PASR

Preparatory Action on the enhancement of the European industrial potential in the field of Security research

Grant Agreement no. 108600
Supporting activity acronym: PRISE

Activity full name:
Privacy enhancing shaping of security research and technology – A participatory approach to develop acceptable and accepted principles for European Security Industries and Policies

Activity type: Supporting Activity

D 5.7 Spanish report - Interview meeting about security technologies and privacy

Start date of Activity: 1 February 2006 Duration: 28 month

Author(s): Vincenzo Pavone, CSIC Unit of Comparative Policy and Politics

Supporting Activity Co-ordinator
Johann Čas,
Institute of Technology Assessment,
Austrian Academy of Sciences
Strohgasse 45, A-1030 Vienna, Austria
jcas@oeaw.ac.at
www.oeaw.ac.at/ita

Partners

Institute of Technology Assessment,
Vienna, Austria
Contact: Johann Čas
jcas@oeaw.ac.at
www.oeaw.ac.at/ita

The Danish Board of Technology,
Copenhagen, Denmark
Contact: Lars Klüver
LK@Tekno.dk
www.tekno.dk

The Norwegian Board of Technology,
Oslo, Norway
Contact: Christine Hafskjold
christine.hafskjold@teknologiradet.no
www.teknologiradet.no

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein,
Kiel, Germany
Contact: Marit Hansen
LD10@datenschutzzentrum.de
www.datenschutzzentrum.de

CONSEJO SUPERIOR
DE INVESTIGACIONES
CIENTÍFICAS
Unidad de Políticas Comparadas

PRISE Project - Spain

Preparatory Action on the enhancement of European industrial potential in the field of security research

REPORT OF THE FINDINGS

Dr. Vincenzo Pavone
CSIC Unit of Comparative Policy and Politics

In collaboration with:

Enriqueta Arteta (OPTA Consultores)

Susana Pablo (CSIC-UPC)

Manuel Pereira Puga

Jesus Ruiz Herrero

Madrid, July 2007

INDEX

C/ Albasanz 26-28, 3ªplanta Módulo D
28037 Madrid, España
Tel.: 91.375.1515
Fax: 91.375.7741
www.iesam.csic.es

I - OBJECTIVE

The general aim of this research was to explore the degree of acceptance that participants in the group interviews have of the new security and privacy technologies under study in the PRISE project. The target population was resident in the Region of Madrid (Spain).

II - METHODOLOGY

The methodology employed in this study, which has been previously elaborated by the PRISE partners, is mainly based on qualitative techniques, such as the interview meeting. The interview meeting is a technique that makes use simultaneously of four focus groups and an individual questionnaire, filled by each of the participants.

III - FIELDWORK REPORT

1 - Recruitment of the participants

The recruitment of the participants to the interview meeting has been realized in the following way:

- Call for participation in Madrid periodicals
- Diffusion of recruitment forms in various areas and neighborhoods of Madrid
- Phone registration of interested persons. We received 104 phone calls of people interested to participate in the group interview.
- Preparation of a recruitment questionnaire.
- People were then asked to answer to the questionnaire in order to find out their gender, age and education.

2 - Selection of participants and constitution of the groups.

- Selection of participants

We finally selected 36 participants in order to match the requirements of the matrix elaborated by the PRISE Project partners.

	18-34 years			35-54 years			+ 55 years		
Man									
Woman									
	L	M	H	L	M	H	L	M	H

Starting from this matrix we constituted 4 groups, divided in two types similar to each other in pairs of two:

C/ Albasanz 26-28, 3ªplanta Módulo D
28037 Madrid, España
Tel.: 91.375.1515
Fax: 91.375.7741
www.iesam.csic.es

Type A (Group 1 and Group 3)

Education	**L**		**M**		**H**	
	Man	**Woman**	**Man**	**Woman**	**Man**	**Woman**
18-34	X			X	X	
35-54		X	X			X
55 y +	X			X	X	

Type B (Group 2 and Group 4)

Education	**L**		**M**		**H**	
	Man	**Woman**	**Man**	**Woman**	**Man**	**Woman**
18-34		X	X			X
35-54	X			X	X	
55 y +		X	X			X

Following this scheme, we made sure that the individuals selected with similar characteristics in each subtype of the matrix would not be repeated in each group. Finally, we also selected 4 individuals as possible substitutes, one each group, so that, in the end, each group had 10 individuals selected.

- Sending out the "Scenario"

  - Phone contact with the individuals selected to find out contact details and address to mail out the "Scenario"
  - Mailing out the letter of invitation and the "Scenario".*
  - Phone confirmation of successful delivery of the "Scenario"

- Confirmation of participation

  - Phone contact with the participants to confirm the eventual participation to the meeting.

- Constitution of the groups

The final composition of the groups was the following:

GROUP 1.

Gender	**Age**	**Education**
Woman	18	Elementary education
Man	18	High School
Woman	32	BA in Journalism
Man	37	BA in English Philology
Woman	42	High School
Man	54	High School
Woman	61	BA in Humanities
Woman	69	Elementary education

* See the Annex

C/ Albasanz 26-28, 3ªplanta Módulo D
28037 Madrid, España
Tel.: 91.375.1515
Fax: 91.375.7741
www.iesam.csic.es

GROUP 2

Gender	**Age**	**Education**
Man	18	Elementary education
Man	24	BA in Telecommunication Engineering
Woman	27	Professional education (cooking)
Woman	36	BA in Law
Man	42	Professional education (Social assistance)
Woman	46	Elementary education
Woman	49	Elementary education
Woman	55	Professional education, (nursery)
Man	64	BA in Law

GRUPO 3

Gender	**Age**	**Education**
Woman	18	Elementary education
Man	24	High School
Woman	30	BA (Images and sound technician)
Man	40	Elementary school
Woman	44	High School
Man	51	BA in business
Man	56	High School
Woman	58	BA in Art history
Woman	60	Elementary School

GROUP 4

Gender	**Age**	**Education**
Man	19	Elementary school
Woman	19	High School
Man	44	High School
Woman	46	BA in Economics
Woman	47	Elementary School
Woman	55	High School
Man	61	Elementary school

C/ Albasanz 26-28, 3ªplanta Módulo D
28037 Madrid, España
Tel.: 91.375.1515
Fax: 91.375.7741
www.iesam.csic.es

3 - Fieldwork dates

The fieldwork was conducted between the 18th of May and the 7th of June 2007.

