PATS

Privacy Awareness Through Security Organisation Branding

Combined National Reports and Cross-national Report on Privacy Awareness of Security Organisations

D 3.4 Report

Deliverable D 3.4

Cross-national Report by WP leader Lodz

Project number
230473

Call (part) identifier
FP7-SCIENCE-IN-SOCIETY-2008-1

Funding scheme
Coordination and support action

University of Lodz

Contents

PART I: Four Perspectives on Privacy Awareness

As was envisaged in the WP3 description, expert reports of 6 partnering countries in WP3 „Privacy Awareness of Security Agencies and Actors" were analyzed focusing on the following four categories:

- ***Legal perspective***
- ***Technology Perspective***
- ***Self-regulatory Perspective***
- ***Performance Perspective***

Legal Aspects

See below the table which compares information gathered from the partnering countries' reports. The comparison covers historical and contemporary legal aspects related to privacy awareness and security orientation with special reference to CCTV and biometrics. The comparison also includes additional legal aspects like the degree to which privacy is codified in law, the privacy violation in cases of higher necessity (public interests) and the role of the Data Protection Officer.

	GERMANY	ISRAEL	UK	FINLAND	USA	POLAND
Historical Aspects	1954: Constitution	1992: Basic Law: human dignity & liberty (Israeli emerging constitution)	No written constitution - no statutory privacy law	1999: Personal Data Protection Act	Privacy not explicitly guaranteed in the constitution caution: 1789 Bill of Rights	1997: Constitution
Specific Acts	2009: Federal Data Protection Act	1981: Privacy Protection Act 2009: Communicative Data Law	1970: Justice Report (privacy and the law); 1988: Data Protection Act; 2000: Regulation of Investigatory Powers Act (RIPA); Regulation of Investigatory Powers Scotland Act (RIPSA); 2000: Freedom of Information Act; 1988-2000: Human Rights Act; 2004: Children Act; 2006 Identity Cards Act	1987: Personal Data File Act; 2000: Communications Act; 2003: National Information Security Strategy; Publicity Law	1968: Omnibus Crime Control and Safe Streets Act, 1974: Privacy Act, 1986: Electronic Communications Privacy Act (ECPA); 2001: Patriot Act; 2002: Homeland Security Act	1997: Act on Personal Data Protection
Biometrics	x Mostly triggered by EU directives	2009 Biometric Data Base Law (more detailed than PPA concerning the saving, preserving & securing of data)	?		No specific laws	Lack of unequivocal legislation
CCTV	2001 Federal Data Protection Act; Data Protection Acts of Germany's 16 Federal States	x	x	Forbidden by law to put cameras on private spaces	No specific laws	Lack of unequivocal legislation
Abidance under EU Directives	? x	?	x	x	no	X
Privacy strongly codified in Law	x	Medium	x	low	no	No
Privacy Awareness	low	Medium	x	low	low	No
Privacy Violation in Cases of higher Necessity	x	x			x	X

Security oriented	no	x	x	no /medium	x	Medium
	GERMANY	**ISRAEL**	**UK**	**FINLAND**	**USA**	**POLAND**
Data Protection Officer	Data Protection Officer, Federal Officer for Data Protection and Freedom of Information	Law information and technology authority	Information commissioner office	Data Protection Ombudsman (DPO); Data Protection Board (DPB)	office of the chief privacy officer (dep. of homeland security); office of management and budget; federal trade commission	personal data protection general inspector; information technology and telecommunications department, protection of non-public information dep. (both within ministry of national defence)
Remarks	Very strong attitude of privacy and data protection that is basic for the legal regulations and affects the regulation of CCTV.	Data is one of the most valued and important products in modern culture. Major public debate on "the big brother law".	National program for IT is also a planned initiative within the Department of Health, to bring all NHS patients records under one central electronic database. Plan of a national database of travel which will hold the records of all journeys made in and out of the UK.	In Finland the law is respected and followed as it is as close as possible to its formal formulation.	The protection of personal information in the private sector generally relies on courts and self-regulation. Details of laws vary widely from state to state. The lack of overarching privacy legislation can be seen as a significant weakness of the US privacy regime.	
General remarks		The law is delayed in relation to technological advances and to the social norms that develop with it. The laws define the general framework of what is forbidden and what is permitted; judgment is left to judicial discretion according to the rights and circumstances.	The legislation is not keeping up with technological advances.		Fair Information Practice Principles (FIPPS) formulated by the Federal Trade Commission are common source of inspiration for how private actors regulate their activities. These ideas were further developed by the Organization for Economic Cooperation and Development (OECD) and codified in the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980)	

Technological perspective – summary

GERMANY

Technology producers see themselves as highly privacy aware and point out the importance of technology when it comes to privacy and data protection. Even though they perceive technology as a solution to existing data protection problems their security orientation is low. Newly introduced technological improvements lead to great acceptance problems among citizens. Market mechanisms determine surveillance practices - there is a central conflict between companies' rationales and the need for privacy protection – perceived as another cost factor. Among the service providers privacy awareness is relatively low; they even offer services that are in stark opposition with privacy and data protection principles.

