by:

- PETs: Secure Visual Object Coding[1] technology uses cryptographic techniques to secure and hide personal information that can only be viewed by authorized personnel.

[1] Martin, K. and Plataniotis, K. N., Privacy Protected Surveillance Using Secure Visual Object Coding, IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY, VOL. 18, NO. 8, AUGUST 2008

3.4 Surveillance technologies summary

Infringements	Questions	Counter Infringement Measures	
People are generally less aware of surveillance cameras and sometimes have no idea about the possible consequences of their images being stored in video servers. There is no alternative that does not include privacy infringement. The right for privacy is based on informed consent, but is a person does not know what will become of his images then there is no consent.	• How can we make surveillance cameras more visible and noticeable to the public? • How can we increase the awareness of people to the possible infringements of surveillance cameras? • How can we guard passenger's privacy from surveillance cameras? • How can we provide a non-intrusive surveillance option to passengers?	Scope	• Limiting their coverage to areas that are more critical. • Limiting the temporal extent of the surveillance cameras. • Limiting the usage of the data (retention, forwarding, etc.)
		Normativity	• Offering an alternative where surveillance cameras are not part of the security system • Requiring signage notifying passengers about the cameras
		Intrusiveness	• PETs: Secure Visual Object Coding technology uses cryptographic techniques to secure and hide personal information that can only be viewed by authorized personnel.

4. Identification technologies

In this section we address LPR (License Plate Recognition) and biometrics technology used in BGIA for passenger's identification.

4.1 Infringements

LPR is quite similar to surveillance cameras. The main difference between the two technologies is that LPR is connected to a database of car registration (and possibly to other databases) which enable it to identify the car's owner. The potential infringements (and counter-infringements) of LPR are therefore similar to those of surveillance cameras.

Biometrics may include face recognition from camera images, but also other technologies. The use of biometrics for identification and authentication infringes human rights since bodily features (face image, fingerprints, DNA, etc.) are intimate, and individuals may not want to relinquish them to others. It is a unique identifier and individuals fear that giving it means losing control and being in danger of identity theft. Privacy concerns may arise several fears in individuals. One of them is the unintended functional scope of the biometric data, or using the data for other purposes. Another fear relates to unintended application scope – identification of subjects who do not wish to be identified.

4.2 Questions

- How can we increase the awareness of people to potential human rights infringements of biometrics?
- Is it possible to limit the use of biometric identification and authentication to a specific scope?
- How can we guard passenger's privacy from biometrics identification?
- How can we provide a non-intrusive biometrics option to passengers?

4.3 Counter infringements

Scope

Reducing the scope of biometrics by:

- Limiting the use of biometric to a very specific desired scope.
- Very strict data protection to avoid at all costs data leakages.
- Limiting the usage of the data (retention, forwarding, etc.).

Normativity

Reducing the normativity of biometrics by:

- Offering an alternative where biometrics is not part of the security system (non-biometric alternative).

Intrusiveness

Reducing the intrusiveness of biometrics by:

- PETs: Biometric Encryption (BE)[2]. The main concerns include fears of potential data matching, surveillance, profiling, and identity theft. Biometric Encryption addresses these concerns. The process securely binds a PIN or a cryptographic key to biometric data so that neither the key nor the biometric data can be retrieved from the stored template. The key is recreated only if the correct live biometric sample is presented on verification.

[2] Cavoukian, A. et al, Advances in Biometric Encryption: Taking Privacy by Design from Academic Research to Deployment, Review of Policy Research, Volume 29, Number 1 (2012)

4.4 Identification technologies summary

Infringements	Questions	Counter Infringement Measures	
The use of biometrics for identification and authentication infringes human rights since bodily features are intimate, and individuals may not want to relinquish them to others. It is a unique identifier and individuals fear that giving it means losing control and being in danger of identity theft. Privacy concerns may include unintended functional scope of the biometric data, or using the data for other purposes, and unintended application scope – identification of subjects who do not wish to be identified.	• How can we increase the awareness of people to potential human rights infringements of biometrics? • Is it possible to limit the use of biometric identification and authentication to a specific scope? • How can we guard passenger's privacy from biometrics identification? • How can we provide a non-intrusive biometrics option to passengers?	Scope	• Limiting the use of biometric to a very specific desired scope. • Very strict data protection to avoid at all costs data leakages. • Limiting the usage of the data (retention, forwarding, etc.).
		Normativity	• Offering an alternative where biometrics is not part of the security system (non-biometric alternative).
		Intrusiveness	• PETs: Biometric Encryption securely binds a PIN or a cryptographic key to biometric data so that neither the key nor the biometric data can be retrieved from the stored template. The key is recreated only if the correct live biometric sample is presented on verification.

5. Detection technologies

In this section we address scanner technologies used in BGIA for detection. The man uses of these scanning technologies are luggage scanning and whole body scanning.

5.1 Infringements

Scanners are showing the items in the luggage, some of which are private, such as diapers for adults, medicines, etc. Such items are private and generally perfectly harmless. The problems of possible infringement include the person who inspects the luggage, and also the fact that the luggage images may be stored with personal identification information. Luggage scanning may result in manual search, which is even more intrusive than mere luggage scanning although the results of manual checking are not kept in a database.

Whole body scanners have graver privacy infringements consequences, since they also show body parts that are considered very intimate similarly to strip search. The privacy concerns are of revealing the individual's naked body, including information about medical conditions, as well as of the protection of personal data that these scans generate. Privacy International claims that the use of body scanners amounts to a significant assault on the essential dignity of passengers[3].