- The recruitment began on the 18th of May and was completed on the 29Th of May 2007.

- The focus groups of the interview meeting were conducted on the 6th of June 2007, one at 5 pm and the other one at 7 pm. The other two groups were held on the 7th of June 2007, again at 5 pm and 7 pm.

4 - Meeting Program

The four focus groups were realized according to the following schedule. First, there was the introduction of an expert on the new technologies of security and privacy (Mr. Emilio Aced Félez, from the Data Protection Agency of Madrid), followed by general questions from the floor (30 min.). Second, the participants were asked to fill in the questionnaire, individually (30 min.). Finally, the discussion group took place, for about one hour each group.

C/ Albasanz 26-28, 3ªplanta Módulo D
28037 Madrid, España
Tel.: 91.375.1515
Fax: 91.375.7741
www.iesam.csic.es

IV - Report of the findings

Summary

The current advances of technology are perceived in contemporary Spain as an increasingly important element of daily life; and a clear indicator of such attitude is given by the strong positive values usually associated with the new technologies, generally described as a crucial element in the advance of progress and social welfare. Within this positive framework, the technologies related to security and privacy enjoy a significant level of support, because they are expected to improve the level of personal protection as well as the protection of goods and properties. In general, however, the lower is the perceived negative impact of these technologies on personal privacy the higher would the level of support be.

In spite of such a positive attitude, however, the participants have occasionally shown perplexity towards a few situations usually associated with the implementation of some of these technologies, which were often perceived as more plausible in the context of a science-fiction novel – with all the dehumanizing and impersonal implications – than in a context of ordinary daily life. On the one hand, the increasing complexity of these technologies raised a sense of anxiety, generally connected with the risk of abuse that such a complexity may carry. On the other hand, the participants acknowledged that, with a proper control exercised by competent authorities, these technologies may indeed improve the level of security in given areas of people's life. In this respect, continuous information and public transparency about the ends and the reasons behind the choice of any given technology would prove crucial to ensure the success of a process of legitimization of these technologies in the eyes of the citizens. More specifically, the participants have expressed deep concern that these technologies may be used for commercial purposes and/or for political control. In addition, it is interesting to point out that those participants who were more familiar with travels and communication technologies demonstrated the highest level of awareness of the implications and, consequently, showed a more critical attitude, especially with respect to the effectiveness and the real benefit of these technologies. From the groups' discourses emerged somehow a dual or ambivalent attitude regarding these technologies, similar to what has been reported for general science and technology issues in Spain

Although in the last years the public debate has been focusing mainly on the issue of terrorism, the latter is not the only issue that has attracted the attention of the participants. In fact, during the debates it emerged clearly a growing concern for other types of risk, such as ordinary criminality and, especially, gender violence. It is the sum of all these concerns that, in the end, justifies the increasing appeal to the new security technologies; actually some of the participants suggested improving and speeding up the research process in order to develop newer and better technologies.

C/ Albasanz 26-28, 3ªplanta Módulo D
28037 Madrid, España
Tel.: 91.375.1515
Fax: 91.375.7741
www.iesam.csic.es

CHAPTER 1

General attitudes

Privacy and Security

The advancement of technology plays an important role in contemporary Spanish society, not only for its economic impact but also for its social implications and repercussions. As demonstrated by several enquiries conducted by the FECYT (1996, 2001, 2006) and by the Eurobarometer (2006) on the public perception of science and technology, the Spanish society seems to hold a benevolent and supportive attitude towards the development and application of new technologies. This study actually confirms how this attitude would also include security and privacy technologies, which seem to be welcomed, at least in principle, because they are expected to improve citizens' security and the general protection of properties and goods. The level of support towards new security technologies, however, varies along with the perceived negative impact on citizen's privacy, in a sense that is higher when the perceived impact on privacy is lower.

The positive attitude towards the new technologies has been also extended to the general research process behind their development, which has been especially approved because it constitutes a mechanism that allows reflection about unexpected or previously unconceivable situations. In this respect, the very process of technology assessment hereby carried out has been considered a good example of the modality of participatory processes that should always be carried out in relation to the development and implementation of new security technologies. In general, the participants were very positive about all the forms of participation that facilitate the assessment of all pros and contras of new security measures, especially with regards to what is to lose and what is to gain.

The majority of the participants, in principle, accepted the implementation of new security technologies, although usually showing some concern for the risk of privacy infringement. In fact, other participants were much more reluctant. On the one hand, some participants clearly stated that if we have nothing to hide there is no problem in being monitored. On the other hand, other participants expressed exactly the opposite view, i.e. if we have nothing to hide there is no reason to be monitored. These sentences reveal this cleavage clearly:

> *"These things are necessary, they help us to move on with transparency, if you have nothing to hide, if I forget my purse over there and I have nothing to hide, I think it is necessary..."*
> *"If I have nothing to hide, why should they monitor me?"*

Therefore, the possibility of privacy infringement gave raise to two different reactions among the participants. In the first case, the participants felt that the privacy margins are increasingly smaller, and suggested that the new security measures are going to be used for perverse and illegitimate purposes. In this case, they usually associated this scenario with the worst situations suggested by the science-fiction literature and novels. In the opinion of these

C/ Albasanz 26-28, 3ªplanta Módulo D
28037 Madrid, España
Tel.: 91.375.1515
Fax: 91.375.7741
www.iesam.csic.es

participants, the increasing implementation of new security technologies is not justified by real dangers but by a growing diffusion of fear among the citizens that is purposively encouraged in order to set up a more effective form of manipulation. In general, this attitude was more common among people with low education, as it was confirmed by the data resulting from the questionnaire.