ISRAEL

There is a general thought that the law is delayed in relation to technological development and to the social norms that evolve with it. Technology frequently challenges the right to privacy. The technological world develops rapidly and makes affordable services available to a wide spectrum of people, in a way that enables privacy violations of many, empowers terror organizations and criminal groups and thus makes security very difficult. In Israel there are two technologies that greatly influence the right to privacy. The one is the usage of closed circuit video recordings (CCTV) and the other one is biometric identification.

The interview results showed a concern within the private sector that legislation and regulation were not keeping up with technological advances in the area of CCTV and biometrics. This was particularly the case with new developments such as audio and video analytics.

In contrast the public sector interview results varied in terms of concern about regulation of CCTV and biometrics, and the privacy infringements that these technologies can bring. In the public sector some see no need for concern; the Data Protection Act is seen as sufficient and the concern is that CCTV cameras and systems need to be made more effective with regard to preventing crime. For others, however, there is a real need for a complete overhaul of the regulatory framework; and for some the way to move forward in this area is through greater public engagement.

The civil liberty groups expressed the concern that regulation and legislation has not kept up with technological advances for a long time, alongside a further concern that data protection legislation is not relevant to CCTV and biometrics. The methods by which civil liberties groups approach this issue differ. There are those who seek more public debate and attention to the issues, and those who feel it is their role to contribute directly to changes in regulation. The overriding demand is the need for change in terms of regulation.

UK

The interviews highlighted a vast difference between the private and public sector in terms of new technological developments and the rate at which these were occurring. This was particularly the case with Intelligent CCTV and biometrics. Many private sector companies are including Privacy Enhancing Technologies (PETs) in the development of visual surveillance equipment, testing these 'intelligent systems' in various places around London.

In general, private sector individuals pointed out the potential for privacy invasion that would derive from technological developments in the field of CCTV and biometrics. In general, this sector showed less concern or awareness of current privacy infringements resulting from these technologies.

The public sector was more concerned with current technologies, discussing either an adequate data protection act that is not enforced properly, or the need for reworking the data protection legislation. In both cases, privacy awareness was discussed in the context of protection of data rather than any other privacy principles (such as the right to be left alone).

FINLAND

It is a general finding that using PET systems is seen as important but people security and protection come first.

In Finland private guards are obliged to attend 100 hours of training for receiving a work permit for a period of five years. After this time they have to renew the allowance by additional training.

When Finnish were living in the countryside the control automatically functioned in the context of villages and small communities. In big cities now, where the high concentration of population gets in the way of such kind of control, CCVT and other technologies take that role. In the end, privacy is not an important topic. Anomalies or threats, disrespect towards laws are often identified by single citizens and subsequently communicated to security operators, so that even in absence of CCTV, social control itself plays a huge role.

USA

Concerning the USA there is a strong synergy between the technical developments in defence and the security sector - technologies originally designed for military applications come to be used in domestic settings such as airports, transit security, and police agencies.

Privacy was rarely seen as an issue for the use of video surveillance in public places, mainly because of the court's position that privacy can't be expected in public space.

POLAND

The security service providers show a great interest in implementing new technologies in their everyday activities. Problems arise due to the introduction of new technologies – mainly IT solutions (new information processing technologies) – which are not regulated by the provisions of law. Still the technological development is faster than the ability of regulating them by law in the aspect of securing privacy and personal data.

According to the respondents the CCTV systems in different institutions and enterprises have favourable opinions unless it infringes privacy of an individual or personnel. Generally the respondents participating in this study ascertain that in almost every institution and enterprise or company the CCTV system should be installed taking into account the needs for supervision of important areas from the point of view of interest of the enterprise and protection of property and control engineering processes, with the simultaneous maintenance of privacy protection of individuals with the exception of rest and refreshment rooms. Employees must be informed in advance about the purpose of introducing the CCTV system and areas of its operations.

