SIAM
Security Impact Assessment Measures

WP 4
Regime Interactions and Freedom Infringements

Project Group Constitutionally Compatible Technology Design

Kassel University

Prof. Dr. Alexander Roßnagel

Christian Ludwig Geminn

Deliverable D4.8

Indicators of Freedom Infringements

Project number
261826

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

Funding scheme
Collaborative Project

Table of Contents

1. Introduction

The purpose of this report is to provide an analysis of the work that has been conducted in WP4 and to produce questions and indicators that can help decision makers to assess the impact of security measures on basic rights. These questions and indicators are designated for inclusion in the SIAM Assessment Support System. Both, indicators and questions, are sorted after the impact dimensions developed in SIAM.

2. Impact Dimensions

The SIAM Description of Work lists four impact dimensions: Scope of infringement, Normativity, Physical intrusiveness and Distribution. The latter was dropped during the course of the project which means that three dimensions remain: Scope, Intrusiveness and Normativity.

The following definitions for these dimensions have been developed in SIAM and are therefore applicable in this text:

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. As such, the description of scope requires the specification of properties that indicate the subject to which this reach applies. **Spatial Exposure** is a property which describes the physical and geographical extent of an infringement in relation to a subject. **Temporal Exposure** describes the temporal reach of an infringement in relation to a subject. 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 longer data is kept or the greater the number of individuals/agencies that have access to this data the greater the scope of the measure.

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 infringements of social norms. In general, the less intrusive a security measure/technology is the less potential for infringement exists. 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 unintrusive that subjects are not aware they are subject to them. The intrusiveness of an infringement can be characterised by the kinds and amounts of damage a measure incurs with the subject. It is important to distinguish between the damage that is perceived by the subject, and the damage that is publicly recognised as such at this point in time according to the laws, rights and norms within a society. Subjectively perceived damage is what the subject subjectively thinks is wrong with some action, in that damaging actions against personal assets or goods must be accepted by the subject in order to be allowed through security. The second element is the concept of a personal asset or good, to be understood in a wide sense (material and non-material). In order to pass through a security measure, scrutinised people (the subjects) may be required to accept an action against some personal asset. Publicly recognised damage is that which relates to some infringeable defined in a code of law, convention, agreement, etc.

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 translate into higher normativity, while lower levels of compulsion mean 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.

3. Questions

The following are questions derived from D4.2 to D4.6 and other research conducted in the course of the SIAM project. The questions are designated for inclusion in the assessment support system under the Freedom Infringement category of the S-T-E-Fi categorization.

The questions should be asked before implementing a security measure in order to expose possible freedom infringements following the use of that security measure. The questions have been sorted in accordance with the impact dimensions outlined above.

3.1 Scope

- Can the purpose of the SMT be fulfilled without storing data?
- Where is data stored?
- How long is data stored?
- In case an SMT uses biometrics, does it use a central database or is a decentralized method used? Can an identification process be substituted with a verification process?
- Is personal data anonymized or pseudonymized? If so, how long is data stored before these measures are taken?
- Is personal data deleted after it is no longer needed for the primary function of the SMT?
- Is the process of deleting data after a specified period performed automatically?

- If personal data is stored, are sufficient measures in place to ensure data protection?

- How long does each individual security check take?

- Are passengers / employees subjected to the SMT over an extended period of time?

- How many persons have access to the data gathered by the SMT?

- How many agencies have (remote) access to personal data? Are measures in place to ensure that only authorized parties have access to personal data?

- Is data shared between countries?

- Is it possible to process personal data through automatized processes, i.e. without involving human operators?

- Are surveillance SMTs installed in a way that they do not observe situations, objects or persons that whose surveillance is unnecessary / unrelated to security / superfluous?

- Do bystanders have the ability to watch the security check being performed / a person being subjected to the SMT? If so, how many?

- Can an SMT that is used for passenger checking be used in a way to monitor employees?

- Is the SMT linked with other SMTs?

- Is the security check performed in the presence of the person that is being checked?

- Is the effect of the SMT local or does it cover a wider area? If the latter is the case: How much space is covered by the SMT?