Within this framework, these technologies were not expected to really enhance the feeling of security but, in fact, to produce the opposite result, i.e. an increase of the sense of fear and vulnerability. These technologies, thus, were perceived as pervasive, invasive and, above all, ineffective in relation to their official purposes; on the contrary they were perceived as very effective in relation to other unofficial purposes, far from benefiting the population. In this view, as they say, we are all vulnerable in a way or another. Some participants even expressed their fear of living under a 'police state' in which we all monitor each other. The general feeling proceeding from these types of comments was one of anxiety, fear and vulnerability. This attitude was actually addressed by the questions 20 and 21 of the questionnaire, which revealed how more than 70 per cent of the participants were worried that the information gathered maybe manipulated by the State and/or used by the criminals.

In the second case, the participants generally accepted the need of introducing new security measures to contrast what they perceive as an increasing and real danger, proceeding from different sources: terrorism, organized crime as well as common criminality. This group of people, in the name of security, would justify all the possible inconveniences that may derive from the implementation of these technologies. In general, they did not feel that their privacy was affected in a serious way because they believe they have nothing to hide and because they believe that there is nobody really interested in monitoring ordinary people's life. Even if this was the case, they suggested that a massive monitoring would not be viable on practical grounds, anyway.

As a consequence, the concern about privacy's infringement is more evident among those who believe that the use of these technologies is vulnerable to be manipulated and diverted to other purposes. In contrast, the people who believe that this possibility is not going to affect them directly because they 'have nothing to hide' show a much lower level of concern. However, both types of participants came to an agreement in relation to some specific issues. First, they all agreed that 1) individual privacy should never be violated unless there is a specific and probable criminal act to investigate or prevent and that 2) being monitored is always unpleasant, even when there is no criminal intention. The data gathered from questions 19 and 20 yielded very similar results (94 per cent agree with the statement). In the same way, the participants shared similar opinions when the issue at stake was a) the risk of errors of the system, such as false positive and false negative outcomes, b) the possibility that the very people that the system is supposed to monitor may succeed in fooling it c) the risk of perverse uses of the technologies and d) the risk associated with various forms of ineffectiveness.

Moreover, the debate about the need of more security focused also on the concept of 'fear', giving raise to two main positions. On the one hand, some participants suggested the need to improve security, generally proceeding from a sense of fear before dangers that were perceived as real. On the other hand, other participants suggested that this sense of fear is exaggerated and

C/ Albasanz 26-28, 3ªplanta Módulo D
28037 Madrid, España
Tel.: 91.375.1515
Fax: 91.375.7741
www.iesam.csic.es

purposively induced among the citizens by a variety of 'interests' that would benefit from a higher level of fear among the population. It is this exaggerated and, in a way, artificial sense of fear that is needed to ensure the acceptability of new security measures and technologies. To many, this concept of 'artificial fear' was the key to an ongoing process based on a growing disinformation that was described as aiming at the manipulation of reality. By the same token, some individuals argued that social reality was ultimately inaccessible and that, therefore, it was very difficult for ordinary citizens to discern what was real. As they argued, this situation made them more vulnerable to being manipulated in many different ways; within this framework, the media are meant to play a crucial role. Either way, the proponents of both positions described the 11th of September as a triggering factor behind the evolution of this process.

Finally, the debate on the trade-off between privacy and security frequently focused on the issue of individual choice. In other words, several participants suggested the possibility of leaving the choice of using some of the new technologies to single individuals, especially with regards to the e-Call. This gave raise to a contradiction, which was acknowledged by the participants themselves, among individual choice and the overall effectiveness possibly deriving from the general introduction of the new technologies.

The effectiveness of security technology

When the participants did consider the actual application of the new security technologies to real cases, e.g. access control to a football stadium, the large majority came to the conclusion that these technologies may well reduce the risks but will never be able to eliminate them. Some participants bitterly concluded that, no matter how powerful these technologies are, they will not prove sufficient against criminal sabotage. Occasionally, various participants have expressed doubts about a) the real capability of these new systems to prevent attacks, b) the capability of the experts of identifying in advance the instruments with which the attacks will be perpetrated and c) the real frequency with which wrong interpretations of people's behavior and identity mismatching may occur.

As a result, the issue of the real **effectiveness** of the new security technology was debated at length. Apart from a general assessment in terms of privacy's infringement, the participants often questioned the validity of these technologies in terms of real effectiveness. Some participants weren't convinced that, considering their doubts about real effectiveness, the benefit deriving from these new technologies would actually compensate the loss in terms of privacy. Although expressed with various degrees of determination, almost all the participants shared doubts about the real effectiveness of the new technologies; in a way, such an attitude of distrust was so common that it often operated as a mediating factor among otherwise different positions.

Going into more details, the participants suggested that the best outcome these technologies should be able to deliver is the real **capability of preventing** crimes. Consequently, they have been assessing the effectiveness of the different technologies in terms of their ability to prevent, giving more support to those technologies that they perceived more effective in these terms. In any event, the participants expressed serious doubts that the technologies

C/ Albasanz 26-28, 3ªplanta Módulo D
28037 Madrid, España
Tel.: 91.375.1515
Fax: 91.375.7741
www.iesam.csic.es

could really exercise a strong preventive power in several of the scenarios proposed, although they acknowledged some dissuasive power.