Technology challenges the right to privacy all the time. In all countries there is a general thought that the law is delayed in relation to technological advances. Even though technology is perceived as a

solution to existing data protection problems great acceptance problems among citizens appear (e.g. in Germany) or introducing new technologies is not regulated by the provisions of law (in Poland). There are two technologies that greatly influence the right to privacy. The one is the usage of CCTV and the other is the biometric identification.

In the UK many private sector companies are including Privacy Enhancing Technologies (PETs) in the development of visual surveillance equipment while for Finnish people's security and protection come first. In Poland CCTV systems in different institutions and enterprises have favourable opinions unless it infringes privacy of an individual or personnel.

Performance perspective

One of the tasks of PATS was to investigate the daily routines in security practices and the manner and extent to which the general social values are protected in particular partnering countries. Owing to very scarce information included in the reports, the analysis is reduced to giving just a few examples of how these issues are addressed in the different countries.

From the reports submitted it results that i.e. in Germany the industry claims to comply with the legal framework at all times. Consequently, companies are aware of data protection laws and do not see a privacy problem.

When it comes to details, however, there is low client demand for privacy products, which may indicate that problems are often ignored on principle. The service sector has more pressing problems than privacy protection – minimum wages and quality, as well as workforce competition from Eastern Europe dominate the discourse. The knowledge about actual privacy protection efforts is missing, although there is a general feeling of trust that someone – the responsible – will take care. Data protection law is difficult to understand and handle and when it is handled, is usually either sourced out to a member of staff or an external data protection officer. Common service staff does not get in touch with principles of privacy unless they receive additional training. Trainings are carried out by external experts or with online learning programmes and tests. Legal provisions are not easily translated into organisational practice. There are Data Protection Officers and there is a Law, but organisations don't put effort into teaching all staff about privacy protection. The black boxing helps all actors involved not to bother any more with it.

In Germany's low profile security service market, qualification levels are very low and "compliance yet needs to be learned". This is a second barrier to privacy awareness within the service sector.

The very principles of privacy and data protection such as data parsimony and sensitivity are thus mostly not addressed.

At organisational level the strengthening of departments concerning data protection and compliance was mentioned. This can be seen as privacy enhancement; it was also said, however, that organisational structures may introduce measures to suggest the protection of privacy e.g. after scandals. There are considerable gaps between legal provisions with regard to privacy protection and the day-to-day practice in security organisations. Data protection law remains mysterious to most of the workforce, and Data Protection Officer Positions are not common in medium-sized companies. Responsibility is shifted to the "professional" data protection colleagues to the effect that organisational

learning is limited and most security workforce do not deal with privacy and data protection issues or concepts.

In Israel installers of the CCTV systems make sure that the cameras' movements are limited so that whoever was controlling them is unable to look inside people's houses. Sometimes, however, a customer's request not to install cameras in changing rooms or toilets is refused, which would suggest that the respect of privacy may vary considerably from company to company.

In Finland data protection and respect towards privacy don't refer to the use of security technologies, but are mainly related to the processing of information. The main issues are related to who has the right to manage information, to the transparency of the control processes, to when, where and in which cases this information can be gathered and used as well as to the limitations in the use of technologies. It's a matter of information management, processing of data, transparency of operations, clear and transparent assignment of responsibilities for the data management, but the personnel in contact with the public are often not aware of the requirements for managing certain information.

In the United States no conditions are currently in effect that would compel public agencies to incorporate privacy protections into video surveillance systems. The result is a highly uneven landscape wherein some jurisdictions follow the DHS guidelines for video surveillance while others regress to the minimal standards set out in the Fourth Amendment.

It seems that in Poland security service providers are very familiar with the problems of data and privacy protection. They understand data and privacy protection as the security function showing the area where data should not be made available or disclosed to unauthorized persons or entities. There are special regulations and procedures concerning access to information by employees. Most of those procedures regulate precisely that only a limited number of employees can have access to personal data which may be disclosed only under reasonable circumstances and in compliance with the Personal Data Protection Law. With respect to property protection, monitoring systems within the framework of CCTV are advisable although they should not infringe personnel's privacy.

Security service providers put strong stress on the protection of the privacy of clients. Personal data of clients is confidential, but it may be disclosed with the customer's approval. The access to the codes is changed after an employee who has access to the confidential information is dismissed. Companies control and keep the records of employees' and visitors' access, and the companies' confidential information is defined and described in special separate documents.

Special attention is given to systematic training of bank personnel on data protection issues. Therefore, all the employees are aware of the necessity to protect the privacy of their clients. The necessity to protect personal data is a requirement included in the terms and conditions of job contracts. In order to strengthen privacy awareness among employees, various trainings and additional schooling to broaden their knowledge and understand the importance of this problem are proposed.

Self-regulatory perspective

In this category the expert report by German partners provides a basis for the whole analysis, although due to the fact that the reports of many partners were analyzed, it was difficult to follow one consistent pattern.

The Germans mentioned three dimensions of self-regulation:

- **incentives** (companies pay attention to *avoid public slaughter, better image, ethical position*),
- **scope** (the effort to *achieve general compliance* which in the service sector can be subsumed under efforts of general professionalization; *achievement of privacy compliance* where companies aim to abide by privacy standards and the broadest scope of self-regulation is what we termed *privacy enhancement – the search for progressive privacy policies and technologies*) and
- **communication** (*intra-organisational* level, *inter-organisational* communication, for example at the level of associations and networks, and *communication to the general public* – this could include publishing Audit results, Codes of Conducts or extended Privacy Policies).

Market structure and mechanisms consist of the following SUPER CODES:

- Demand for privacy by clients
- Levels of privacy awareness among industry
- Communication about privacy by organisations

Demand for privacy by clients

It is safe to say that clients of security technology and service providers do not actively ask for privacy enhancing efforts. They do not even ask for data protection compliance, which is more readily offered by the providers than driven by clients, e.g. the demand for data protection consulting services as an add-on to CCTV cameras is low, even though this service is offered by companies. The relationship between security service and technology providers and their clients is clearly market based, and clients will simply not buy add-ons as long as they are not under pressure themselves – pressure that could transform into a financial risk, and thus render awareness and privacy services a monetary reward. Particularly family owned, traditional companies have high privacy awareness, but their strong efforts aren't communicated. There is a strong conviction that values exterior to economic maximization need to be upheld. These actors have been attributed "privacy enhancing" self-regulation efforts and thus quite high privacy awareness by us after analyzing the interviews. Attempts at improving the privacy standards in products and offering additional safeguards had been made, and authenticity was considered central rather than just a good image to be presented to shareholders. The incentives dimension is thus "ethical position" - the highest level. The communication about privacy only makes it to the inter-organisational level, for example when business partners are offered privacy friendly products. No public communication or even advertisement is carried out pointing at the comparably good privacy awareness and performance.

While it is clear that privacy awareness had been non-existent before the scandals, the reactions to this involuntary public communication vary. We distinguish two subtypes following different compensation strategies: there is compensation of image damage through active and vociferous communication of new privacy efforts, with potentially low effective change. A second strategy is to avoid presence in any discourses, especially public communication and media presence - achieving compliance is more important than repairing image damage, thus he prefers to stay silently in "the kennel" which means that communication remains at the intra-organisational level.

Levels of privacy awareness among industry

At big corporations' level communication is then extended to whomever needs to be persuaded; mainly at the intra-organisational level, but sometimes at the inter-organisational in order to reassure investors that no scandals will threaten the business in a way described above. On the motiva-

tional side, this actor remains largely uninterested and pragmatic, that is: only "public slaughter" is feared, no privacy furthering activities would be taken unless they generated income.

The fact that big data leakage (and worse) scandals in Germany have not translated into customer departure and thus monetary damage is interpreted by companies such that it is simply not that important an issue for citizens.

Levels of privacy awareness are perceived as relatively low especially among the service providers. Privacy is really no topic at all in most security firms, and that there is a discrepancy between legal text – which no one understands – and everyday practice.

Communication about privacy by organizations

While technology producers see themselves as very privacy aware, their notion of privacy also is a very narrow one. As long as everyone complies with legal frameworks, at least organisationally, and no one calls for more than this, there is no incentive for security organisations to even mention the topic in public. This is not the case in the field of the specialised technology producers whose names are not even known to the people using their technology, e.g. in biometric systems. These organisations "do not generate markets" through a better image among the public. Their communication is purely sectoral or directed towards political actors and decision makers.

From the perspective of the organisations dealing with data, it is the public's fault that their data is available especially on the World Wide Web. Against this backdrop, security professionals do not perceive a public demand or interest in more privacy protection.

Most of the interviewees **in Israel** expressed **minimal levels of privacy awareness** whatsoever, or felt that privacy issues were irrelevant to their day to day work with only small exceptions. In most cases, they show an abrogation of all ethical responsibility regarding the usage of their products.

Most responders don't deal with the concept of privacy. They just produce the equipment and have nothing to do with its installation or usage. Therefore, in companies privacy is not discussed, it does not come up in strategy meetings and it is not considered in discussions of their products' features.

Most customers want the technology that provides as much information as he can gather. Security is more important than privacy considerations. Mostly there is no interest in what happened with the equipment after it had been sold.

Security comes first: "Cost-benefit" with regards to security and privacy

Since 9/11 privacy stands in the shadow of security. In Israel, the multitudes of terror incidents over the last decade minimized the public discourse of privacy. 75% of Israeli citizens are willing to give up some of their privacy rights for more effective personal security.

"If there are privacy considerations, they are rendered irrelevant by security considerations". This attitude shows that in case of Israeli companies and society considering the security of people is more important than their privacy. Companies only take privacy into consideration if it is important to the customers. Only some companies put stress on privacy preserving features of their products.

In Finland, in addition to legal constraints, self-regulations are in accordance to people's own moral values.

The **US** privacy regulatory regime functions by issuing limited prohibitions rather than permissions. There is relative lack of legal regulations for private sector actors and privacy relays on self-regulation.

From the report of the **Polish** partners results that on the one hand the respondents are of the opinion that those modern security systems and technology, which have not been examined comprehensively, are unethical. On the other hand the use of these systems by a variety of entities such as the Police, the Polish Internal Security Agency, the Polish Government Protection Bureau is very important. Manufacturers of pharmaceutics are the ones that are extremely interested in privacy protection with regard to data protection.

PART II: Contributions of Project Partners to the General Conclusions resulting from the Interviews

This part of the report presents the contribution of project partners resulting from interviews conducted under the framework of WP 3 of the PATS project. We will now zoom out and summarize the main findings to contribute to a more focused generalization for the comparison between the different national reports related to WP 3.3. In their contribution all partners took into consideration the following aspects:

- Evaluation of privacy awareness among security sector actors: public and private (differences)
- Main concerns raised by interviewees in every partner country
- Main reasons for privacy measures implemented
- Some solutions for privacy enhancement proposed by main actors
- Threats to privacy

GERMANY

Evaluation of privacy awareness among security sector actors

There are quite different views on privacy between public and private actors. Firstly we will revisit the findings about private and then about public actors. This will clarify the differences. Before we want to stress that in general privacy is understood as data protection or more narrow: data security. This shows low privacy awareness with regard to the broader understanding of privacy including principles as data parsimony and the right to be left alone.

Private actors especially technology producers see themselves as very privacy aware, but again: they talk about data privacy, and eventually data security – a subset of privacy. The general effect of the products they support with their infrastructures is not questioned under the notion of privacy. Among the service providers privacy awareness is relatively low, they even offer services that are in stark opposition with privacy and data protection principles. Most interview partners emphasise that compliance with legal frameworks of data protection is given – *"of course"*. This rhetoric does not keep the same interviewees from stating that privacy is really no topic at all in most security firms.

So we have a general attitude of law abidance while law is somehow a black box which is the matter of data protection officers or ISO-Standards. Beyond that we find a higher awareness of privacy issues in organisation affected through image damage in consequence of privacy scandals, which is however often more a compliance backdrop then an effective instrument. Sometimes even after big data leakage (and worse) scandals in Germany this was not translated into customer departure and thus monetary damage, which is interpreted by companies such that it is simply not an important issue for them.

Public actors however show a different category of thinking: „If private actors conformed to our standard, their data protection would probably be better. But one thing is clear: we are a public security agency, and we do some things at high cost. An enterprise, contrary to us, wants to make a profit. If you want to make a profit, you act according to other premises."[1] This shows both a central conflict between companies' rationales and the need for privacy protection – perceived as another cost factor and the higher privacy awareness of public agencies hence there is a stronger public attention, and they have different priorities in regard to privacy vs. costs.

Main concerns raised by interviewees in every partner country

The issue of privacy is mainly reduced to the protection of data within a black boxed system. This part of the discourse is subsumed under the term IT security and thus ignores the quality of the data handled. A lack of qualification in privacy issues was reported from security service providers and even high level experts have a translation problem: Law experts do not understand the technological systems while engineers do not understand the law text.

The black boxing of such terms helps all actors involved not to bother any more with it. Interviewees have repeatedly pointed towards black boxes such as ISO certificates (quality management) and Data Protection Officers in order to locate accountability outside of their own field of activity, and to excuse lack of knowledge.

Further problems concern the lack of a demand for privacy in the market (again: clients are demanding surveillance technologies, scrutinised people are outside the market relations) and low public communication about privacy beyond scandals.

Main reasons for privacy measures implemented

There were single cases of interviewees showing efforts in privacy enhancement because of ethical reasons. But the application is difficult: One interviewee mentions that general qualification problems are more urgent, one interviewee avoids the communication about privacy because it is seen as a difficult and dangerous debate ("cat-and-mouse-atmosphere) and in one case, a privacy enhancing add-on was offered but not demanded – again this points towards a lacking demand for privacy at least within the market.

For public agencies a driver for privacy measures is the higher public attention on their activities, and furthermore their priority to maximize profits is beneath the priority to abide privacy laws.

Some solutions for privacy enhancement proposed by main actors

Privacy enhancements were mentioned in different dimension. With regard to Technologies (PET) blanking out technologies for CCTV-systems were offered, but there was no demand for it. Regarding data security measurements there are technologies as data encryption and access control systems to e.g. sensitive databases, but again, this is a limited understanding of privacy.

On the organisational level the strengthening of departments concerning data protection and compliance were mentioned. This can be seen as privacy enhancement, however it was also mentioned that these organisational structures may be used as pro forma measurement to pretend privacy efforts (e.g. after scandals).

Another mentioned possibility is the establishment of self-regulatory institutions like a privacy seals. There is already one institution offering privacy evaluation and seal, but this still needs to get established.

Threats to privacy

As mentioned, the main threats to privacy are lacking law abidance or a narrow interpretation of privacy as data security. This is related to the problem of black boxes as ISO standards and even legal regulations (lacking qualification and difficult translation between different fields of expertise).

Another threat is the lack of demand for privacy which is either related to a lack of market power concerning the demand for more privacy or stronger structures beyond the market assuring the effective application of existing data protection laws.

This can also be expressed as an accountability problem: Security organisations hold clients accountable for privacy issues of their customers and furthermore claim that citizen aren't privacy aware.

Further Suggestions

Especially the evident market problem challenges the PATS project's premise that self-regulation can be furthered through marketing activities, dialogue and the construction of privacy awareness as organizations' unique selling points. In our further conceptual work, we need to continue mapping the markets and actors' relationships and roles in order to point to those missing roles (e.g. a popular privacy watchdog organization) and functions or missing communication channels that inhibit self-regulatory incentives.

ISRAEL

This report has provided an overview of the methodology and results from the interview phase of the PATS project. The aim of the interviews was to assess the degree of privacy awareness across various sectors, firms and across international government agencies that promote or use security technologies.

The results of the interviews showed a concern within the private sector that legislation and regulation was not keeping up with technological advances in the area of CCTV and biometrics. This was particularly the case with new developments such as audio and video analytics. The potential for privacy protection to be built into systems at the outset was highlighted during interviews as a real possibility.

The public sector interview results varied in terms of concern about regulation of CCTV and biometrics, and the privacy infringements that these technologies can bring. For some in the public sector there is no need for concern; the Data Protection Act is sufficient and the concern is that CCTV cameras and systems need to be made more effective with regard to preventing crime. For others, however, there is a real need for a complete overhaul of the regulatory framework; and for some the way to move forward in this area is through greater public engagement.

Arising from the civil liberties interviews was a concern that regulation and legislation has not kept up to date with technological advances for a long time, alongside a further concern that data protection legislation is not relevant to CCTV and biometrics. The method by which civil liberties groups approach this issue was different (there are those who seek more public debate and attention to the issues, and those who feel it is their role to contribute directly to changes in regulation), the overriding concern was one of a need for change in terms of regulation.

UNITED KINGDOM

Evaluation of privacy awareness among security sector actors

Discussions of privacy amongst both public and private sector actors tended to centre on data protection principles and the CCTV Code of Conduct set out by the Information Commissioner in the UK. In general, private sector individuals detailed the potential for privacy invasion that would derive

from technological developments in the field of CCTV and biometrics. There was less concern, or awareness, of privacy infringements coming from these technologies currently.

The public sector was more concerned with current technologies, discussing either an adequate data protection act that is not enforced properly, or the need for a re-working of data protection legislation. In both cases, privacy awareness was discussed in the context of protection of data rather than any other privacy principles (such as the right to be left alone).

Main concerns raised by interviewees in every partner country

With regard to future developments and privacy, the private sector argued that there is an absence of personally identifiable information at the moment. However, the concern is the accidental collection of information, collection and storage of information on databases, which may be used in future for other purposes. Automatic Number Plate Recognition (ANPR) was highlighted as a major concern, with one interviewee stating “it is widely used, but not actively managed”, and another to suggest that the “Police would like ANPR for people”.

In sum, the majority of private sector organizations could be summarized as concerned that privacy and data protection legislation is not adhered to currently, while there are others who are characterized by concern about future rather than current developments in terms of privacy infringements. The overriding issue addressed in the private sector interviews was one of rapid technological developments in the area of CCTV and biometrics and a concern that legislation and regulation was not developing at the same pace.

With regard to the public sector, in terms of regulation and standards, the Interim CCTV Regulator was seen by several interviewees as a key figure in attempts being made to persuade all sides in the development of standards. However, the regulator cannot enforce these standards. The public sector interviewees also highlighted the continuing development of image quality standards, alongside a discussion over whether the Data Protection Act is applicable to CCTV. With reference to voluntary codes of conduct, the public sector abides by those set out by the Information Commissioner (although one interviewee did suggest that the Commissioner has “no teeth” in terms of regulation and enforcement of standards).

In sum, there are those within the public sector who believe data protection legislation to be adequate, just not enforced properly. There are others who suggest that an overhaul of regulation is required prior to being able to tackle privacy issues from surveillance systems.

Main reasons for security measures implemented (comparison)

In general, the private sector seemed concerned with future 'intelligent' CCTV designs and the inclusion of Privacy Enhancing Technologies (PETs) to combat any potential privacy invasion. For some this is seen as a unique selling point; the inclusion of privacy protection features will be more publicly acceptable.

The public sector seems unconcerned with public opinion regarding privacy issues, stating that the debate on CCTV has been won (i.e. the public has accepted and even support the continued use and expansion of CCTV).

Some solutions for privacy enhancement proposed by main actors

As mentioned previously, for the private sector Privacy Enhancing Technologies were viewed as the way forward in terms of privacy protection in the future. For current technologies, the Data Protection Act or Code of Conduct set out by the Information Commissioner was seen as adequate (on the whole). There was also a minority of private sector individuals who suggested a re-modelling of the Data Protection Act and the transfer of more power of enforcement to the Information Commissioner in order to combat privacy invasion.

The public sector did not discuss the technological as much as the legislative framework and the lack of adequate regulation surrounding CCTV and biometrics currently. It was suggested that a re-working of the Data Protection Act and privacy legislation in the UK was the solution. In this area the private and public sector were entirely at odds.

Threats to privacy

As mentioned at various points above, the main threat to privacy for the private sector were rapid technological advances in the area of CCTV and biometrics for which a technological solution was proposed.

For the public sector, the current lack of regulation or enforceable regulation was discussed as being the main threat to privacy.

USA

Evaluation of privacy awareness among security sector actors

The public and private actors demonstrated a degree of privacy awareness insofar as they acknowledged that the protection of privacy can be an issue for the security industry, but rarely was privacy identified as a significant factor structuring the business activities of the companies we profiled. For the most part, the industry views privacy as a matter for customers or government to define, which industry actors can then 'build in' to security systems as required on a case-by-case basis. This most often was the case for government programs that require the collection of large amounts of personal information. Privacy was rarely seen as an issue for the use of video surveillance in public places, largely because of the position of the courts that there is no expectation of privacy in public space.

Main concerns raised by interviewees in every partner country/threats to privacy

Our report outlines a number of concerns that our interviewees expressed pertaining to privacy protections in the US, three of which are highlighted here. The first has to do with the sectoral approach that the US has taken with respect to the protection of personal information. Unlike many other countries, the US does not have an overarching data protection act. Instead, multiple acts have been brought forth over the years to govern the protection of personal information in specific economic or institutional spheres. A subset of this concern is the lack of an independent office for enforcing these statutes as well as any regulation governing the use of video surveillance in public space. The second has to do with the grants program of the Department of Homeland Security, which some of our interviewees said allowed law enforcement and public safety agencies free reign to develop video surveillance networks without much oversight or input from the public. The third has to do with the pace of technological development and the inability of law and policy to keep up with these developments.

Main reasons for security measures implemented (comparison)

Security measures can be implemented for a wide variety of reasons, and our research did not specifically look at these reasons. But on the whole, September 11th 2001 significantly sharpened the perception of need for enhanced domestic security at all levels and contributed to the growth of a multi-billion dollar annual market in domestic security.

Some solutions for privacy enhancement proposed by main actors

Almost all of our interviewees expressed agreement with the idea that technology can be used to protect privacy. In practice, however, there are few compelling reasons to develop or implement privacy enhancing technologies in ways that are above legally-mandated requirements. Currently, market incentives overwhelming favour the use of technology in ways that diminish rather than enhance privacy. For this reason the idea of technological fix for privacy concerns, while technically feasible in most instances, is not likely to be advanced by the industry in the absence of some compelling reason to do so. As such, until the protection of privacy translates into a commodifiable asset, other grounds for the protection of privacy are needed.

