Public assessment of new surveillance-oriented security technologies: beyond the trade-off between privacy and security

Public assessment of new security technologies:

Beyond the trade-off between privacy and security

Vincenzo Pavone, PhD
Research Fellow
Institute of Public Policies
CSIC – Consejo Superior Investigaciones Científicas
Centro de Ciencias Humanas y Sociales
Calle Albasanz, 26-28
28037 Madrid
SPAIN
vincenzo.pavone@cchs.csic.es
Tel. +34 916022351

Sara Degli Esposti, MA
Department of Business Administration
University Carlos III, Madrid
Calle Madrid 126, 28903, Getafe, Madrid,
SPAIN
sdegli@emp.uc3m.es
sara.degliesposti@gmail.com

First Submission to Public Understanding of Science

Draft date: February 8, 2010

Disclaimer: Please contact one of the authors if you wish to cite this document. There are differences between this version and the final published version that must be considered at the time of assessing the essay's contribution. In regard to the matter in question: figures reported in tables and graphs have not been altered, while the definition 'security technologies' has been turned to 'surveillance-oriented security technologies'. The text could contain typing or orthographical errors.

Public assessment of new security technologies:

Beyond the trade-off between privacy and security

ABSTRACT

Although finding an effective response to security threats remains a contested issue, after 9/11 European governments have introduced new technologies as part of their security strategies. As these technologies are considered security enhancing but also privacy infringing, citizens are expected to trade part of their privacy in exchange for higher security. Whilst this forces citizens to consider security and privacy as exchangeable commodities, the trade-off obscures possible authoritarian implications of security technologies (STs). Drawing from the PRISE project data in Spain, this study tries to cast some light on how citizens actually assess security technologies. Qualitative data from focus groups are used to grasp citizens' ways of reasoning, whilst the existence of a trade-off between privacy and security is tested through analysis of correlations based on survey data. The outcomes suggest that people do not assess STs in abstract terms but in relation to their specific institutional and social contexts. Second, from this embedded view-point, citizens either express concern about government's real surveillance intentions and consider STs as essentially privacy infringing, or trust political institutions and endorse the adoption of STs to enhance their security. Neither group, however, faces a trade-off because concerned citizens see their privacy being infringed without having their security enhanced, whilst trusting citizens see their security being increased without their privacy being affected.

Keywords: privacy, security, biometrics, public perception, security policy, Spain

Public assessment of new security technologies:
Beyond the trade-off between privacy and security

1. Introduction

Global threats like international terrorism and transnational organized crime have constituted a serious challenge for domestic and foreign security since the end of the Cold war. Although an effective response to these threats remains a contested issue, after 9/11 several western governments have chosen to invest in new technological devices to foster a proactive attitude towards terror and crime. While expected to enhance national security, these technologies are subjecting ordinary citizens to an increasing amount of permanent surveillance, often causing infringements of privacy and a restriction of civil rights (Lodge, 2007; Levi and Wall, 2004).

An important debate has, thus, emerged around the impact of these technologies on the degree of security and privacy enjoyed by society. Mainstream approaches, drawing from economic theory, frame the relationship between privacy and security as a trade-off, whereby any increase in security levels curbs the amount of privacy enjoyed by citizens (Davis and Silver, 2004; Bowyer, 2004; Strickland and Hunt, 2005; Riley, 2007). As a result, these studies generally aim at enquiring how much privacy citizens are willing to trade in exchange for security.

The trade-off model, however, has been criticised on two main grounds. In cognitive terms, it has been argued that it approaches privacy and security in abstract terms, whilst they should in contrast be understood in a real context (Dourish and Anderson, 2006). It also reduces public opinion to one specific attitude, which considers these technologies as both useful in terms of security and potentially harmful in terms of privacy. Alternative attitudes may exist which consider these technologies either useless and risky or useful and harmless. (Tsoukala, 2006; Gaskell et al., 2004). In social and political terms, the trade-off approach has been criticized *as* it narrows the security policy debate down to a mere issue of striking a balance between security and privacy. In this way, though, it diverts attention from its technocratic implications, the possibility of authoritarian slippery slopes, but also the risks of function creep, data commercialization and social and racial discrimination (Spence, 2005; Amoore, 2006; Liberatore, 2007; Lodge, 2007b; Côté-Boucher, 2008).

The present study tries to cast some light on the relationship between security, technology and democracy as it is framed by lay public when assessing the introduction of new security technologies. Combining qualitative and quantitative methods, we try to explore, on the one hand, whether citizens adopt a trade-off approach and what could be the factors that citizens take into consideration when performing this assessment, and, on the other hand, whether citizens are aware of the social and political implications of security technologies, as suggested by critical studies.

This study draws on the data gathered by the PRISE project, conducted in 2007 to explore public assessment of new security technologies in five European countries. It focuses on the Spanish data and is divided into five sections: a revision of literature; a brief methodological note explaining the research design adopted; an in-depth presentation of the Spanish focus group records; the analysis of the cross-country survey data collected; conclusions and implications for policy makers.