In their opinion, the limits of these technologies are related to several factors. First, the new technologies will never be able to cover it all: "there will always be holes". I quote:

> "*I believe that catching a plane does not carry the same risk of shopping in a shopping mall, that is, they can always put a bomb in a plane as well as in any other place, and you can't monitor all of them*"

Second, the criminals are capable of fooling the security systems:

> *"Well, I believe that no matter how many cameras, how much security you have, I believe that the terrorists are actually kind with us ... they can always fool all these technologies".*

Third, the real effectiveness of these technologies depends on the capability of the individuals actually dealing with the acquired information. In this respect, the participants used 'capability' to express both the technical/professional capability as well as the moral/ethical one. As to the technical capability:

> *"I don't know, how many of these CCTV cameras are attended by security guards, which is a job like many others, I mean it does not entail special requirements. I mean, if you spend your time monitoring people and you have to decide whether any person is showing a 'strange' behavior, you really need to have some knowledge about people's attitudes.*

As to the moral/ ethical one:

> *"I believe that they should be careful about who is going to have access to our data, to all our data, to all our private things".*

Indeed**,** one of the main questions debated in relation to the issue of privacy was the problem raised by the **interpretation** of the data. It was not so much the worry associated with being exposed to people they did not know, but rather the fear of being 'interpreted', judged on the basis of the gathered information. This very issue gave raise to several doubts. First, it raised doubts about the capability of security officers of interpreting correctly the information received. Second, it raised concerns about the pervasiveness of clichés and stereotypes, that is to say the need to standardize and homogenize people and behaviors in order to match the interpretative scheme of those who are in charge of the security systems.

In sum, these were the main concerns expressed by the participants across the four groups:

a) Who is going to be in charge of treating and interpreting the data;
b) Who is going to control the 'controllers' and how;
c) Whether such control will, in fact, respect established values and rules;
d) Whether this surplus of information will eventually benefit specific interested actors such a multinational companies;
e) Whether the citizens will actually be involved in monitoring all the phases of the implementation of these technologies;
f) Whether some of these technologies will eventually result too invasive;
g) Whether the use made of these technologies will be efficient.

Conclusion: not everything goes

C/ Albasanz 26-28, 3ªplanta Módulo D
28037 Madrid, España
Tel.: 91.375.1515
Fax: 91.375.7741
www.iesam.csic.es

In all the groups, the assessment of the positive aspects of these technologies followed an individualized approach. In other words, the technologies were positively assessed as long as they were perceived as directly providing personal benefits. For instance, the e-Call was positively assessed because it is a technology whose benefits could be easily evaluated in personal terms. Nonetheless, it is interesting to point out that in general the participants had troubles in specifically assessing positive and negative aspects of each technology. Although they had read the documents received and listened to the expert's introduction very carefully, the general conclusion produced by the groups is that these are both largely unknown and very difficult issues. Actually, it could be detected a general reluctance to go into details about the opinions expressed towards each of the scenarios suggested. As a result, the participants tended to form their opinion by reasoning more about those technologies they perceived as more known and familiar. Biometrics, the scanner and the technologies applied in defense of privacy were perceived as distant and unfamiliar, whilst cameras, data retention and the e-call were perceived as close and familiar.

In general, there was a remarkable consensus on the need of additional security related to some aspects of ordinary life, such as circulation in the streets, in commercial areas and shopping malls, and the protection of on-line data. However, there was also a clear tendency to judge negatively those technologies that can effectively invade their private and intimate life, such as the cameras. In this respect, the participants often used images and metaphors from family life in order to state clearly that the violation of this sphere is not acceptable, not even in the name of security.

In the balance between security and privacy, the groups generally reached a consensus on the adoption of these new technologies only in relation to specific cases and issues, generally related to terrorism. This acceptance however was granted only upon the condition that these technologies would be used for specific crimes, in specific contexts, in proportion to the gravity of the crimes, and for prevention purposes. In addition, all the participants agreed that these technologies should always be employed under specific guarantees, given that it is necessary to regulate in details both their development and their implementation, on a case by case basis. An unregulated implementation of these technologies would produce a loss of confidence in the framework of law and rights of the democratic states. In other words, if concern for security turns into an obsession, this would inevitably cause the end of the achievements so far obtained by western civil society.

C/ Albasanz 26-28, 3ªplanta Módulo D
28037 Madrid, España
Tel.: 91.375.1515
Fax: 91.375.7741
www.iesam.csic.es

CHAPTER 2

Security and Privacy technologies

When asked about the technologies presented in the Scenario they had received at home, the large majority of the participants tended to focus on cameras, data retentions and location technologies, like the e-Call, which are the technologies they considered more familiar. In effect, nearly all the participants have seen a CCTV camera in various places, knew the GPS system and were aware that some of their data are usually stored whenever they get access to given services. Whenever they mentioned the other technologies, like biometrics, the scanner and eavesdropping, it was clear that they felt somewhat disoriented, occasionally wondering whether the technologies at stake were indeed real or not. In contrast, the technologies related to privacy enhancement did not capture the attention of the participants at all. In fact, these technologies were never spontaneously mentioned, and even when the participants were explicitly asked, they expressed skepticism about their real efficacy.

With respect to **biometrics,** the participants showed a general ambivalence, sometimes characterized by the tendency to consider this technology as closer to science fiction movies:

"To me, this iris, this iris recognition left me... I don't know, I think I saw it in a movie, where the put the eye forward and the door opened".

In general, these technologies have been associated to airports, state borders and places where there are similar conditions of danger and crowd, such as train stations and stadiums. These results were confirmed by the quantitative data, although it is interesting to point out that people that travel rarely insist more on biometrics at state borders and that housewives are more inclined to put biometrics in football stadiums. It is also puzzling to realize that those who travel more frequently with public transports are also those who are more critical with biometrics in airports and in football stadiums.

Among the positive aspects mentioned, many participants remarked the opportunity provided by this technology of saving time and queues, by reducing waiting times (38 per cent in the questionnaire data). They also mentioned the potential contribution of biometrics in preventing terrorist attacks. I quote:

"I'd say, for when you travel, so that you do not lose time"

"If it is to avoid terrorism and so on, then I accept it"

However, many participants also pointed out negative aspects, such as the risk of having the biometric identity stolen, which was considered a very serious problem (nearly 50 per cent in the questionnaire) but also the risk that this information could also be used for commercial purposes.