3.2 Intrusiveness

- Does the use of the SMT pose a health risk, however small?
- Is the SMT connected to an analysis software?
- Does the SMT gather personal data that is not relevant for fulfilling its primary function?
- Is it necessary to create a link between gathered data and a person's identity?
- Does the SMT gather data that can be used for profiling?
- Does the SMT (in itself or in combination with others) make it possible to create movement profiles? Can the SMT be used to track passengers / employees?
- Is it possible to employ privacy enhancing measures to SMTs that gather or rely on personal data?
- How can potential embarrassments following the use of detection SMTs be mitigated?
- Has the human factor been accounted for? Are human operators of SMTs motivated, well trained and burdened with no more than a manageable workload? Do operators receive training in conflict resolution and on how to deal with unusual events?
- Does the use of a certain SMT cause specific problems when dealing with children, disabled persons, the elderly or pregnant women?
- Does the way that the SMT is used stigmatize certain groups of people?
- How many people are involved in performing each individual security check? What are their roles?

- Is a less intrusive SMT available that can perform the desired task at a comparable level?

3.3 Normativity

- Are there areas that are of minimal relevance to security where people can be free from surveillance? Which degree of surveillance is necessary for which area? Do unobserved areas remain?

- Are alternative screening methods available for passengers to choose?

- Is the SMT used indiscriminately? If not, are there measures in place that ensure that profiling is performed within the bounds of the law?

- Are there groups of people that are affected by the SMT more than others?

- What is the existing regulatory framework that governs the use of a certain SMT? Are there any changes in this framework forthcoming?

- Are there any voluntary standards that give recommendations on how to use a certain SMT? Would it be beneficial to adhere to these standards on a voluntary basis?

- Are passengers aware what kind of SMT is used and in what way it is used? Is the SMTs visible or hidden? Are there signs that indicate that the SMT is in operation? Are there any obligations to inform passengers? Have language barriers been taken into account?

- Is the structure of SMTs transparent? Can passengers comprehend which SMTs are used in which manner and context? Can the structure of SMTs be revealed to the public without sacrificing the integrity of the security concept as a whole?

- Are passengers informed about the data protection standards in use?

- Are passengers familiar with a certain security technology? If a new technology is introduced, are passengers informed about the features of this technology?

- Is the purpose of the SMT clear to passengers?

- Is there a data protection officer that helps to ensure compliance with data protection laws? Is the neutrality / independence of the data protection officer ensured?

4. Indicators

The following indicators are derived from the workshops conducted by project partners UNEW, TUB, ICTAF and SiTI during WP4 and other research conducted in the course of the SIAM project. The indicators are designated for inclusion in the assessment support system under the Freedom Infringement category of the S-T-E-Fi categorization.

Like the questions, the indicators have been sorted in accordance with the impact dimensions outlined above.

4.1 Scope

- personal data is stored

- a large number of persons / agencies has access to personal data

- data is shared between countries

- data from different sources is crossed

- combined use of SMTs

- sharing of data between SMTs
- length of a security check
- “push” method for data transfers
- merging of databases
- the effect of the SMT is not just local
- SMT registers persons / objects over an extended period of time (and not just in passing)

4.2 Intrusiveness

- physical contact
- SMT invokes fear
- SMT invokes anxiety
- disabilities are exposed
- personal property has to be given up / is confiscated
- personal property is destroyed or damaged
- personal data is gathered / requested / has to be provided
- a piece of clothing has to be lifted
- a person has to (partially) undress
- SMT uses radiation with an unclear or potentially negative impact on health

- intimate details are being revealed
- religious beliefs / feelings are violated
- children / disabled persons are subjected to inappropriate treatment
- people feel demeaned / criminalized / humiliated
- touching intimate areas of the human body
- SMT is used for purposes other than maintaining security
- SMT has the potential to cause harm or injury
- SMT can be used to create movement profiles
- SMT can be used to create personality profiles
- information about a passenger's health are revealed
- a high rate of false positives
- function creep
- aggressive behavior of security personnel

4.3 Normativity

- discrimination
- no alternatives available for screening
- the sentiment of being under surveillance

- having no place to retreat from surveillance
- people feel uneasy
- people feel intimidated
- people feel persecuted / discriminated against
- disproportionality (= violation of the principle of proportionality)
    - SMT is not used to achieve a legitimate aim
    - SMT is not suitable
    - SMT is not necessary
    - STM is not adequate / not used in a reasonable way
- people are reluctant to use a certain mode of transportation because of the security measured used there
- no or limited redress possible
- no or limited transparency
- SMT does not work with certain persons (e.g. biometrics using fingerprints – amputees)
- concealed operation