2. Technology, security and democracy

Over the past ten years, in the face of global terrorism, nuclear proliferation, and trans-national organized crime, new approaches to terrorism and security have emerged (NATO, 2001; European Union, 2003; Rasmussen, 2001; Coker, 2002). As a result of the spatial and temporal unpredictability of criminal actions and of their global repercussions, the nature of security threats is indeed changing (Coker, 2004). Accordingly, the traditional means-ends rationality applied to the deterrence of specific threats is gradually replaced by a *risk management* perspective (Spence, 2005; Williams, 2005; Rasmussen, 2006; Heng, 2006; Kessler, 2008; Willams, 2008). From this new perspective, a safer society is often pursued through the implementation of new security policies trying to prevent the materialization of security threats through increasing reliance on technological devices and data exchange programs (Zureik and Hindle, 2004; Beck and Lau, 2005; Muller, 2008; Amoore, 2006; Tsouakala, 2006; Rasmussen, 2006, Zureik and Salter, 2005; Juels, Molnar and Wagner, 2005; Lyon, 2007; Lodge 2007; Côté-Boucher, 2008).[1] The lobbying effort of the industry is further fuelling this process, making technology uptake a crucial factor for security policies across the globe (Spence, 2005) and encouraging the redefinition of security in technological terms—i.e. as a problem whose solution should actually be found on technological grounds.

Although these technologies constitute a potential threat to individual privacy, their introduction has been justified in terms of a beneficial trade-off, whereby the amount of privacy lost is allegedly compensated by an increase in national and social security. For instance, presenting the 2007 rules on air passenger information exchange to fight terrorism, the vice-President of the EU Commission, Franco Frattini stated: "*Our goal remains preserving the right balance between the fundamental right to security of citizens, the right to life and the other fundamental rights of individuals, including privacy and procedural rights*." On the basis of this argument, many European countries are experiencing a gradual restriction of civil rights, which has provoked three main reactions, ranging from those who support emergency rules and technologies and justify the reduction of civil liberties in the name of national security to those who believe these restrictions to be undemocratic, unjustified and useless (Tsoukala, 2006).

As a consequence, a variety of participatory technology assessment processes have been organized in Europe to address what is perceived as a crisis of both cognitive and democratic legitimacy (Beck, Boss and Lau, 2003: 14-15). The EU and national governments seems to find themselves entrapped in what can be defined a *proximity paradox*: "*At the very time when technology has made it possible to bring the EU closer to the citizen more directly than ever before, EU citizens and residents appear to be more suspicious of it than ever before*" (Lodge, 2005: 535). In other words, public distrust of government increases as government agencies reach ever deeper into the space of individuals. As a result, while governments feel compelled to introduce new security technologies, the public perception of these new technologies gradually emerges as a sort of universal measure to guide governmental actions (PRISE Report, 2008).

Inspired by the privacy-security trade-off, many studies have paid special attention to citizens' perception of security technologies in order to elaborate responsible and shared guidelines on the implementation and regulation of security technologies. These studies, however, tend to reduce all public opposition to a privacy problem (Bowyer, 2004; Strickland and Hunt, 2005; Riley, 2007). Whilst privacy is often defined as "*the right of the individual to have one´s personal information protected from the undue prying eyes of government and private organizations seeking to use such personal information for trade and profit, without the consent of the individual, except in exceptional circumstances dictated by the law*" (Riley, 2007: 2) security has been defined in different ways. In general, it refers to the right and duty of national governments to (*a*) ensure personal safety for its citizens—otherwise presented as ‘freedom from fear’ (Manners, 2006; Tsoukala, 2006) or human security (Liotta and Owen, 2006)—(*b*) to enforce the laws and taboos of society (Loenen et al., 2007) and (*c*) to protect its geopolitical and economic integrity (Amoore, 2006).

Whatever the definition, these technologies are likely to force governments to make a clear distinction between those liberties that can be sacrificed to security needs and those that cannot be included in the trade-off (Bowyer, 2004). Yet, whilst a generalised lack of understanding of how security technologies function may also encourage a public sense of mistrust (Strickland and Hunt, 2005), acceptance of security technologies is highly context-dependent (Furnell and Evangelatos, 2007).

Actually, people’s decision in the trade-off between privacy and security raised by surveillance technologies is also affected by demographic, institutional and cultural factors. For instance, if trust in institutions depends on the type of technology in use, trust in technology is also a function of level of trust in institutions that use technology (Knights et al., 2001; Lodge, 2007). By the same token, ethnic identity, education and age strongly influence not only citizens’ acceptance of biometrics but also their willingness to trade privacy in exchange for security (Davis and Silver, 2004).

However, while it has been contested that more surveillance necessarily implies more security, it has also been denied that increased surveillance needs to come at the expense of privacy (PRISE Report, 2008). Moreover, it has been suggested that people tend to approach new technologies along a trade-off model only when they consider these technologies as risky *and* useful at the same time (Gaskell et al., 2004). In principle, it is possible to find at least three alternative positions to the issue (tab.1). People who believe that security technologies are risky in terms of privacy and do not increase the level of security, face a lose-lose situation (Group 2), whilst in the opposite case (Group 3), people would rather face a win-win situation. In neither case, however, there seems to be a trade-off at stake.

Tab. 1 about here

If privacy and security are socially embedded concepts rather than universal and abstract terms, it becomes necessary to pay special attention to the cultural and social factors that induce citizens to consider STs a solution to a security problem or, rather, a threat to privacy. It has been suggested, therefore, to study the relationship between privacy and security from a more discursive approach, which considers privacy and security as social products and technology as a site where social meaning is constantly negotiated and produced (Dourish and Anderson, 2006).

In fact, the cognitive validity of a trade-off approach between privacy and security is by no means the only controversial issue raised by the introduction of new security technologies. The adoption of the trade-off approach has also obscured a number of ethical, social and political implications increasingly associated with the introduction of security technologies, such as, for example, questions about data retention, ownership and exchange. Once in the database, not only the biometric data no longer belong entirely to the physical holders, they can also be stolen, commercialized or used for political purposes. In the face of these risks, the EU has not been able to elaborate and introduce a common and effective juridical framework to protect citizens from potential abuses (Lodge, 2007a, 2007b). The retrieval, storage and free exchange of biometric data also raise questions about the technocratic features of the process of technology development and implementation and about the potential authoritarian implications of an extensive use of these technologies (Levi and Wall, 2004). Given the actual flow of data among EU countries and the lack of a common juridical protection, biometric technologies constitute a serious challenge to current norms of democratic accountability

(Lodge, 2007b), although recent efforts to enhance citizen participation may represent a first step towards more accountable practices (Liberatore, 2007).