"Actually, I am afraid that, as they mentioned before, we may get our identity stolen".

"Private companies, I think they can be interested in biometrics in order to know consumption habits".

C/ Albasanz 26-28, 3ªplanta Módulo D
28037 Madrid, España
Tel.: 91.375.1515
Fax: 91.375.7741
www.iesam.csic.es

As a general remark, it is interesting to note that the degree of biometrics 'aggressiveness' is not measured against an objective level of accuracy of the data gathered but against a subjective perception of what is more intimate, and therefore more vulnerable to the technology gaze.. In other words, the less one's own identity is affected the more biometrics controls will be accepted. Even according to the quantitative data, the most acceptable forms of biometrics are the fingerprints and the iris scan. I quote:

> *"According to this book, it seems that the iris recognition is not so aggressive, but I do not know and I cannot really express an opinion, but between recognizing my face and reading my iris... well, I almost prefer that they read my iris".*

In a way, this opinion can be extended to all security technologies, which will enjoy more support the less they are perceived to affect personal identity. From a technical point of view, maybe the iris recognition offers more personal and biological information but it is perceived as less personal, and raised less resistance. Finally, some participants have expressed concerns about the health risk that these technologies may carry, such as the iris recognition for the health of the eyes.

With respect to **cameras**, the situation was different because the majority of the participants were familiar with cameras in the city, in the streets as well as in the internal space of various buildings. Actually, this technology has been spontaneously associated to places where people tend to create crowd, or where there is a higher level of danger or of conflict, like airports, metro stops, football stadiums, concert halls and even shopping malls; again the quantitative data are consistent with this result. In some cases, it has also been associated to ordinary places, like the entrance door of the buildings. It is interesting to point out that the idea of placing CCTV cameras in the airports was very popular among very young participants and quite controversial for people between 25 and 30.

Among the positive aspects mentioned, priority was given to the capability of preventing crimes, the contribution to identify and catch a criminal and the dissuasive power. More specifically, according to the quantitative data, the CCTV cameras should be used only where several crimes have been already committed and if there is no risk of being exchanged for someone else. In fact, some participants expressed doubts about the effectiveness of cameras in the prevention of crimes. I quote:

> *"In the case of the metro, you know they are recording you, you know as soon as you enter that they are going to record you, and this does not really protect you because people get assaulted in the metro anyway"*

Among other concerns, many participants expressed fear of falling victim of a false positive case, that is, when the system incorrectly identifies someone.

> *"I am really worried about mistakes, that is, a situation in which they charge you with a crime just because there is a camera saying that it was you, and maybe you really look like another one, but it wasn't you".*

The issue of false positives was also connected to the issue of 'who' works behind the cameras, especially about their formation, because they may interpret what they see incorrectly. On top of that, a few participants claimed that an excessive proliferation of cameras would inevitably reduce their dissuasive power, without reducing their invasiveness. In this respect, several

C/ Albasanz 26-28, 3ªplanta Módulo D
28037 Madrid, España
Tel.: 91.375.1515
Fax: 91.375.7741
www.iesam.csic.es

participants expressed concern that a massive use of camera might convert in policemen those who should never do that, like the neighbors. However, if we look at the quantitative data, 40 per cent considers the number of cameras already existing are appropriate, whilst 20 per cent wants more (especially people with children) and another 20 per cent wants less.

> *"Put cameras in the entrance door of the buildings? I'll tell you, the community of neighbors should never adopt the attitude of the police, that ism they should not act as policemen ... that we impose to ourselves a regime of control, I think, it is a little absurd."*

The **scanner** provoked reactions very similar to those associated with biometrics. However, the use of traditional scanners like those of metal objects and x-ray machines in airports has been presented as something normal, as part of a routine. In contrast, the scanner of the new generation, known as the *naked machine*, was perceived as substantially new and gave raise to uncertainty and distrust as well as curiosity and interest. Although willing to acknowledge its positive aspects, like better security, precision, and speed, all the people agreed that this technology should only be allowed to visualize a dummy without visible sex characteristics; otherwise this machine was perceived as potentially violating privacy in an intolerable way. The reasons behind this precise statement were various, ranging from the fear of being exposed to the worries about how these images would be used by those working behind the cameras.

> *"No, for instance, if you or I... I am right now in a phase of my life in which... I mean, I am ashamed of my body, no?"*

These general opinions are consistent with the quantitative data, which reveal how the naked machine with the mannequin option got 18 per cent of approval, whilst its pure version only 11 per cent. Again, this opinion confirms the general impression that there exists a private and intimate sphere of life, a special personal space, which should be protected by an inviolable right, which should constitute a basic principle in the negotiation on where and when it should be allowed to install new security systems.

Location technologies, like the el E-Call, are the technologies that have enjoyed stronger support, especially in relation to the possibility of localizing vehicles and children and elderly people. I quote:

> *"The most positive (technology) is the e-Call, the one of the car"*
>
> *"The elderly people, if they could be located somehow, this would be very interesting. The children, if they could also be located..."*

In general, the participants have positively welcomed these technologies because they have been perceived as very useful to locate and arrest criminals, to recuperate stolen objects and to facilitate emergency rescue in road accidents. These findings are also consistent with the results delivered by the questionnaire.

In any event, this technology has been framed as an 'optional' one, i.e. a technology whose use and application should be generally left to individual choice. It is the individual that should decide whether to activate it or not, at any point in time (more than 70 per cent in the questionnaire data). Yet, in some cases, this 'optionality' has been questioned as potentially affecting the final effectiveness of the technology. Actually, the very idea of being located at all

C/ Albasanz 26-28, 3ªplanta Módulo D
28037 Madrid, España
Tel.: 91.375.1515
Fax: 91.375.7741
www.iesam.csic.es

times was considered and, in the end, assessed in very negative terms with respect to privacy protection (more than 80 per cent in the questionnaire data).

