SIAM

Security Impact Assessment Measures

WP4 Workshop Report

Deliverable D 4.4

Workshop Report

Global Urban Research Unit

Newcastle University

Phil Boyle
David Murakami Wood

Project number
261826

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

Funding scheme
Collaborative Project

Introduction

This report conveys the findings of a workshop held in July 2012 by members of the Newcastle University research team for the purposes of Work Package 4 of SIAM. While the empirical work of the project to date has focused on understanding the formal and informal factors at work in the evaluation and implementation of security measures at our case studies as well as future directions in security threats and technologies we have not yet advanced our understanding of the impact of security measures upon civil liberties and human rights. The aim of WP4 is to close this gap by generating knowledge about how new and existing technologies in use for transportation security may infringe upon individual rights and how these infringements may be mitigated. This has been discussed within SIAM to date in the closely coupled concepts of *infringements* and *counter-infringement measures*. These and associated concepts will be defined below after a brief review of the workshop procedures.

Workshop Procedures

The workshop was held on Friday, July 6th on the campus of UCL in London. Prospective participants were identified through websites, referrals from other participants and project members, or were otherwise known to members or the research team through scholarly networks. Approximately 15 individuals from human rights, civil liberties, and academic communities were invited to participate in the workshop with a short description of the project and workshop via email in mid-June 2012. Those expressing interest were subsequently contacted again with a more detailed invitation. Six individuals agreed to participate, resulting in a response rate of 40%. Participants were informed in the invitation of our intention to record the workshop with the permission of all participants and that this information would be used anonymously in this report. Participants were asked at the outset of the workshop to indicate their agreement to being recorded by signing a consent form. All participants provided written consent. Copies of the signed consent forms are on file with Charles Raab, SIAM Ethics Consultant, with the originals on file at Newcastle University. Both members of the UNEW research team attended the workshop (P. Boyle & D. Murakami Wood).

Definitions

As stated above, the concepts of *infringements* and *counter-infringement measures* are central to this work package. 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. The approach of the project to developing counter-infringement measures involves invoking three other concepts: scope, normativity, and intrusiveness. These terms are defined as follows:

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 unintrusive that subjects are not aware they are subject to them; there should be no secret security measures.

The idea driving these concepts is that acceptable security measures are those that incorporate effective counter-infringements measures across these three dimensions, thereby reducing the infringement profile of selected security measures. The findings below provide some initial starting points in this direction.

Workshop Results

The following sections present the findings of the workshop. Each section corresponds with the typology of technologies used in WP2 and WP5. To review, this typology consists of the following categories: surveillance technologies, detection technologies, identification technologies, and intrusion protection and defense technologies. Each section contains a discussion of infringements and counter-infringement measures associated with one technology of the type as discussed during the workshop. These findings are summarized in table form at the end of this report.

Surveillance Technologies

The discussion of surveillance gravitated around the issue of surveillance cameras. As we reported in D2.5, there were approximately 4,000 surveillance cameras used across the London Underground in 2007, and the goal of TfL at the time was to have 12,000 cameras operational by 2012 and 14,000 operational by 2014. More recent reports state that TfL has exceeded these goals and that 15,500 cameras will be in operation by the end of 2012. Efforts to build on this numerical expansion of cameras include the integration of cameras into centralized, system-wide networks and augmenting the system with analytical capabilities such as face recognition and behaviour analysis. Participants were sceptical that either of these aims would be realized in the near future but nonetheless expressed concern about the rapid growth of surveillance cameras throughout the Underground.

One of the most prominent issues associated with video surveillance identified by participants is the lack of evidence that it achieves any of the objectives ascribed to it. They noted that almost two decades of research showing that surveillance cameras reduce crime only under narrow conditions has not slowed down the growth of cameras to the point that it is now impossible to travel on the Underground without being captured on camera. As one participant put it, the only way to revoke consent to being recorded on the Underground is to not use the Underground. Related to this, participants also expressed concern that cameras appear to be deployed everywhere across the Underground in a 'just in case' fashion that places all persons under surveillance at all times rather than in relation to specifically-defined and achievable objectives. These concerns could be mitigated in the future by establishing a strong evidence base of the effectiveness of cameras to prevent certain actions and deploying cameras only for those uses.

Participants also expressed concern of the possibility of linking camera footage with Oyster card data as doing so would be able to provide a verifiable record of a persons travel patterns. While acknowledging that TfL has data protection policies in place that limit authorities from obtaining this data except through access to information requests participants expressed concern with the regime through which this policy is enforced. In relation to camera footage, participants voiced concern than there is no specific regulatory policy for how camera footage must be handled in the UK, only a voluntary code of conduct promoted by the Information Commissioner's Office. Therefore, TfL or

any public authority operating a camera network could change their policy at any time or define the terms under which footage is released of release in extremely broad terms so that the divulgence of camera footage could still be allowable according to policy. Participants therefore called for an enhanced review and enforcement regime for the regulation of surveillance cameras in the UK that includes specific rules on the collection, retention, and sharing of surveillance footage with law enforcement and security agencies.

Summary: Surveillance Cameras

Infringements

- Deployed despite lack of evidence base that they reduce crime or enhance safety
- Indiscriminate use; all users of Underground are under surveillance at all times
- Impossible to avoid, makes giving or revoking consent meaningless
- No clear legislative framework for governing the retention and sharing of footage

Questions:

- How can we ensure that our security measures are accomplishing their intended goals and only their intended goals?
- How can we limit our security measures to these objectives?
- What government or industry regulations can we look to for guidance?

Counter-Infringement Measures

- Ongoing review of specific policy objectives
- Ongoing research and evaluation to see that those objectives are met
- A nation-wide regulatory framework for surveillance cameras is needed

Detection Technologies

Detection technologies are systems or practices intended to screen people and/or objects for prohibited items, notably explosives, drugs or illegal weapons. Detection technologies may also include behaviour analysis protocols whereby staff members are trained to identify suspicious or anomalous behaviour amongst passengers by picking up on non-verbal cues. For workshop purpose the discussion of detection technologies centered on sniffer dogs and behavioural analysis.

Regarding sniffer dogs, one participant raised the point that members of certain ethnic groups, notably Muslim populations, will likely object to being screened by dogs due to religious/cultural reasons. More broadly, any individual may object to being screened by sniffer dogs out of fear or simple dislike of dogs. Broader still, participants also objected to the standing justification that the dogs do not constitute a search when it is only because of their detection capabilities that the dogs are a desirable police tool to begin with. Finally, participants also raised

the issue of false positives associated with sniffer dogs. Specifically, questions have been raised whether sniffer dogs may react to the unintended cues of their handlers more than expected, thus simply masking the propensity for human error behind the ostensible neutrality of the dog rather than removing it. Regarding behavioural analysis, participants were almost unanimous that at best it is an excuse for poor police work and at worst a legitimized form of racial profiling. Participants were reluctant to say that either form of detection could be improved upon in ways that are acceptable in democratic societies; for example, by improving behavioural assessment procedures or offering a choice of different types of dogs to be screened by. Instead, almost all participants agreed that the only standard for stop and search should be the existing legal standard of reasonable suspicion.

Summary: Sniffer Dogs and Behavioural Analysis

Infringements:

- Being near to or touched by a dogs may offend cultural sensibilities
- Some people may fear or simply dislike dogs
- Sniffer dogs may mask rather than remove propensity for humans to judge others based on stereotypes
- The use of dogs may constitute an unwarranted search
- Behavioural analysis lends itself to establishing suspicion on stereotypes and racial profiling

Questions:

- How can we respect an individual's cultural and/or personal preferences regarding dogs?
- How can we ensure that dogs are not reacting to the cues of handlers?
- How can we ensure that behavioural analysis does not open the door to racial profiling?

Counter-Infringement Measures

- Dogs should not come into contact with a person
- Dogs should only be used once suspicion is established, not in order to establish suspicion
- The use of dogs should be considered a search and therefore subject to existing search laws
- Behavioural analysis is inherently flawed and should not be a substitute for existing legal standards of stop and search

Identification & Intrusion Protection

This section merges the categories of Identification and Intrusion Protection and focuses on issues associated with Oyster cards. The Oyster system was introduced by Transport for London in 2003 to simplify the fare payment system in 2003. The system uses an RFID-enabled credit card sized card that users must touch to an electronic reader upon entering or departing the London Underground and other transport services where the card is accepted. The card is identified by an RFID reader at gates inside the station and the appropriate fare is deducted from the holder's account, which users

can top up in a variety of ways. This necessarily involves collecting data on the point of origin and end point of travel in order to determine the fare, which is calculated according to mode and distance travelled. In terms of the SIAM typology, Oyster cards thus serve the primary function of granting or denying physical access to the Underground. What is of interest here is how it increasingly serves a secondary identification function. According to Transport for London there are around 12 million Oyster cards in use today and 13 million 'taps' each day. This is a tremendous amount of data, and though this data wasn't intended to serve security purposes it has become of interest to police and counter-terrorism authorities in the UK for its potential to track an individual's movement. After the July 2005 bombings considerable pressure was brought to police and security authorities to have unfettered access to Oyster data but this access is currently limited by legislation to specific requests on specific individuals. As we reported in WP2 the London Metropolitan Police has lodged approximately 22,000 such requests since 2008.

One participant offered the appropriate clarification that the number of requests made by authorities for Oyster data is not as important as the number of requests where data is actually turned over to authorities. It should also be noted that Oyster data is anonymized after three months, after which it would be impossible to associate the data with an individual. All participants, however, agreed that Oyster cards present the danger that authorities can reconstruct an individual's travel history. Particularly troubling for one participant the possibility of this information being used for political purposes, for example by tracking journalists or dissenters. One solution identified by participants is to anonymize the data at a much sooner point in time than the current practice of three months, perhaps one month of even a week. While doing so would minimize privacy issues TfL may be reluctant to do so as it would undermine certain customer services that rely on individualzed data. Another solution may be to create the system so that all personal information is stored on the card rather than in a centralized TfL database, which in practice would mean that TfL only received anonymous travel data.

Summary: Oyster Cards

Infringements:

- It is possible that Oyster data may be obtained by authorities and used to reconstruct one's travel patterns

Questions:

- How can we limit the use of individualized travel data?

Counter-Infringement Measures

- Anonymize travel data sooner
- Hold all data on card rather than central database

Concluding Thought

It should be noted that while the overall aim of the project was generally well-received by the group one of our participants voiced the concern that the end product of SIAM may end up being rubber stamp used by industry and/or government to show that a given system or initiative is ethically approved. This is a real concern that deserves attention. If SIAM aims to provide users with a usable program of system that takes ethics into account, how do we ensure that ethical considerations do not simply become a tick-box or, worse yet, a means to legitimize the further intensification of surveillance? How do we retain the hard edge of ethical critique while creating something useful and usable? These are questions that have to been raised in the past and must be kept at the forefront as SIAM moves forward.

WP4 Workshop Summary of Findings				
Security Measure/Technology & Technology Type (in brackets)	**Infringements**	**Questions**	**Counter Infringement Measures**	
Surveillance Cameras (Surveillance)	Arbitrary use; deployed despite lack of evidence base that they accomplish goals.	How can we ensure that our security measures are accomplishing their intended goals and only their intended goals?	Scope	
			Normativity	On going research and evaluation to assess effectiveness so that deployment is based on evidence of effectiveness
			Intrusiveness	
Surveillance Cameras (Surveillance)	Indiscriminate use; all users of Underground are under surveillance at all times.	How can we limit our security measures to these objectives?	S	Limit use of cameras to defined objectives; no indiscriminate surveillance
			N	On going review of objectives of cameras; not arbitrary surveillance
			I	On going review of internal policies to ensure camera footage is handled appropriately

Surveillance Cameras (Surveillance)	No clear legislative framework for governing the retention and sharing of camera footage in UK	What government or industry regulations can we look to for guidance?	S	A national regulatory framework for surveillance cameras is needed
			N	Cameras should only be deployed as a last resort
			I	
Sniffer Dogs (Detection)	Being near to or touched by a dogs may offend personal or cultural sensibilities	How can we respect an individual's cultural and/or personal preferences regarding dogs?	S	Dogs should only be used after suspicion is established
			N	Persons should not be screened by dogs without consent
			I	Dogs should not come into physical contact with a person

Behavioural AnalysisSniffer Dogs (Detection)	Behavioural analysis lends itself to racial profiling	How can we ensure that racial profiling does not lead to racial profiling?	S	Behavioural analysis is inherently flawed and should not be relied upon to enhance security
			N	
			I	
Oyster Cards (Identification & Intrusion Protection)	It is possible that Oyster data may be obtained by authorities and used to reconstruct one's travel patterns	How can we limit the use of individualized travel data?	S	Anonymize data as soon as possible
			N	Locate data on card rather than central databases
			I	

Sniffer Dogs (Detection)	Use of sniffer dogs may constitute an illegal search	How can we ensure that the use of dogs stays within current law pertaining to search and seizure?	S	Dogs should be used only after suspicion is established, not as a basis of suspicion
			N	
			I	