POLAND

In summarizing the Polish part of the report, it may be stated that there is a lack of unequivocal legislation defining principles of the application of CCTV in Poland. Regulations are based on the general protection of personal data and concrete regulations on individual public locations (mass public events, city monitoring, etc.). The situation is similar in the area of biometric technology. Apart from the Act on Passport Documents, there is no unequivocal regulation relating to methods for guaranteeing data protection. The ongoing development of technology should force the legislator to create unambiguous standards and laws effective in this area, as this is of great significance in the securing of the basic rights and liberties of each and every citizen of the Republic of Poland.

Based on the interviews carried out within several representatives of the security institutions, the general conclusions and reflections are the following:

- According to the respondents representing the entities and institutions described in this study, the understanding of privacy is convergent with the narrow understanding of this term. All respondents agree that privacy is confidentiality understood as the security function showing the area where data should not be made available or disclosed to any persons, processes or entities.

- The outcomes of this study show that the notion of privacy awareness is best understood by security service providers and personnel of the security agencies. This results from the specific nature of these services and governing laws and making possible the provision of detective services.

- It is important to pay attention to some system solutions in respect of the security of information designed for the purposes of prevention of any threats concerning unauthorized access, destruction or loss of information data.

- The producers of the security technologies and representatives of the banking sector make endeavors not to infringe human privacy and personal dignity by offering specific technologies and

security systems and to prevent the use of the products for criminal purposes or for the activity contradictory to the rules of community life and ethics.

- Bank employees are aware of the importance and meaning of privacy in this sector of services, and trainings provided to them will contribute to the consolidation of privacy awareness.

- A very important issue is the assuring of proper training for the employees of each respondent in personal data protection. Especially the constant education of the employees dealing with the security problems is a must in order to convince people to the broader implementation of the security technologies and services.

- The employees should be aware of the special requirements while dealing with the privacy issues, which is a very sensitive problem for the society and consumers of the security goods.

- It seems that a slightly weaker sense of privacy awareness is common among the respondents who represent higher education institutions. This results from the fact that educational services provided and research carried out by such institutions are not always oriented towards the privacy policy.

- The respondents representing the entities and institutions described in this study most frequently pointed out that there is a need for the development and use of surveillance technologies. In banking these technologies are used in access control systems. However, the respondents gave some examples of limitations regarding the use of these techniques set forth in regulations on personal data protection.

- Biometric technologies are fully accepted by detectives, however according to their statements they do not give any specific reasons for such use. On the one hand, biometric techniques arrange data and they make it possible to systematize traits typical of an individual and this may facilitate the work of many entities and institutions. On the other hand, this can cause some discomfort to individuals. The respondents confirm that it is necessary to enact some laws regarding biometrics, especially at the European level.

- According to the respondents the CCTV system in different institutions and enterprises is viewed favourably unless it infringes privacy of an individual or personnel. The respondents from the manufacturing company and the detective and security agency give some reasons why it is necessary to install monitoring systems.

- Generally the respondents participating in this study ascertain that almost in every institution and enterprise or company the CCTV system should be installed taking into account the need of supervision of important areas according to the enterprise's interests and the protection of property and control engineering processes, with the simultaneous maintenance of privacy protection criteria for individuals with the exception of rest and refreshment rooms. Employees must be informed in advance about the purpose of introducing the CCTV system and areas of its operations.

- It should be ascertained that data and information security is the high-level goal for employees. They point out that information security management techniques should be developed although more and more often customers demand the guarantee of inviolability of data provided by them or the information concerning the undertakings assigned to them. Thus, privacy and its protection should be an issue of interest to representatives of both supply and demand.

Additional final remarks

The cross country analysis of security and privacy issues clearly indicates vast differences between views on privacy and awareness of problems. Different voices were raised about the degree of legislations and regulations. Some interviewees claimed that it is adequate, a majority pointing out the possibility that the rapid technological developments in the area of CCTV and biometrics were not followed in the same pace by legislation and regulation development. This is particularly the case with the new developments such as audio and video analytics. The potential for privacy protection to be built into systems at the outset was highlighted as a real possibility during the interviews. Some believe that data protection legislation is adequate, just not enforced properly. This was expressed in the analysis following the “performance” perspective on the gap between law and practice.

From the questionnaire one can see that in most countries at the industry level the producers of surveillance technologies delegate the question of privacy to users since technology itself in contrast to its application is privacy neutral. The problem is that despite the fact that new technologies often have the potential to protect privacy, the economic, political and bureaucratic systems all have incentives to use them to undercut privacy and nobody really has an incentive for using them to protect privacy. The public good of privacy is too diffuse and is not well represented, as indicated by one of the American respondents.