> *"I'd say yes, if it is activated in the moment of a car accident, but the idea that they can trace you at all times this would be too invasive".*

Data Retention technologies have triggered the debate that most revealed how strongly is the acceptance of these technologies associated to the purposes for which they are used. On the one hand, all the participants would accept an improvement of data retention in case the latter would be used by the police in relation to the data belonging to criminals, or in relation to the creation of a database to prevent terrorist attacks and increase security. On the other hand, the very idea that this data could be used for commercial purposes provoked a strong reaction, which revealed a high sensitiveness towards this specific type of privacy infringement. In the questionnaire, the use of data retention technologies for commercial purposes got no approval at all.

> *"These technologies should not be used for purposes different from those that are officially established, that is the security of all the citizens"*

In addition, it is interesting to point out that, during the discussion, the focus moved to the possible application of this technology to medical purposes, eventually suggesting the creation of a medical database of all the citizens.

> *"I think that the database deriving from data retention could be very useful, as we mentioned earlier on, for the doctors ... in a sense…so that you can go to any hospital and they already know your personal medical record and so on".*

Even this technology, however, did not fail to provoke doubts about its effectiveness, especially with regards to the prevention of terrorist attacks.

> "*For instance, this data retention* [...] *the guy who crashed with plane (reference to the 9/11)... what was contained in his database? That he had studied as an aviator? And so what? This is not dangerous, they can get around it, and this is why I think this technology doesn't lead anywhere."*

In sum, this technology has been generally rejected as a general and unconstrained practice, although it can be acceptable always after the permission of the judicial system, when the police already possesses a significant variety of reliable information. In other words, data retention technologies were considered acceptable to gather final and decisive evidences but not during the very first stages of police investigations. It was remarkable to notice that, contrary to our expectations, people living in a city largely affected by terrorist attacks did not appear especially sensitive, or at least not to the point of being willing to accept unrestrained police actions in exchange for an improvement in security levels.

Eavesdropping technologies also belong to the category of technologies associated with science-fiction or movies, and, in the debate, they were often linked to a worrying scenario of political monitoring:

> *"...Or, for example, when your write an email. I, for instance, work for an NGO and we often talk about things that are occurring in various countries and, most of the times, we do not know to what extent we are not monitored. Most of the times, you have to be careful about your words and things like these".*

C/ Albasanz 26-28, 3ªplanta Módulo D
28037 Madrid, España
Tel.: 91.375.1515
Fax: 91.375.7741
www.iesam.csic.es

Although the participants acknowledged that this very type of technology may play a crucial role in the fight against terrorism (85 per cent in the questionnaire data), the risk of privacy infringement was considered very high (again 85 per cent of the questionnaire data). Therefore, the participants reached a consensus on the need of placing the use of these technologies under strict judicial authorization.

Last but not least, **privacy enhancing technologies** have been generally associated to the parallel advancement of security technologies but never attracted the attention of the participants, who clearly expressed serious doubts about both effectiveness and resistance to criminal attacks. I quote:

"If you can encrypt the receiver of your messages, anyone can do or undo that".

In sum, as a general attitude, the participants acknowledged that, due to terrorism at a global scale and to the increase of general crime, it is necessary to use new security technologies, even if this change would imply a reduction in terms of privacy right and protection of intimacy. Yet, they are determined in making sure that this reduction should only occur in exchange for a real security enhancement. Considering all the opinions expressed in the four groups, it is possible to make a brief summary of all the problematic issues potentially provoked by the eventual application of these technologies.

- The use of these technologies for purposes other than security.
- The difficulty of assessing when a behavior or an attitude of the citizens may be defined as suspicious. They believe the probability of making mistakes is very high.
- There is special concern about the profile of those people in charge of monitoring the citizens. Someone suggested that the State should 'control the controllers'.
- There is fear that the massive use of these technologies may result in a violation of basic rights.
- Privacy reduction can only be justified if these new security technologies prove actually reliable.
- Security technologies are expensive; some of the participants fear that the diffusion of them would have repercussions in the price of a variety of goods, such as public transports.
- Are they safe from the health point of view? Some participants objected that a massive use of scanner and iris reader may carry health risks for human body.

C/ Albasanz 26-28, 3ªplanta Módulo D
28037 Madrid, España
Tel.: 91.375.1515
Fax: 91.375.7741
www.iesam.csic.es

CHAPTER 3

Dilemmas

As previously mentioned, the majority of participants supported the idea of increasing security measure through the adoption of new technologies, but only in specific cases and places, and in any event only within the public sphere. The infringement of privacy in the private and intimate sphere, in contrast, has been consistently described as intolerable. With regards to the latter sphere, the use of invasive technologies can only be accepted in extreme cases, where urgency, gravity are of the highest level and there is no alternative. The use of technologies, in this case, must be justified by serious and unambiguous evidences.

> *"This is it, it is a violation of your privacy but if it truly is for your security you can't really complain"*

In the debate, the participants went further and even specified in which cases they would accept the violation of their privacy. First of all, they mentioned gender violence and sexual harassment. In case these technologies may be effective in preventive violence against women, they can be accepted.

> *"Violence against women, in this sense we ought to put much more effort in terms of security"*

Second, they mentioned ordinary crime and petty criminality, like street violence. In order to prevent crimes like theft, rape, murder, and pedophilia, the use of new technologies was welcome

> *"The type of criminals that keep committing the same crime, such as rape and pedophilia... these people should be monitored much more intensively"*

Third, as it easy to expect, these technologies were also welcome in the fight against terrorism. The participants were willing to lose part of their privacy in order to gain more in security in public places as well as in all the places where people form crowd, like football stadiums, concert halls, train and bus stations, airports and shopping malls.

> *"I believe these measures are appropriate for international crime and terrorism, this is clear... I mean that the citizen should know that these measures may occasionally be annoying, that there are people who cannot stand them, cannot stand being controlled in the airport, and so on, but it is for their benefit. If there was no terrorism, all of that would not be necessary".*

Finally, the participants suggested a further example in which these technologies would be useful, i.e. the monitoring of elderly people, children and people that suffers from serious handicaps. These examples, somewhat unexpected, came out spontaneously in the course of the groups.

> *"It could also be positive for the old people who live alone at home, positive because they are looked after and will not die alone"*

In all groups, several participants expressed some concern that the effort in increasing security measures would be concentrated only against terrorism and

C/ Albasanz 26-28, 3ªplanta Módulo D
28037 Madrid, España
Tel.: 91.375.1515
Fax: 91.375.7741
www.iesam.csic.es

only in places considered as sensitive targets, leaving the citizens unprotected and vulnerable in other places and in relation to other types of crimes. In this respect, they fear that there is a new "elite" security that is emerging and considers terrorism as the main danger, as opposed to the concept of security normally shared by ordinary people, which focuses more on other types of danger and crimes connected to daily life. The latter concept places less emphasis on the threat of terrorism because it acknowledges not only its changing nature but also the ability and creativity of the terrorists in elaborating new strategies of attack and violence.

Finally, the impact of new security technologies has been assessed also in terms of their potential to generate social discrimination and/or stratification.

> *"No, I believe that sometimes there is a risk of confusion... I know what happened to me when I went to Miami, I had some problems, especially after the 11th of September... they stop me all the times to ask for my documents, to ask whether I really was Spanish and put me in the cabin to check my luggage. Why was that so? Because I look like an Arab or a Mexican... you can feel badly when these things happen... I mean just because of your physical appearance, they affect your privacy and there is no respect for the people and this doesn't really prevent a massacre"*

C/ Albasanz 26-28, 3ªplanta Módulo D
28037 Madrid, España
Tel.: 91.375.1515
Fax: 91.375.7741
www.iesam.csic.es

CHAPTER 4

Democratic Issues

Although the participants have expressed a strong interest in a more participatory process of development and implementation of the new technology in the questionnaire, during the discussion they seemed to assign more importance to transparency of information and clarity and effectiveness of general rules than to direct participation. In other words, in their ideal priority list, the introduction of new security technologies should be carried out 1) with absolute transparency 2) with the highest level of information possible 3) in a clear framework of rules, procedure, controls and sanctions 4) under the control of the State and the judicial authority and 5) with a wide participation of various social actors. Although this priority list was common to almost all participants, the latter show a high degree of uncertainty and hesitation when trying to identify who was expected to develop and introduce and who was later supposed to manage and control their ordinary utilization.

In the specific case of public participation, the question on who was expected to participate gave raise to a debate characterized by the emergence of two positions. Some participants addressed the question in a positive way, trying to identify who was supposed to participate, whilst other participants preferred to focus on who was *not* supposed to participate. Whilst there was general agreement on the crucial importance of involving experts, consumer organizations and human rights associations, the debate was far more fragmented when addressing the participation of ordinary citizens and of the politicians.

Arguing that the lay public should indeed participate, some participants specified that only the participation of ordinary citizens will ensure that their interests would be respected and their concerns taken into account. At the end of day, as they say, it is the citizens who have to live with these technologies on a daily basis. The forms of participation most frequently suggested were the referendum or the realization of *ad hoc* surveys.

> *"Because, if things go wrong these are the people who are going to suffer from their consequences, both negative and positive ones".*

In contrast, the participants who expressed skepticism the participation of ordinary citizens argued that it would be impossible for them to reach a viable consensus.

> *"*(...) *Because I believe that the ordinary citizen... that we would never reach a consensus on these measures, never".*

In addition, they also argued that the lay public is not well informed or prepared to effectively participate in the development and implementation process.

> "*I believe that these should be highly qualified people, or maybe the city council, or those who will actually be responsible for their operation in the city or in the specific place where these technologies are going to be used... because I believe that the citizen will never be (qualified)".*

C/ Albasanz 26-28, 3ªplanta Módulo D
28037 Madrid, España
Tel.: 91.375.1515
Fax: 91.375.7741
www.iesam.csic.es

At the same time, there were different opinions about the participation of state representatives, and more specifically of politicians. Some participants argued that it is the State that has to guarantee the protection of privacy and the correct implementation of these technologies and therefore its participation is absolutely necessary. I quote

> *"I believe that they should accept this, not only the States but also the regions and the European Union, but these (technologies) should be regulated with very strict directives (...)"*

Yet, other participants felt very negative about this proposal and voiced a deep skepticism about the real value and capability of their political elite. I quote:

> *"Maybe it is better to keep the politicians out, maybe they should not express their opinion because they may give a very personal opinion, it would be better to have others who might be able to see our interest in a more objective way."*

In any event, the participants had a very clear (and shared) opinion about who should never be involved in the participatory process: banks and multinational corporations. In general, all the participants shared a very negative opinion of these organizations for they were perceived as permanently seeking their own interests without ever taking into account the social interest at large.

> *"Banks are not monitored, telephone companies are not monitored. Only terrorists are monitored, but there are other forms of terrorism, like the one operated by banks charging far more than they should, that are not monitored"*

By the same token, the large majority of participants also agreed on the absolute necessity of introducing clear regulative and participative frameworks, in which not only the State and the lay public, but also the judicial system is expected to play a significant role. In fact, the judges are expected to have the final word on the actual implementation and correct utilization of these technologies.

> *"When there is need to violate the privacy, this should be always authorized by a judge, who has to decide the methods as well as the appropriate time and space constrains"*

Conclusions and proposals

In sum, the participants, with different levels of support, seemed to accept the need to introduce new security measures, even if these technologies may seriously affect their own privacy. Yet, their acceptance does not encompass a-critically all the technologies and does not extend to all circumstances. Consistently with the results proceedings from the questionnaire, the participants made clear that the introduction of new security technologies should be a) gradual and transparent and b) occur always in a context of clear rules and widespread information. In addition, the introduction of new security technologies c) should be focused on specific cases and places d) should be proportionate to the danger and the situation and, finally, e) should affect the private sphere of intimate life as little as possible. In one case, a participant made this point explicitly, suggesting that there is no point in introducing CCTV cameras when it would be sufficient to have more light in the streets. In fact, in several occasions, the participants have expressed their need of feeling safer

C/ Albasanz 26-28, 3ªplanta Módulo D
28037 Madrid, España
Tel.: 91.375.1515
Fax: 91.375.7741
www.iesam.csic.es

but they also specified that it was not a question of 'more' security but of 'better' security.

Although accepting that the use of new technologies to improve their security is important as well as necessary, the participants clearly specified that they are not willing to accept the use of these technologies for any other purpose, especially commercial and political ones. They were aware that 'fear' is a very powerful and rentable feeling in both economic and political terms; therefore they vividly expressed their concern of falling victims of abuses, occasionally speaking of an authoritarian slippery slope.

Moreover, they also explicitly argued that errors and mistakes are very likely to occur, in security technologies as well as in any type of technologies. In fact, they claimed that errors may spring not only from the limits of the technologies but also from the limits of the people who operate with these technologies. As a consequence, the participants claimed the necessity of clear rules and reliable mechanisms of sanction in case of human errors. As we have seen, the professional and moral profile of the operators of these technologies has actually been a very important issue throughout the debate

Finally, there was a proposal that was generally shared by all the participants, though again with different opinions on its general applicability. This proposal was based on the idea that each citizen, whenever possible, should autonomously decide when, where and to what extent make use of these new security and privacy technologies. The idea of having tailor-made technologies was considered as the ideal solution to strike a viable balance between improving security and respecting individual privacy.

-"Ehm, I believe this is the separation of privacy, that whenever you want, if you surf the net, and you enter a database and they offer you a little gift or so, you may choose whether to enter your data or not"

C/ Albasanz 26-28, 3ªplanta Módulo D
28037 Madrid, España
Tel.: 91.375.1515
Fax: 91.375.7741
www.iesam.csic.es

CHAPTER 5

Impact of the event on the opinion of the participants

The general discussion normally came to end with a question on how the event and the info presented to them, in its various steps from the scenario to the final focus group, has influenced the opinion of the participants. A few participants affirmed that they kept the very same opinion with which they had come, or that they were not particularly impressed. I quote:

> *"I keep thinking the same as before"*
>
> *"I believe this, I believe that is going to happen, and is not far away. This is why I was not particularly impressed"*

Some other participants affirmed that the information delivered by the event helped them to formulate a more positive opinion, because they felt safer and more protected as well as more prepared for future changes.

> *"I believe that* (this event) *has positively changed my opinion because we are now aware of several things we totally ignored before and that are going to happen, sooner or later".*

Yet, the majority of participants shared the conclusion that the event has increased their worries and has provoked an increase of their fear and mistrust towards these technologies. To some of them, the information delivered has even provoked indignation. I quote:

> *"I mean, the document* (the scenario) *had an impact on me. I already knew certain things but what I learned I had to read two, three times, because I truly could not believe them. And then I was really upset".*

Others claimed to have finished the group with more worried than they had when they had arrived.

> *"I... I did not know some of these technologies and... yes, I can say what I said at the beginning... I feel even more concerned".*

In any event, the interview meeting was considered very helpful to open an interesting debate among all participants, especially in relation to privacy and security; it has also been effective in helping them to figure out when and how the implementation of these technologies should be regulated in order to minimize the relative impact whilst maximizing their efficiency.

Specific elements associated to the Spanish context

Some results of this interview meeting may have been significantly affected by some factors that belong specifically to the Spanish context. First, the focus groups were conducted in Madrid with people living either in the capital city or in some towns nearby, i.e. in a metropolitan context characterized by a relative familiarity with terrorist attacks, even in the recent past. Consequently the participants were also familiar with various types of security measures. If realized in smaller cities, barely affected by terrorism, the interview meeting might have yielded very different results. In fact, issues related to the political juncture such as the recent end of the "temporary cease fire" from the terrorist organization ETA was mentioned a few times in the debate, and was implicitly present as a background situation in all the groups.

C/ Albasanz 26-28, 3ªplanta Módulo D
28037 Madrid, España
Tel.: 91.375.1515
Fax: 91.375.7741
www.iesam.csic.es

Second, gender violence and sexual harassment, which are very important issue in Madrid and in Spain in general, have been the subject of various sociological studies, and enjoy a very high level of attention in the media. This issue was mentioned frequently in the discussions, revealing a remarkable sensitivity of both men and women towards its implications. In some instances, the technologies have received more support when they have been perceived as useful or effective in the fight against these types of crimes.

Third, the participants revealed a high level of mistrust towards the political actors of the state, although this mistrust did not affect the juridical system and its protagonists, the judges. Clearly, politicians and bureaucrats do not enjoy the support and the trust of Spanish citizens. This specific attitude significantly contributed to increase the worries about the implementation of new security technologies, probably producing more fear and concern than in other national contexts. This is especially true because most of the concerns focused not so much on the limits intrinsic to technological reliability but on the errors that human operators may cause and on the shift of purposes that these technologies may allow.

Finally, it is important to mention that many participants did study a lot at home, sometimes deepening their understanding through internet searches and further personal readings, or discussing the issues with friends and colleagues. As they say, the topic caught them deeply and turned them into very interested protagonists.

C/ Albasanz 26-28, 3ªplanta Módulo D
28037 Madrid, España
Tel.: 91.375.1515
Fax: 91.375.7741
www.iesam.csic.es

Overview of ANNEXES

(In Spanish)

Additional information and data are provided in a separate document containing the following annexes:

Annex 1 – Documents and material delivered to the participants

Annex 2 – Questionnaire

Annex 3 – Transcripts

Annex 4 – Frequency and CrossTables

Annex 5 – Comments to final questions (in English)

C/ Albasanz 26-28, 3ªplanta Módulo D
28037 Madrid, España
Tel.: 91.375.1515
Fax: 91.375.7741
www.iesam.csic.es