The breadth and impact of these technologies is especially visible when they are employed at national borders. On the one hand, through the diffusion of surveillance technologies, national borders have been extended well beyond their geographical locations, constituting "diffuse" borders where the state of law remains permanently suspended, paving the way to racial, ethnic and religious discrimination against the "migrants," now easily identified as potential "terrorists" (Côté-Boucher, 2008). On the other hand, these technologies are endorsing a discriminating process of *risk profiling,* a procedure through which all monitored citizens are encoded with a risk profile, turning people into low risk "trusted travellers" or high risk "suspicious immigrants." This procedure, usually carried out by private companies like *Accenture,* ends up endorsing certain types of global transfers (business men, managers) whilst restricting others, like immigrants or asylum seekers (Amoore, 2006; Muller, 2008).

Taking current studies on the social and political implications of new security technologies and the recent critiques to the trade-off model of privacy and security as a starting point, this study aims at exploring in deeper empirical details the relationship between security, technology and democracy as it is conceived and framed by Spanish citizens. Combining quantitative and qualitative methods, our work tries to address the following research questions:

(Q1) Do people actually evaluate the introduction of new security technologies in terms of a trade-off between privacy and security?

(Q2) Which security threats do they considered as most urgent and compelling?

(Q3) Are people aware—and concerned—about the risks of function creep for political purposes, data commercialization, and social discrimination?

(Q4) In what circumstances and under what conditions would people accept the introduction of new technologies for security reasons?

(Q5) How do they feel about public participation in security policy decision-making?

3. Methodology

The data hereby analysed and discussed have been retrieved from May to July 2007 in six European countries as part of the PRISE Project,[2] which was financed by the EU Commission, under the PASR[3] 2005. The methodology employed is called "interview meeting"[4] which consists of group interviews complemented by a questionnaire. Each meeting involves around 30 participants without any expert or professional knowledge about the technology at stake and of different ages and educational backgrounds. Before the meeting, participants receive informative material about the new technology and their potential implications. The meeting begins with an expert introducing the topic. Main advantages and disadvantages of the technology are discussed. Participants have the opportunity to ask for clarifying questions. At the end of the meeting participants complete a questionnaire and they are then divided into focus-groups of 6-9 people with a mediator. Discussion lasts approximately an hour and aims at revealing participants' reasons in their own language.

This technique is expected to increase the reliability of results in two ways. On one hand, the qualitative component allows enriching the set of feasible explanations beyond theory. On the other hand, the questionnaire isolates individual attitudes and provides a useful benchmark against weak or spurious inferences. We must clarify that the interview meeting pursues different objectives compared to a survey. In fact, it is not representative of any distribution of preferences at national or regional level. In contrast it uses demographic characteristics to ensure opinions' heterogeneity (see tab. 2). The idea is to explore the range of possible reactions a ST can generate. Running an interview meeting is particularly suitable in cases where prior public knowledge is limited and the issues at stake either are technically complex or pose ethical or political dilemmas.

Tab. 2 about here

4. Presentation of the qualitative results: The Spanish case

We decided to focus on Spanish-meeting records because Spanish society is known to hold a supportive attitude towards the development and application of new technologies (FECYT, 2005, 2007; Eurobarometer, 2003, 2005, 2006). In contrast, Spanish citizens have a critical attitude towards their political and administrative institutions, especially with regards to data retrieval and protection (Eurobarometers, 2008a, 2008b, 2009). Besides, Spain has been target of both ETA and Muslim fundamentalist terrorist activities. The city of Madrid, where the meeting was carried out, is accustomed to extensive surveillance though STs.

4.1 Technology, security and democracy in Spain

Whilst, in principle, the majority of the participants in the focus groups acknowledged that the introduction of new security technologies may give raise to a potential trade-off between security and privacy, in practice, the participants divided into two separate groups. One group clearly stated that if we have nothing to hide there is no problem in being monitored; whilst the other groups argued that if we have nothing to hide there is no reason to be monitored.

> *These things are necessary; they help us to move on with transparency, if you have nothing to hide… I think it is necessary …*
>
> *If I have nothing to hide, why should they monitor me?*

Confirming Gaskell's analysis (2004), therefore, these two groups actually considered these technologies either risky and useless, or useful and harmless. The first group felt that the privacy margins are increasingly smaller, and suggested that the new security measures may be used for perverse and illegitimate purposes. In their opinion, not only the increasing implementation of new security technologies is not justified by real dangers but it also fuels on a growing diffusion of fear among the citizens, which is purposively encouraged by the government for political purposes of control and manipulation.

More specifically, they seemed especially concerned with political use of the data collected *"They look at us; they control us and who is in possession of these data? If later there is a change in government, those who have been under scrutiny and are considered negatively by the government will easily find themselves in on a black list …"* Otherwise, the commercial implications of using fear to promote business interests were mentioned: *"In this consumer society, they offer you something that is presented as absolutely necessary, but in fact it is not necessary at all."* In fact, these technologies were not expected to really enhance the feeling of security but to produce the opposite: an increase of the sense of fear and vulnerability. The prospective of living in a 'police state', in which we all monitor each other, provoked in this group a general feeling of anxiety, fear and vulnerability.

In the second group, the participants accepted the introduction of new security measures to contrast what they perceive as real risks, proceeding from different sources: terrorism, organized crime as well as common criminality. These people, however, did not feel that their privacy was affected because they believe they have nothing to hide and nobody would be interested in monitoring ordinary people's life. In their view, security technologies increase security without affecting privacy. They do not see themselves as potential suspects.

In general, the ascription to either group seemed to be strongly affected by people's level of trust towards the interplay between technologies and institutions. People displaying a low level of trust towards the scientific and political institutions implementing these technologies tend to join the first group, prioritizing privacy and expressing concern that these technologies can be manipulated and diverted to other purposes. In contrast, the people more trustful towards both technologies and institutions tend to join the second group, prioritizing security and show a much lower level of concern for privacy.

4.2 Effectiveness and appropriateness

Independently from their opinion on privacy and security, participants agreed that these technologies may reduce the risks but will never eliminate them. In fact, more participants questioned security technologies more in terms of real effectiveness than in terms of privacy infringement. More specifically, some participants expressed serious doubts that technologies could actually prevent crimes, although they acknowledged some dissuasive power. First, the new technologies will never be able to cover it all: "there will always be holes" and, second, the criminals are capable of fooling the security systems. 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.
>
> 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, some participants argued that the real effectiveness of these technologies depends on the capability of the operators to deal with the acquired information. In this respect, ‘capability’ was used to express the technical/professional capability as well as the moral/ethical one.

> 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 anybody is showing ‘strange’ behavior, you really need to have some knowledge about people’s attitudes.
>
> 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.

In fact, the participants discussed at length the problems associated with the *interpretation* of the data. It was not so much the worry associated with being monitored, but rather the fear of being ‘interpreted’, judged on the basis of the gathered information. Confirming the problems of discrimination identified by Amoore (2006), the participants raised concerns about the pervasiveness of clichés and stereotypes, generally used to match the interpretative scheme of those who are in charge of the security systems.

> 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 stopped me all the time 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.

4.3 Not everything goes

As a result, several participants supported the idea of increasing security through the adoption of new technologies *only* in specific cases and places strictly belonging to the public sphere. In the private sphere, the use of invasive technologies can only be accepted in extreme cases, where urgency and gravity are of the highest level and there is no alternative, such as in the case of gender violence and sexual harassment *“violence against women, in this sense we ought to put much more effort in terms of security,”* and pedophilia: *"the type of criminals that keep committing the same crime, such as rape and pedophilia … these people should be monitored much more intensively."* Only in the third place of an ideal list of priorities, these technologies were associated to the fight against terrorism.

> I believe these measures are appropriate for international crime and terrorism, this is clear … I mean, the citizen should know that these measures may occasionally be annoying and 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.

In fact, all participants expressed concern that the effort in increasing security measures would be concentrated only against terrorism and only in places considered as sensitive targets, leaving the citizens unprotected and vulnerable in other places and in relation to other types of crimes: "*I am personally worried about other types of crimes… the introduction of new technology is fine, but it should not merely focus on terrorism*." 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 crimes connected to daily life: "*There are far more victims for gender violence than terrorism, I do not know the exact figures, but I am pretty sure about this.*"

4.5 Participation

Although positive about participatory processes of development and implementation of the new technology, the participants assigned more importance to transparency of information and effectiveness of general rules than to direct participation. However, the question about who was expected to participate gave again raise to the emergence of two groups, those who tried to identify who was supposed to participate, and those who focused 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 politicians.

Those who supported the participation of lay public specified that their participation would ensure that their interests were 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: *"Because, if things go wrong these are the people who are going to suffer from the consequences, both negative and positive."*

In contrast, the participants who expressed skepticism about 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).

In fact, the participation of state representatives, and more specifically of politicians, was more controversial. Some participants argued that it is the state that has to guarantee the protection of privacy and the correct implementation of these technologies so its participation is absolutely necessary: "*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: "*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 clearly stated that banks and multinational corporations should not be involved in the participatory process. 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."*

In the end, participants agreed on the necessity of introducing clear regulative and participative frameworks, in which also the judges are expected to play a significant role, given that they are responsible for the correct utilization of these technologies: *"When there is need to violate privacy, this should be always authorized by a judge, who has to decide the methods as well as the appropriate time and space constraints."*

5. Security and privacy: beyond the trade-off model

When citizens face a recently installed security camera in the street, they may have different reactions: whilst some consider the camera as a technical device that may discourage criminal acts and potentially increase their security, others could believe that the camera is a tool for political propaganda, which, rather than increasing security, allows for permanent monitoring and threatens individual privacy.

This situation, which often emerged during the focus groups, suggests that, whilst participants tended to have polarized opinions, effectiveness and appropriateness of security technologies are not the only issues at stake. In fact, people's opinion about security technologies may also be affected by other factors, which relate more to how this technology addresses their social priorities, to the social and institutional context in which these technologies are going to be implemented and to the actual agents that are likely to be in charge of the implementation, control and regulation of the use of technological devices. The more citizens actually trust public institutions, the more they see security as a priority and technology as an effective way to address this priority. In contrast, the more they distrust the government, the more they consider privacy as a priority, question the existence of a security problem and express doubts about the way in which "security" as an issue is presented and manipulated. Some of them question even whether technology can really be a solution to security threats.

Inspired by these outcomes of the Spanish focus groups, we decided to explore the existence and the background of these contrasting views in the whole sample. First, we selected a set of questions from the survey, which explicitly associate a specific technology (e.g. scanning, eavesdropping, CCTV, etc.) either to privacy infringement or to security enhancement. Each question is measured through a 5-points Likert scale from "completely agree" to "completely disagree" without forced answer. Then, we run exploratory factor analysis (Lawley and Maxwell, 1962) and from twelve variables we obtain just two factors able to explain 63% of the total variance.[5] As components are—by construction—mutually orthogonal, we allow factors to correlate by applying oblique rotation to the factor space.[6] This transformation makes it also relatively easy to identify each variable with a single factor without altering the results (Garson, 2009). We named the factors "SECURITY" (STs as security enhancing) and "PRIVACY" (STs as privacy infringing) respectively (see tab. 3).[7] By computing Spearman's rank correlation coefficients (Chen and Popovich, 2002) we observed an inverse significant relationship between the two dimensions. In other words, those citizens who believe that STs enhance their security tend to underestimate STs' impact on their privacy, whilst those citizens who are concerned about STs' impact on their privacy, tend to neglect their potential benefit in terms of security.

This finding deserved further attention because it seemed to contradict an implicit assumption of the trade-off model, which considers security technologies as both privacy infringing and security enhancing. We decided, thus, to check whether this effect was produced at a different level. During the focus groups, we noticed that people's assessment of security technologies were strongly affected by their prior opinion a) on the norms and functioning of the institutional context in which STs are likely to be implemented, b) on the capability and accountability of those who actively use these technologies and the data thereby retrieved and c) by their estimated risk of function creep and abuses. We decided, therefore, to select from the survey those questions that dealt directly with these issues (see tab. 4). By applying the same procedure explained before, we obtain two other factors that we call respectively "TRUST" (which relates not only to the trustworthiness of the institutional context in which STs are likely to be implemented but also to the legitimacy of technology as a solution to security problems) and "CONCERN" (which relates to the opposite case, and denotes fear of function creep and abuses while it questions STs as an effective solution to security problems).[8]

Finally, we computed partial correlation for all four factors (fig. 1). We can observe a significant positive correlation between "TRUST" and "SECURITY" as well as between "CONCERN" and "PRIVACY." Besides, we find a negative significant correlation between "TRUST" and "PRIVACY," and a negative, and yet not significant, correlation between "CONCERN" and "SECURITY." In other words, it seems that a more trusting attitude leads to consider STs as an effective solution to enhance security without infringing privacy. In contrast, a more concerned attitude leads to interpret security technologies merely as privacy infringing.

Fig. 1 about here

These findings show that citizens actually divide into two groups, trusting and concerned people, with different attitudes towards privacy and security. For trusting people (see tab. 1, group 3), privacy is not likely to be affected by enhanced security measures. In fact it is not even an issue: they do not see a trade-off, simply because they do not see their privacy being curbed. Concerned people (see tab. 1, group 2) believe that these technologies only restrict privacy. For them there is no trade-off either, because they do not see security being increased while their privacy is affected.

To confirm cross-factor relationships, we made a regression of "Security" and "Privacy," against the remaining factors and control variables without appreciating any visible change. As robustness checks, we replicated the analysis after applying an orthogonal rotation of the factor axes (Varimax) and results remained consistent.

Among the limitations it has to be said that running a structural equation model could have been more adequate in the analysis of the covariance structure. But, due to the limited sample size and to the exploratory character of our study we preferred not to use it. Concerning our analysis, we use 156 cases and always observe communalities below 0.6, therefore we are quite confident about the appropriateness of the sample size in running each factor analysis (MacCallum et al., 1999). The Kaiser-Meyer-Olkin measure of sampling adequacy provides further evidences of the appropriateness of our choice. Indeed, we observe a middling result (0.736) in the TRUST-CONCERN case and a meritorious result (0.866) in the PRIVACY-SECURITY case (tab. 3, tab. 4).[9] While the research design does not allow for a generalization it does, at least, support this hypothesis and suggest the need for further research on these issues, which may take these results as a guiding direction.

Tab. 3 about here

Tab. 4 about here

6. Conclusions and Recommendations

Whilst participants agreed that 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—was indeed necessary, they considered the adoption of new technologies as a possible solution *only* for specific crimes, in specific contexts, in proportion to the gravity of the crimes, and for prevention purposes. In addition, they suggested that these technologies should always be employed under specific legal and institutional guarantees, to avoid political abuses and deterioration of the democratic framework of law and rights.

The participants also acknowledged that these technologies may be useful against terrorism, but they also expressed concern that an over-emphasis on terrorism may come at the expenses of other risks that they perceive as more imminent and familiar. Moreover, they insisted that the use of these technologies for commercial and political purposes is not acceptable. 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, especially because they pointed at the difficulty of assessing when a behavior or an attitude of the citizens may be defined as suspicious.

As a result, there was special concern about the profile of those people in charge of monitoring the citizens. The participants were aware that errors may spring not only from the limits of the technologies but also from the limits of the people who operate them. As a consequence, participants not only expressed concern about the professional and moral profile of the operators of these technologies but they also insisted on the introduction of clear rules and reliable mechanisms of sanction in case of human errors. Interestingly, they suggested that a superficial or dishonest application of security technologies raises as much security concerns as the threats they are expected to address. The participants, therefore, argued 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.

From these results, we can draw two main conclusions. First, without denying the existence and relevance of technology-specific implications, the qualitative data suggest that context-specific implications do exist and are utterly relevant because citizens do take these implications into account when assessing security technologies. Citizens' concern about the introduction of security technologies is often due more to their mistrust towards the institutions that are supposed to employ and regulate these technologies, than to their alleged lack of knowledge about science and technology. This outcome in many respects, confirms the validity of the critiques raised by Wynne (2006, 2008) who made clear that the point of participatory science is not that the lay public is epistemically and scientifically more competent than scientific experts, but that lay publics assess technologies not only on the basis of technical information, but also on the basis of other types of knowledge (institutional, legal, social, moral), which are not technical but are nonetheless utterly relevant when technologies jump from laboratory to policy and social domains. This complex, contextual form of assessment, therefore, is of utter importance when policy decisions have to be taken but is often neglected by current assessment exercises based merely on abstract, technical expertise.

The adoption of a contextual approach partially explains why citizens assessing the introduction of new security technologies seldom approach the relationship between security and privacy according to the economic trade-off model. The latter assumes that security technologies are both privacy infringing and security enhancing. In contrast, the participants in this study divided in two main groups, which considered new security technologies either risky and unnecessary or very useful and harmless. In fact, a deeper line of demarcation seems to exist, which in turn affects citizens' approach to security and privacy. This line of demarcation runs along the dilemma between two broad political attitudes, trust and concern, of which the divide between privacy and security is only a by-product. In other words, the participants can be divided among those who generally trust technology and institutions, and those who are actually concerned about them. For the former, security is the main issue, whilst privacy is crucial issue for the latter. Political attitudes, however, may be changed but no exchanged, as it is instead possible between two political goods, i.e. security and privacy.

Our second conclusion, therefore, is that, when dealing with the public assessment of new security technologies, the adoption of an economic trade-off model between security and privacy may be misleading. In a context of rising security concerns, expanding definitions of risk and growing governmental monitoring activities, these results shed some light on the persisting gap between the governmental and the lay public perception of security agenda as well as on the political implications of the new public discourse on security.

Public assessment of new security technologies:

Beyond the trade-off between privacy and security

Tables and Figures

Tab. 1

Surveillance Technologies interpreted as…		… Privacy Infringing Devices	
		YES	NO
… Security Enhancing Devices	YES	*Trade-off model*	*Trusting attitude*
	NO	*Concerned attitude*	*Uninterested*

Tab. 2

	Male	Younger than 50	Having children	Living with children	Living alone	Undergraduate or inferior education	Living in a metropolitan area	Belonging to High Middle Class	N. of participants
Countries	%	%	%	%	%	%	%	%	
Austria	41,2	43,8	52,9	5,9	52,9	47,1	82,4	47,1	17
Germany	61,9	57,1	42,9	14,3	47,6	52,4	81,0	47,6	21
Denmark	51,9	55,6	74,1	40,7	22,2	22,2	81,5	63,0	27
Spain	42,4	66,7	48,5	45,5	12,1	69,7	81,8	30,3	33
Hungarian	50,0	52,9	55,9	44,1	23,5	52,9	85,3	20,6	34
Norway	42,3	60,0	80,8	69,2	3,8	46,2	69,2	46,2	26

Tab. 3

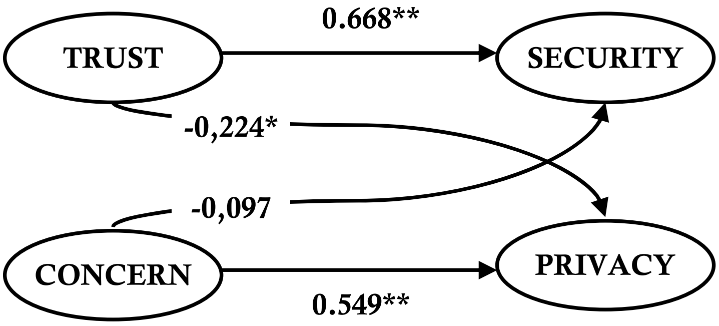
		Factor Loadings: Rotated Results	
	Variable	Factor1: SECURITY	Factor2: PRIVACY
25. Storing biometric data (e.g. fingerprints or DNA samples) of all citizens in a central database is an acceptable step to fight crime.	q25biom	**0.6830**	-0.1988
33. Scanning of persons for detection of hidden items is an acceptable tool for preventing terror.	q33visual	**0.7654**	-0.0591
38. The possibility of locating a suspect's mobile phones is a good tool for the police in investigating and preventing terror and crime.	q38local	**0.8478**	0.1716
40. The possibility of locating all cars is a good tool for the police in investigating and preventing terror and crime.	q40local	**0.8114**	-0.0475
43. Government institutions should store all data they find necessary for security reasons for as long as they consider it necessary.	q43data	**0.6811**	-0.2822
46. Scanning of and combining data from different databases is a good tool for police to prevent terror.	q46data	**0.8468**	-0.0108
50. Eavesdropping is a good tool for police investigation.	q50wire	**0.6276**	-0.0649
32. CCTV surveillance infringes my privacy.	q32visual	-0.0939	**0.6879**

37. The possibility of locating all mobile phones is privacy infringing.	q37local	0.0546	**0.8454**
39. The possibility of locating all cars is privacy infringing.	q39local	0.0315	**0.8586**
45. Scanning of and combining data from different databases containing personal information is privacy infringing.	q45data	-0.0875	**0.8114**
51. Eavesdropping is a serious violation of privacy.	q51wire	-0.2240	0.7238

Tab. 4

	Variable	Factor loadings: Rotated Results Factor1: TRUST	 Factor2: CONCERN
15. The security of society is absolutely dependent on the development and use of new security technologies.	q15general	**0.8269**	0.0401
17. If you have nothing to hide you don't have to worry about security technologies that infringe your privacy.	q17general	**0.8111**	-0.1465
18. When security technology is available, we might just as well make use of it.	q18general	**0.8242**	-0.0103
16. Many security technologies do not really increase security, but are only being applied to show that something is done to fight terror.	q16general	-0.0573	**0.6902**
20. It is uncomfortable to be under surveillance, even though you have no criminal intent.	q20general	-0.0173	**0.6840**
21. New security technologies are likely to be abused by governmental agencies.	q21general	-0.2587	**0.6662**
22. New security technologies are likely to be abused by criminals.	q22general	0.1213	**0.6559**

Fig. 1



** p < 0.001
* p < 0.05
* significance level of 0.05 (95%).
** significance level of 0.001 (99.9%).

Notes

[1] More specifically, the security technologies recently employed, or currently under review, generally include surveillance smart cameras; location and movement monitoring, mainly through mobile devices of RFID tags; biometric identification technologies, such as iris recognition, facial scan and the more traditional fingerprints; scanning technologies, like x-ray or the recently tested full body scan, eavesdropping technologies, data retention and data mining, as well as privacy enhancing technologies, such as encryption.

[2] PRISE stands for: "Privacy enhancing shaping of security research and technology – A participatory approach to develop acceptable and accepted principles for European Security Industries and Policies."

[3] Preparatory action for security research.

[4] For more information about this method and the other projects in which it has been implemented please visit the Danish Board of Technology's web site. URL: http://www.tekno.dk/subpage.php3?article=1234&toppic=kategori12&language=uk

[5] We use principal component extraction method (Hotelling 1933) and retain factors with eigenvalues greater than one. All analyses are conducted using STATA 10.

[6] We use Promax routine and set power equal to 2.

[7] The internal consistency of our instrument results a Cronbach's Alpha of 0.89 which is considered well acceptable (Nunnally 1978).

[8] Reliability was ensured by a Cronbach's Alpha of 0.73.

[9] "Stata 11 help for factor postestimation" (09/09/2009) provided by StataCorp LP, 4905 Lakeway Drive, College Station, TX 77845 USA. http://www.stata.com/help.cgi?factor+postestimation.

References

Amoore, L. (2006) "Biometric borders: Governing mobilities in the war on terror," Political Geography 25(3): 336—351.

Beck, U. and Lau, C. (2005) "Second Modernity as a research agenda: theoretical and empirical explorations in the 'meta-change' of modern society," The British Journal of Sociology 56 (4): 525—557.

Beck, U., Bonss, W. and Lau, C. (2003) "The Theory of Reflexive Modernization—Problematic, Hypotheses and Research Programme," *Theory, Culture & Society* 20 (2): 1—33.

Bowyer, K.W. (2004) "Face recognition technology: security versus privacy," *IEEE Technology and Society Magazine* 23(1): 9—19.

Chen, P.Y. and Popovich, P.M. (2002) *Correlation: Parametric and nonparametric measures*. Thousand Oaks, CA: Sage Publications.

Coker, C. (2002) *Globalization and Insecurity in the Twenty—First Century: NATO and the Management of Risks*. Oxford: Oxford University Press.

Coker, C. (2004) "NATO's unbearable lightness of being," *The RUSI Journal* 149(3): 18—23.

Côté—Boucher, K. (2008) "The Diffuse Border: Intelligence—Sharing, Control and Confinement along Canada's Smart Border," Surveillance and Society 5 (2): 142—165.

Davis, D.W. and Silver, B.D. (2004) "Civil Liberties vs. Security: Public Opinion in the context of the Terrorist Attacks on America," *American Journal of Political Science* 48 (1): 28—46.

Dourish, P. and Anderson, K. (2006) “Collective Information Practice: Exploring Privacy and Security as Social and Cultural Phenomena,” *Human-Computer Interaction* 21(3): 319—342.

European Union, Council of the (2003) *European Security Strategy: A Secure Europe in a Better World* (Brussels, 12 December 2003). URL: http://www.consilium.europa.eu/uedocs/cmsUpload/78367.pdf (accessed 28 September 2009).

EU Eurobarometer (2003) *Europeans and Biotechnology in 2002*. Eurobarometer Series n. 58.0.

EU Eurobarometer (2005) Social values, Science & Technology. Special Eurobarometer Series n. 225.

EU Eurobarometer (2006) Europeans and Biotechnology in 2005: Patterns and Trends. Final report on Eurobarometer n. 64.3.

EU Eurobarometer (2008a) *Data Protection in the European Union Citizens' perceptions: Analytical Report*. Flash Eurobarometer Series n. 225.

EU Eurobarometer (2008b) *Data Protection in the European Union Data controllers' perceptions: Analytical Report*. Flash Eurobarometer Series n. 226.

EU Eurobarometer (2009) *Confidence in the Information Society: Analytical Report*. Flash Eurobarometer Series n. 250.

FECYT, Fundación Española para la Ciencia y la Tecnología (2005) *Percepción Social de la Ciencia y la Tecnología en España 2004.*

FECYT, Fundación Española para la Ciencia y la Tecnología (2007) *Percepción Social de la Ciencia y la Tecnología en España 2006*.

Furnell, S. and Evangelatos, K. (2007) “Public awareness and perceptions of biometrics,” Computer Fraud & Security 2007(1): 8—13.

Garson, G.D. (2009) “Factor Analysis, last update 7/18/09,” from Statnotes: Topics in Multivariate Analysis. http://faculty.chass.ncsu.edu/garson/pa765/statnote.htm (accessed 7 September 2009).

Gaskell, G., Allum, N., Wagner, W., Kronberger, N., Torgersen, H., Hampel, J. and Bardes, J. (2004) “GM foods and the misperception of risk perception,” *Risk Analysis* 24(1): 185—194.

Heng, Y. (2006) “The ‘Transformation of War’ Debate through the Looking Glass of Ulrich Beck's World Risk Society,” *International Relations* 20 (1) 69—91.

Hotelling, H. (1933) “Analysis of a complex of statistical variables into principal components,” *Journal of Education and Psychology* 24(6): 417—441.

Juels, A., Molnar, D. and Wagner, D (2005) “Security and Privacy Issues in E-passports.” Proceedings of the First International Conference on Security and Privacy for Emerging Areas in Communications Networks, pp. 74—88. Washington, DC: IEEE Computer Society.

Kessler, O. (2008) “From Insecurity to Uncertainty: Risk and the Paradox of Security Politics,” *Alternatives: Global, Local, Political* 33(2). URL: http://vlex.com/vid/insecurity-uncertainty-risk-paradox-56022031.

Knights, D., Noble, F., Vurdubakis, T. and Willmott, H. (2001) “Chasing shadows: Control, Virtuality and the production of trust,” *Organization Studies* 22 (2): 311—336.

Lawley, D.N. and Maxwell, A.E. (1962) “Factor Analysis as a Statistical Method,” *Journal of the Royal Statistical Society* 12 (3): 209—229.

Levi, M. and Wall, D.S. (2004) “Technologies, Security, and Privacy in the Post-9/11 European Information Society,” *Journal of Law and Society* 31 (2): 194—220.

Liberatore, A. (2007) “Balancing Security and Democracy, and the role of Expertise: Biometrics Politics in the European Union,” *European Journal on Criminal Policy and Research* 13(1-2): 109—137.

Liotta, P. and Owen, T. (2006) “Why Human Security?” *The Whitehead Journal of Diplomacy and International Relations* 7(1): 37—55.

Loenen, B. van, Groetelaers, D., Zevenbergen, J. and Jong, J. de (2007) “Privacy versus national security: The impact of privacy law on the use of location technology for national security purposes,” in S.I. Fabrikant and M. Wachowicz (eds) *The European Information Society: Leading the way with Geo-Information*, pp. 135-52. Berlin: Springer.

Lodge, J. (2005), “e-Justice, Security and Biometrics: the EU’s Proximity Paradox,” *European Journal of Crime, Criminal Law and Criminal Justice* 13(4): 533–64.

Lodge, J. (2007a), “A Challenge for Privacy or Public Policy – Certified Identity and Uncertainties,” *Regio: Minorities, Politics, Society* 2007(1): 193-206.

Lodge, J. (2007b), “Freedom, security and justice: the thin end of the wedge for biometrics?” *Annali Istituto Superiore Sanità* 43(1): 20-26.

Lyon, D. (2007) “Surveillance Security and Social Sorting: Emerging research Priorities,” *International Criminal Justice Review* 17(3): 161—170.

MacCallum, R.C., Widaman, K.F., Zhang, S. and Hong, S. (1999) “Sample Size in Factor Analysis,” *Psychological Methods* 4(1): 84—99.

Manners, I. (2006) “Normative power Europe reconsidered: beyond the crossroads,” *Journal of European Public Policy* 13(2): 182—199.

Muller, B.J. (2008) “Securing the Political Imagination: Popular Culture, the Security Dispositif and the Biometric State,” *Security Dialogue*, 39(2-3): 199—220.

NATO (2001) “Chapter 2: The Transformation of the Alliance,” in “The Strategic Concept of the Alliance,” *NATO Handbook*, pp. 33—58. Brussels: NATO Office of Information and Press.

Nunnally, J. C. (1978) *Psychometric theory (2nd ed.)*. New York: McGraw-Hill.

PRISE Report (2008) “D6.2—Criteria for privacy enhancing security technologies.” URL: http://www.prise.oeaw.ac.at/docs/PRISE_D_6.2_Criteria_for_privacy_enhancing_security_technologies.pdf (accessed 9 September 2009).

Rasmussen, M.V. (2001) “Reflexive Security: NATO and International Risk Society,” *Millennium—Journal of International Studies* 30(2): 285—309.

Rasmussen, M.V. (2006) *The Risk Society at Work: Terror, Technology and Strategy in Twenty-First Century*. Cambridge: Cambridge University Press.

Riley, T.B. (2007) “Security vs. Privacy: A Comparative Analysis of Canada, the United Kingdom, and the United States,” *Journal of Business and Public Policy* 1(2): 1—21.

Shearing, C. and Johnston, L. (2005) “Justice in the Risk Society,” *The Australian and New Zealand Journal of Criminology* 38 (1): 25—38.

Spence, K. (2005) “World Risk Society and War against Terror” *Political Studies* 53(2): 284—302.

Strickland, L.S. and Hunt, L.E. (2005) “Technology, Security, and Individual Privacy: New Tools, New Threats, and the New Public Perceptions,” *Journal of the American Society for Information Science and Technology* 56 (3): 221—234.

Tsouakala, A. (2006) “Democracy in the Light of Security: British and French political Discourses on Domestic Counter-terrorism Policies,” *Political Studies* 54(3): 607—627.

Williams, M. J. (2005) “Revisiting Established Doctrine in an Age or Risk,” The *RUSI Journal* 150(5): 48—52

Williams, M.J. (2008) “(In)Security Studies, Reflexive Modernization and the Risk Society,” *Cooperation and Conflict* 43(1): 57—79.

Wynne, B. (2006) “Public Engagement as a Means of Restoring Public Trust in Science — Hitting the Notes, but Missing the Music?” *Community Genetics* 9(3): 211—20.

Wynne, B. (2008) “Elephants in the rooms where publics encounter “science”?: A response to Darrin Durant, “Accounting for expertise: Wynne and the autonomy of the lay public,” *Public Understanding of Science* 17(1): 21—33.

Zureik, E. and Hindle, K. (2004) “Governance, Security and Technology: the Case of Biometrics,” *Studies in Political Economy* 73(Spring/Summer): 113—38.

Zureik, E. and Salter, M.B. (2005) *Global Surveillance and Policy: Borders, Security, Identity*. Cullompton, Devon: Willan Publishing.