5.2 Questions

- How can we increase the awareness of people to the possible infringements of scanners?
- How can we build trust with passengers including the option of informed consent?
- How can we guard passenger's privacy from scanners detection?
- How can we provide a non-intrusive scanning option to passengers?

5.3 Counter infringements

Scope

Reducing the scope of scanning by:

- Very strict data protection to avoid at all costs data leakages.
- Limiting the usage of the data (retention, forwarding, etc.).

Normativity

Reducing the normativity of biometrics by:

- Offering an alternative where automatic scanning is not part of the security system (manual scanning alternative).

[3] Privacy International, "PI statement on proposed deployments of body scanners in airports", 31 Dec 2009.

- Providing passengers with information about what data are processed, who is processing the data, legal remedies for protection against misuse of body scanners.

Intrusiveness

Reducing the intrusiveness of biometrics by:

- PETs: unlinking the luggage images from the personal information of its owner. This can be dine by randomal scanning that where the operator cannot identify the passenger.
- PETs: The images produced by these scanners were too revealing (showing intimate body parts) and it became clear that they would harm passengers privacy and offend them (and would also embarrass their security officials). To overcome the objections, one of the developers of scanners technology (Pacific Northwest National Laboratory – PNNL) decided to develop privacy algorithms that enable the elimination from the imagery of all human features that may be considered intrusive[4].
- Develop proper codes of practice.

[4] Cavoukian, A., Whole Body Imaging in Airport Scanners: Building in Privacy by Design, 2009. http://www.ipc.on.ca/images/Resources/wholebodyimaging.pdf

5.4 Detection technologies summary

Infringements	Questions	Counter Infringement Measures	
Scanners are showing the items in the luggage, some of which are private, such as diapers for adults, medicines, etc. Such items are private and generally perfectly harmless. Whole body scanners have graver privacy infringements consequences, since they also show body parts that are considered very intimate similarly to strip search. The privacy concerns are of revealing the individual's naked body, including information about medical conditions, as well as of the protection of personal data that these scans generate.	• How can we increase the awareness of people to the possible infringements of scanners? • How can we build trust with passengers including the option of informed consent? • How can we guard passenger's privacy from scanners detection? • How can we provide a non-intrusive scanning option to passengers?	Scope	• Very strict data protection to avoid at all costs data leakages. • Limiting the usage of the data (retention, forwarding, etc.).
		Normativity	• Offering an alternative where automatic scanning is not part of the security system (manual scanning alternative). • Providing passengers with information about what data are processed, who is processing the data, legal remedies for protection against misuse of body scanners.
		Intrusiveness	• PETs: Unlinking the luggage images from the personal information of its owner. Developing privacy algorithms that enable the elimination from the imagery of all human features that may be considered intrusive.

6. Information processing

In this section we discuss pre check-in information technologies for determining traveler's risk. The idea is that airport security will engage in information processing activities of potential passengers prior to check-in at the airport (sometimes called PreCheck). Passengers will be given a trusted traveler certificate stating their security level and will be treated accordingly when they arrive at the airport.

6.1 Infringements

Using information technologies in order to determine the level of risk associated with potential passengers infringes human rights if it discriminates people on the basis of race, ethnicity, national origin, sexual orientation, etc. Profiling based on these characteristics goes against major human rights treaties, such as the International Covenant on Civil and Political Rights (ICCPR)[5]. Naturally, the knowledge of the public about such information processing activities may invoke "big brother" feelings. Individuals may reject the fact that the authorities are using their social media interactions for determining their riskiness level. There is also a need to guard the secrecy of passengers whose security level does not allow them the benefits of trusted traveler.

6.2 Questions

- How can we increase the awareness of people to the possible privacy infringements of information processing and PreCheck plans?
- How can we guard passenger's privacy from data protection breaches?
- How can we provide an equally efficient alternative to PreCheck plans?

6.3 Counter infringements

Scope

Reducing the scope of information processing by:

- Limiting data collection to data that are strictly relevant to security.
- Very strict data protection to avoid data leakages.
- Limiting the usage of the data (retention, forwarding, etc.).

Normativity

Reducing the normativity of information processing by:

[5] http://www2.ohchr.org/english/law/ccpr.htm

- Offering an alternative to passengers where pre-check is not part of the security system (opt out).
- Transparency: allowing passengers to access their personal data.

Intrusiveness

Reducing the intrusiveness of profiling by:

- PETs:

6.4 Information processing summary

Infringements	Questions	Counter Infringement Measures	
Using information technologies in order to determine the level of risk associated with potential passengers infringes human rights if it discriminates people on the basis of race, ethnicity, national origin, sexual orientation, etc. Profiling based on these characteristics goes against major human rights treaties, such as the International Covenant on Civil and Political Rights. Individuals may reject the fact that the authorities are using their social media interactions for determining their riskiness level. There is also a need to guard the secrecy of passengers whose security level does not allow them the benefits of trusted traveler.	• How can we increase the awareness of people to the possible privacy infringements of information processing and PreCheck plans? • How can we guard passenger's privacy from data protection breaches? • How can we provide an equally efficient alternative to PreCheck plans?	Scope	• Limiting data collection to data that are strictly relevant to security. • Very strict data protection to avoid data leakages. • Limiting the usage of the data (retention, forwarding, etc.).
		Normativity	• Offering an alternative to passengers where pre-check is not part of the security system (opt out). • Transparency: allowing passengers to access their personal data.
		Intrusiveness	• PETs: