Acceptable Surveillance-Orientated Security Technologies

Degli Esposti, S. and Santiago Gómez, E.

Original citation:
Degli Esposti, S. and Santiago Gomez, E. (2015) Acceptable Surveillance-Orientated Security Technologies *Surveillance & Society* (13) 3-4, 437-454

https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/acceptable_technologies

Surveillance Studies Network

Surveillance & Society

Article

Acceptable Surveillance-Orientated Security Technologies: Insights from the SurPRISE Project

Sara Degli Esposti

Information Security Advancement Society, Spain.
sara.degliesposti@ismsforum.es

Elvira Santiago Gómez

Consejo Superior de Investigaciones Científicas (CSIC), Spain.
elvira.santiago@cchs.csic.es

Abstract

Pre-emptive security emphasises the necessity of envisioning and designing technologies enabling the anticipation and management of emergent risks threatening human and public security. Surveillance functionalities are embedded in the design of these technologies to allow constant monitoring, preparedness and prevention. Yet surveillance-orientated security technologies, such as smart CCTVs or Deep Packet Inspection, bring along with their implementation other risks, such as risks of privacy infringement, discrimination, misuse, abuse, or errors, which have often triggered public outrage and resistance. The same measures meant to foster human security can potentially make people feel insecure, vulnerable, and exposed. This outcome is the result of a narrow approach toward problem solving that does not take into account the same people the technology is supposed to protect. Drawing from both the socio-cultural and psychometric approaches to risk analysis and from the literature on public engagement in science and technology, this article presents a new methodological tool, which combines the traditional citizen summit method with an innovative mixed-method research design. The objective of this new form of participatory exercise is to engage the public and gather socially robust and in-context knowledge about public acceptance of surveillance technologies. The method has been developed as part of the SurPRISE project, funded by the European Commission under the Seventh Framework Program. The article explores qualitative data gathered during the Spanish Citizen Summit.

-

1. Introduction

Over the past ten years, in the face of global terrorism, nuclear proliferation, and transnational organised crime, new approaches to safeguard national and personal security have emerged. As a result of the spatial and temporal unpredictability of criminal actions and of their global repercussions, a safer society is often pursued through the implementation of policies foreseen the adoption and deployment of surveillance technologies (Ceyhan 2002). More specifically, Surveillance-Orientated Security Technologies (SOSTs) are technologies which collect information about the general population to monitor the activities of potential suspects and to prevent criminal acts from occurring. These technologies rely on ubiquitous surveillance and interconnected data exchange systems to identify and prevent malicious behaviours and criminal activity (Lippert and Walby 2012). Since SOST systems are based on the assumption that public security can only be enhanced through the deployment of mass surveillance measures, they impose on ordinary citizens a very high level of monitoring and control which have serious social implications (Lyon 2001; Lyon 2014).

Although the role played by the shifting nature of security risks and the national reactions to security threats have been studied (Kroener and Neyland 2012), little work has been done on how the public perceive the massive and often indiscriminate deployment of SOSTs (Luther and Radovic 2012; Pavone

Degli Esposti, S. and E. Santiago Gómez. 2015. Acceptable Surveillance-Orientated Security Technologies: Insights from the SurPRISE Project. *Surveillance & Society* 13(3/4): 437-454.
http://library.queensu.ca/ojs/index.php/surveillance-and-society/index | ISSN: 1477-7487

and Degli Esposti 2012; Strickland and Hunt 2005; Timan and Oudshoorn 2012). Diverging national understandings, political traditions and institutional settings may affect the way these technologies are perceived, implemented and managed (Luther and Radovic 2012). SOSTs migrate across countries and are often implemented throughout Europe regardless of cultural and social differences. To date, decisions on matters concerning security and privacy have left essential questions unanswered: to what extent is surveillance used for tackling security issues considered acceptable from a lay public perspective? How do Europeans diverge in the way they understand ideas such as privacy, surveillance and security and their mutual relationships?

The SurPRISE project, funded under the EU 7th Framework Programme for Research, has represented an attempt to shed light on these issues through the adoption of an innovative public-engagement method. SurPRISE, which stands for "*Surveillance, Privacy and Security: A large-scale participatory assessment of criteria and factors determining acceptability and acceptance of security technologies in Europe*" re-examines the relationship between security, privacy and surveillance—usually framed as a zero-sum game—through the adoption of a large-scale participatory method called citizen summit in order to dig into the reasons behind public acceptance, or opposition, to SOSTs. This article presents the citizen summit method adopted within the SurPRISE project and some preliminary findings gathered as part of the Spanish event.

The rest of the article is organised into three main sections. First an overview of the research streams informing the study—i.e. the risk studies and the science and technology studies perspectives (Pavone, Degli Esposti and Santiago 2013)—is offered. Then, the Surprise Citizen Summit method, with details regarding the organisation of the Spanish Citizen Summit, is presented. Finally, insights based on comments and opinions expressed by Spanish citizens during the Spanish summit held in February 2014 are reported.

2. Public perception of technology and associated risks

The Risk Study Perspective

The concept of 'risk' gained momentum in public and academic debates after World War II and it was associated to the development of new technologies, such as nuclear energy applications. Nowadays the concept of risk is relevant to many scientific disciplines. With regards to technology-related risks, there are three fundamental approaches to the study of how people perceive risks.

The *technical approach* insists on the possibility of obtaining a scientific and objective measure of the risks related to each technology. The objective of this approach is to develop valid measurements of risk in order to compare different types of risks. The rigorous process of defining the components of risk in precise quantitative terms, calculating the probabilities for unwanted consequences, and aggregating both components by multiplying the probabilities by the magnitude of the effects, is known as the risk assessment process (Kolluru and Brooks 1995).

Starting from considerations related to the discrepancy between what can be counted as an acceptable risk from a technical standpoint, and what people are actually willing to consider an acceptable risk (Fischhoff et al. 1981), the *psychological approach to the study of risk* identified important limitations in the technical approach (Festinger 1957; Kahneman and Tversky 1979) by suggesting that the distinction between objective and subjective risks should be better interpreted as a difference between two sources of subjective risks: one proceeding from the experts, and the other one proceeding from lay people. In brief, the psychological approach postulates a dualism between objective risks—defended by the technical approach—and subjective risks, understood in terms of cognitive representation of mental states of individual agents with their subjective perceptions influenced by contextual variables, beliefs, norms, or behavioural rules (Slovic 1987). As a result, risk is seen as a multidimensional concept which cannot be reduced to a mere probability calculus, but which should be expanded to include subjective judgements about the nature and magnitude of risk, personal preferences for expected outcomes, and personal judgements and values (Lopes 1983; Luce and Weber 1986). More recent studies, which adopt a psychometric paradigm, suggest that it is possible to quantify and to identify similarities and differences in the perception of different risks (Covello 1983; Fischhoff 1995; Fischhoff et al. 1981; Renn et al. 1992; Sjöberg 2000; Slovic et al. 1986; Slovic 2000; Slovic et al. 1985). The assessment of subjective risks can yield helpful information to understand public acceptance of new technologies (Schmidt 2004).

Nonetheless, technologies, and the risks they bring, are not implemented in a vacuum. A third stream of studies focuses on the importance of social and cultural elements in the investigation of risk perceptions. On this approach, known as the *sociological approach*, risks are not merely linked to the technology at stake, but proceed also from the context of implementation, from the actions, the culture, and the preparation of the people who manage and supervise the technology or the technological system (Douglas and Wildavsky 1982; Douglas 1992; Pavone, Goven and Guarino 2011). The sociological approach considers risks as social constructs which depend on sociocultural factors associated with given social structures (Rayner 1992). The sociocultural perspective focuses on events which are socially constructed as well as on 'real' consequences that are always mediated through different types of social interpretations, usually linked with distinct values and interests (Renn 1998). According to this perspective, the degree of trustworthiness of both institutions and operators is the key factor in the complex articulation of public perception of risks. As a result, the acceptance of technologies largely depends on issues such as social values, trust in institutions or the ways in which media present and interpret information. While the psychological approach pays attention to risk acceptance as a result of subjective individual decisions, the sociological approach focuses on the factors that make risks dominant in certain social groups and on potential conflicts regarding the distribution of these risks (Kasperson et al. 1988).

With respect to risks related to SOSTs, the introduction of new surveillance measures can be perceived by some people as a threat to their privacy or to their freedom of expression, caused by the fact that being under surveillance may induce self-censorship or conformism; a phenomenon known as the 'chilling' effect (Hughes 2012). Technology can also be inaccurate, or can be inappropriately handled, and produce false positive results reinforcing discriminatory practices. As a result, a measure that is conceived to help people feeling more secure (i.e. *subjective security*), by fighting crime and terror (i.e. *objective security*), may, in fact, produce the counterintuitive effect of making people feel exposed and self-conscious (Ball 2009). For these reasons, studies assessing people's perceptions of risks associated with given technologies appear to be very relevant in trying to understand public acceptability of SOSTs (Sanquist et al. 2006; Sanquist, Mahy and Morris 2008).

The Science and Technology Studies Perspective

However, technologies are complex realities which cannot be assessed only on the basis of the risks they entail. By relying on their own experiential knowledge, citizens come often to question the need, appropriateness and actual usefulness of several proposed, or recently implemented, technologies. For this reason, scholars in science and technology studies (STS) take into consideration additional factors at the time of investigating how citizens perceive and assess emerging technologies. Whilst earlier studies, inspired by the Deficit Model, used the level of scientific knowledge—or the lack of knowledge—as an independent variable and considered the level of support for science and technology as the dependent variable, contextual approaches have focused on more institutional and contextual variables, such as trust in public institutions or scientists, or technology operators (Pavone, Osuna and Degli Esposti 2011). Considering that citizens and lay public possess societal and experiential knowledge that is potentially very relevant to assess the risks and benefits of new technologies (Pavone, Goven and Guarino 2011; Wynne 2008), more recent approaches have tried to involve citizens and civil society organisations in participatory technology assessment exercises, such as citizen summits and consensus conferences, in order to promote *Public Engagement with Science* approaches (Felt and Wynne 2007). These approaches aim at asking new questions on the relationship between science, politics and society. Issues related to the kind of society envisioned in current innovation policies as well as the level of priority given to different phases of scientific discovery and technological innovation (Macnaghten, Kearnes and Wynne 2005). This approach wants to offer a more holistic view of the way technologies are studied and assessed to address these overarching questions (Wynne 2006). New participatory methods also need to be used in order to enrich and expand our understanding of modern technologies.

Factors influencing the way the public perceive SOSTs

The complexity and uncertainty surrounding the development and implementation of new technologies suggest that none of the approaches mentioned above can explain support or opposition toward SOSTs in an exhaustive manner. For instance, traditional approaches employed in risk analysis, which focus on the trade-off between technological risks and benefits, cannot be applied in the case of SOSTs because people tend to frame the benefits of SOSTs in individual terms, i.e. in relation to the increase of their own perception of security, while framing risks in social terms, i.e. in relation to the potential harm that these technologies may constitute for society and democracy at large.

In order to address and study individual assessments of risks and benefits of surveillance technologies, it is necessary to take into account not only the main factors identified by the psychometric paradigm in risk analysis—such as, for instance, familiarity with and proximity of risks—but also traditional elements studies in STS, such as how much people know and understand how the technology works. Other factors, identified by the socio-cultural approach in risk analysis, such as trust in public institutions and in technology designers and operators, should also be taken into consideration. In brief, on the one hand, we will consider how the amount and quality of information about the potential advantages, disadvantages and risks of the technology will affect the way people perceive any SOST. On the other hand, we will take into account how fairness and reliability of the institutional environment in which SOSTs are implemented affects public perceptions.

In addition, as studies investigating both public understanding of science and risk perceptions have explored the way a variety of publics frame and assess controversial technologies, we will rely on a participatory method in order to facilitate the emergence of new topics. This method, called Surprise Citizen Summit, is a participatory tool which not only includes simultaneously quantitative and qualitative methods, but also enables and promotes open spaces for debates, which enhance a democratic sharing of ideas, knowledge and proposals. Citizen summits help citizens express their opinions, interests, and priorities *and* share their knowledge with researchers. The citizen summit gives the opportunity to people to share their own experiential knowledge and shed light local dynamics and priorities often neglected in traditional risk assessment exercises. The method represents a new approach, which not only emphasises the importance of socio-cultural factors, but also considers lay people's knowledge to be a relevant type of knowledge which can guarantee the sustainable development and implementation of new technologies.

The following section will offer a detailed description of the methodology. The Surprise Citizen Summit has been used not only to retrieve sound qualitative and quantitative data, but also to create an open context where citizens have had the chance to interact and democratically discuss and evaluate different security technologies and offer suggestion to improve security policies.

3. The Surprise Citizen Summit Method

The citizen summit participatory model originates from the US local governments' desire to reinvent traditional public hearings (Moynihan 2003). When Anthony Williams took office in 1999 as the new mayor of Washington D.C., he asked the *Office of Neighborhood Action*, with the aid of *AmericaSpeaks*,[1] to create a new model of public participation that could contribute to district strategic planning. About 3,000 citizens attended the summit and for more than seven hours discussed citywide priorities, courses of actions, and the draft strategic plan, which was presented in four-page tabloid format prepared for the event by the *Office of Neighborhood Action*. Citizens were divided into tables of ten. Each table had a networked laptop computer and wireless polling keypads. Trained facilitators sat with each group to promote dialogue. Each group had to finally agree on the content of the message to be given to the mayor through the networked laptop. The mayor could reply to these messages in real time during the summit. The mayor could also ask citizens to vote on any question at any point during the summit by using the polling keypads. Results of the voting were immediately displayed on large screens at the front of the room.

In Europe, the *Danish Board of Technology Foundation* (DBT) has been applying the method—which they call ‘borgertopmøde’—for almost ten years now. DBT’s adoption of the citizen summit is mainly devoted to gaining a clear picture of citizens’ attitudes towards specific political priorities and possible courses of action (DBT 2015). The method has been used in global citizen consultation initiatives such as the on-going World Wide Views project,[2] which, since 2009, has been bringing citizens’ ideas and opinions on environmental issues to policymakers. The aim of a citizen summit is to gain insights about what citizens think of certain controversial matters, to unveil their political priorities, and to inform policy makers about alternatives for action.

A revised version of the citizen summit method has been used as part of SurPRISE project’s activities. The fundamental difference between the *Surprise Citizen Summit* (SCS) and previous citizen summits can be found in its research design. The citizen summits organised by the SurPRISE consortium differ from traditional citizen summits in three main ways: (1) the questions asked to the citizens reflect a specific theoretical model and are meant to measure constructs identified in previous academic studies; (2) discussions performed by group participants during their consultations are meant to be transcribed, at least partially, by note-takers and table facilitators in order to be analysed afterwards; (3) it is not just a participatory exercise but a proper investigative attempt, meant to generate knowledge far beyond the scope of the specific project.

Questions asked to participants during the event were developed to measure specific constructs and variables identified in the theoretical model developed as part of the project (Pavone, Degli Esposti and Santiago 2013). Questions were elaborated according to high-quality standards in survey design and under the supervision of Professor Sally Dibb, of the Open University Business School. Question validity was also tested during three pilot events—respectively in Hungary, Denmark and the UK—before the realisation of the actual summits. The research design also informed the development of the information material: a 40-page booklet translated into eight languages, and three short documentary films on Smartphone Location Tracking (SLT), smart CCTV (sCCTV) and cyber-surveillance through Deep Packet Inspection (DPI). Films were produced by Professor Kirstie Ball of the Open University in collaboration with the film company *Two Cats Can*.[3] The booklet and the films can been seen and downloaded from the project’s website.[4]

Twelve citizen summits were organised in nine European countries between January and March 2014. All summits were public meetings where about 200 citizens per country gathered together to have face-to-face conversations about the use of two specific SOSTs.

[1] http://americaspeaks.org/.

[2] www.wwviews.org.

[3] http://www.twocatscan.co.uk/.

[4] http://surprise-project.eu/dissemination/information-material-from-the-participatory-events/.

	Surprise Citizen Summits dates and locations	*SOSTs*
1.	Denmark (Aarhus 18/Jan)	SLT & sCCTV
2.	Hungary (Budapest 25/Jan)	SLT & sCCTV
3.	Norway (Oslo 01/Feb)	DPI & SLT
4.	Spain (Madrid 01/Feb)	sCCTV & DPI
5.	Italy (Florence 08/Feb)	DPI & SLT
6.	Austria (Vienna 22/Feb)	sCCTV & DPI
7.	United Kingdom (Birmingham, 01/Mar and 15/Mar)	sCCTV & DPI
8.	Switzerland (Zürich 8/Mar, Iverdu 22/Mar, Lugano 29/Mar)	DPI & SLT
9.	Germany (Kiel, 29/Mar)	SLT & sCCTV

***Table 1**: Couple of SOSTs used in each summit*

All participants in all countries, before the summit, received an invitation letter and the booklet translated into their national language. People participating in the nine citizen summits engaged in the same activities and answered the same set of questions during each event. Summit participants were selected to ensure they were not security experts. The demographic composition of the audience was meant to reflect the diversity of the country where the summit was held. Different people in terms of ethnicity, age, gender, education and employment status were invited to participate. The aim was not to closely represent the composition of the local community, but to give a say to the widest variety of perspectives and attitudes.

This article focuses specifically on the citizen summit held in Spain. Results highlight the existence of an interesting security paradox: even though participants considered their country a safe place to live in, they were nevertheless in favour of investing in security solutions. They were also highly concerned about the amount of personal information collected by SOSTs and the erosion of privacy that these technologies may cause. The relatively low level of trust in political authorities and the security agencies managing these systems complicates the issue further, as presented in the next section.

4. The Spanish Surprise Citizen Summit

In Spain, the Surprise Citizen Summit was held in Madrid, on Saturday 1st February in the Holiday Inn Hotel close to Santiago Bernabéu football stadium. Out of 220 people who had confirmed their attendance the day before the event, 185 people actually came and participated in the event. The recruitment method employed by the marketing agency hired for this purpose was "on site recruitment".

Participants were recruited on the street, at shopping malls or at other public places. Individuals were approached by recruitment agents who informed them about the aims of the project, the format of the citizen summit, and the kind of participation expected. People who agreed to participate were asked to complete a recruitment questionnaire. The aim of the recruitment questionnaire was to ensure that a fair representation of people with different socio-demographic characteristics, in terms of gender, age, education, employment conditions, were recruited to participate in the event. In Spain, the citizen summit's participants received as a compensation for their time a €50 gift voucher to be spent at a large shopping mall. The value of the voucher was considered high enough to make participation attractive for people already willing to participate and, at the same time, low enough not to constitute undue inducement.

Overall, *on site recruitment* helped ensure good coverage of individuals with different demographic characteristics, enabled the recruitment, and inclusion, of minority groups, and reduces the risk of people not attending the event after registering. Another advantage was to reduce the presence of individuals who frequently participate to marketing surveys and focus groups. The sample obtained was a convenience sample, whose objective was to give a say to individuals with different backgrounds and opinions and avoid as much as possible the representation of the views of a specific group of people. As a result, the sample of participants involved was balanced in terms of gender (52% females, 46% males) and age, though young people (under 30 years old) and elderly (over 60 years old) were slightly underrepresented with respect to adult people (between 30 and 40 years old). To ensure the success of the event, diversity and respect for others' opinions were embraced as key values.

Categories	*Frequency*	*Per cent*	*Valid Per cent*	*Categories*	*Frequency*	*Per cent*	*Valid Per cent*
18-29	23	12.8	14.0	Female	86	47.8	52.4
30-39	43	23.9	26.2	Male	75	41.7	45.7
40-49	41	22.8	25.0				
50-59	31	17.2	18.9				
60-69	19	10.6	11.6				
Over 70	6	3.3	3.7				
No answer	1	0.6	0.6	No answer	3	1.7	1.8
Total	164	91.1	100.0	Total	164	91.1	100.0
Missing data	16	8.9		Missing data	16	8.9	
	180	100.0			180	100.0	

***Table 2**: Summit participants' gender and age distribution*

In terms of preparatory information, citizen summit's participants received the Spanish version of the Surprise booklet two weeks before the event. The booklet contained explanations of three SOSTs, which were smart CCTV (sCCTV), Deep Packet Inspection (DPI), and Smartphone Location Tracking (SLT). Only two of these technologies, which were smart CCTV and Deep Packet Inspection, were discussed during the summit.

The day of the event, participants were divided into groups of eight people. Groups were heterogeneous in terms of gender, education and age. Group members were seated around a table. At each table, a facilitator was present to help people feel comfortable, share their views in a respectful manner, and understand how to answer questions by using *wireless audience response system*, known as 'clickers'. The head facilitator, Elvira Santiago, guided citizens throughout the event from the main stage. As part of the introduction, she explained how to use 'clickers' to answer questions, which were read by her and shown on a large screen at the centre of the venue. A representative from the Spanish Data Protection Authority gave a short speech introducing the topic and acknowledging the contribution of all participants to the success of the participatory exercise.

The wireless audience response system recoded each person's responses anonymously, and made aggregate results instantly available for display. These aggregate statistics helped foster the debate by providing instant feedback on the level of controversy around each issue discussed. The event ran smoothly throughout the afternoon, interrupted only by a coffee break organised in a room opposite the main venue. When the event ended most people were so engaged in the conversation they wished the event had lasted longer.

Time	*Activity*
14:45	Registration
15:20	Introduction given by Elvira Santiago and Vincenzo Pavone
15:40	1st round of questions – general questions
15:50	Emilio Aced's presentation, Head of the Support Unit of the Spanish Data Protection Authority (AEPD)
16:20	2nd round of questions – questions on sCCTV
16:25	Smart CCTV Film
16:35	Questions on Smart CCTV – questions on sCCTV
16:45	45-min Discussion Round on Smart CCTV
17:30	3rd round of questions – questions on sCCTV
17:50	Coffee break
18:20	4th round of questions – questions on DPI
18:25	DPI Film
18:35	5th round of questions – questions on DPI
18:45	45-min Discussion Round on DPI
19:40	6th round of questions – questions on DPI
19:50	Recommendation round
20:35	7th round of questions – general questions
20:50	8th round of questions – demographic questions
20:55	9th round of questions – evaluation of the event

***Table 3**: Programme of the Surprise Citizen Summit held in Madrid*

The initial introductory phase was followed by a series of general questions related to security, such as the use of technology to tackle security problems, or the level of anxiety perceived by people with regard to their safety. Once participants finished answering this set of questions, the head facilitator explained that the discussion focused on two specific SOSTs; advantages and disadvantages of each of them was explained during a documentary film of about seven minutes. After the film, the head facilitator handed over the discussion to table moderators, who facilitated both exchange of opinions and deliberation at tables.

Meanwhile, the table moderators took notes on participants' comments and remarks. Some tables had a table secretary who took detailed notes of everything said. People had the chance of discussing advantages, disadvantages and alternatives to each technology and to answer questions directly associated with each SOST. At the end of the summit, summit participants were invited to formulate their own recommendations to policy makers.

The summit ran smoothly throughout the day without interruptions. Group members were allowed to take breaks and have refreshments at different times during the day, in order to avoid disruptions and massive movements of people across the venue. At the end of the day, participants were asked to express their degree of satisfaction with the experience and the overall event. 69% of participants considered they gained new insights by participating in the citizen summit and 61% of participants believed that the citizen summit had generated valuable knowledge for the politicians.

5. Overview of Main Results

This section presents some qualitative results emerging from the information gathered during the Spanish citizen summit. 92% of participants said they were fairly knowledgeable about SOSTs after watching the documentary films, discussing with fellow participants and reading the information booklet. Regarding citizens' opinions, SOSTs generated a wide range of different reactions. Differences in the way the technologies are conceived and operate impact the way the technology is perceived. As showed in the tables, smart CCTV (sCCTV) was considered a far more acceptable solution than Deep Packet Inspection (DPI). 63% of participants considered Smart CCTV an effective national security tool, while only 43% of participants considered DPI an effective national security tool. 36% of participants felt more secure thanks to smart CCTV, while only 14% of participants felt more secure thanks to DPI. Participants were also concerned about how both smart CCTV (83%) and DPI (87%) could develop in the future. Participants were also equally concerned about the fact that both CCTV (67%) and DPI (78%) could reveal sensitive information about them.

	In my opinion, Smart CCTV is an effective national security tool	*Smart CCTV is an appropriate way to address national security threats*	*I feel more secure when smart CCTV is in operation*	*The idea of smart CCTV makes me feel uncomforta-ble*	*I feel that smart CCTV is forced upon me without my permission*	*I worry about how the use of smart CCTV could develop in the future*	*Smart CCTV only bothers me if it is used in the areas where I live and work*	*Smart CCTV worries me because it could reveal sensitive information about me*
Agree and stronly agree	62.8	48.9	36.1	41.7	72.8	83.3	21.7	66.7
Neither agree nor disagree	16.7	43.0	27.2	23.9	13.3	4.4	16.1	13.9
Disagree and strongly disagree	13.3	19.4	25.0	26.1	7.2	2.8	50.0	10.6
DK/NA	0.0	0.6	0.6	0.6	0.0	0.0	2.2	0.6
Total	92.8	92.8	88.9	92.2	93.3	90.6	90.0	91.7
Missing data	7.2	7.2	11.1	7.8	6.7	9.4	10.0	8.3
N = 180	100.0	100.0	100.0	100.0	100.0	100.0	100.0	100.0

***Table 4**: Opinions on smart CCTV*

	In my opinion, DPI is an effective national security tool	*DPI is an appropriate way to address national security threats*	*When I am online, I feel more secure because DPI is used*	*The idea of DPI makes me feel uncomfort-able*	*I feel DPI is forced upon me without my permission*	*I worry about how the use of DPI could develop in the future*	*DPI only bothers me if it is used to track my online activities*	*DPI worries me because it could reveal sensitive information about me*
Agree and stronly agree	43.3	41.7	13.9	66.1	78.9	87.2	48.3	77.8
Neither agree nor disagree	20.6	23.9	23.3	17.2	3.9	2.8	10.0	6.7
Disagree and strongly disagree	26.7	22.2	49.4	9.4	2.8	2.8	31.1	5.0
DK/NA	2.2	1.7	3.3	0.6	2.2	0.0	1.1	0.6
Total	92.8	89.4	90.0	93.3	87.8	92.8	90.6	90.0
Missing data	7.2	10.6	10.0	6.7	12.2	7.2	9.4	10.0
N = 180	100.0	100.0	100.0	100.0	100.0	100.0	100.0	100.0

Table 5*: Opinions on Deep Packet Inspection*

The difference in the level of acceptance of these two measures could be partly explained by the level of familiarity with each technology (Slovic, Fischhoff and Liechtenstein 1986). The presence of Closed-Circuit Television (CCTV) systems in European cities' public spaces is nowadays no longer perceived by citizens as seriously intrusive or particularly annoying (Hempel and Töpfer 2004). Citizens seem familiar with this type of surveillance technology.

> It was mentioned how cameras on public streets are not so annoying because public squares are not intimate places and in general participants agreed they were not bothered by seeing cameras in public places.
> (Discussion Table no. 1, facilitator's comments)

Smart CCTV

Even though citizens were familiar with CCTV (60% of the participants said they see cameras sometimes, often or all the time; and more than the 80% said they understand well what CCTVs are), they make a clear distinction between cameras in public spaces (e.g. on streets, or in public buildings) and cameras in private spaces (e.g. in shops or in private neighbourhoods).

In the area where you live, how often do you see CCTV cameras?		
	Frequency	*Per cent*
Never	26	14.4%
Rarely	34	18.9%
Sometimes	53	29.4%
Often	23	12.8%

I understand what smart CCTV is		
	Frequency	*Per cent*
Strongly agree	86	47.8%
Agree	64	35.6%
Neither agree nor disagree	11	6.1%
Disagree	3	1.7%

All of the time	34	18.9%	*Strongly disagree*	5	2.8%
Total	170	94.4%	Total	169	93.9%
Missing Data	10	5.6%	Missing Data	11	6.1%
Total	180	100.0%	Total	180	100.0%

***Table 6**: Familiarity with CCTV*

In order to understand why people considered smart CCTV as a more suitable security solution, it is important to distinguish whether cameras are managed by public authorities or by private entities and for what purpose. The way citizens perceive and interpret the institutional context in which CCTV is installed makes a fundamental difference in the kind of considerations made. Video surveillance carried out by public authorities is widely more accepted than the one carried out by private companies.

> Talking about cameras one participant said: "I don't understand cameras in the working space, in private firms, in the office. There are not there for security reasons, they are there to monitor employees." Again somebody said "But who would be interested in monitoring me?" and the participant replied: "Well, maybe you are not an important person today, but who knows if tomorrow for whatever reason you don't become an objective."
> (Discussion Table no. 21, facilitator's reflections)

People considered that cameras located in public spaces submit all people to the same type and level of surveillance; rather than considering it blanket surveillance, they interpreted CCTV surveillance as a universal and fair practice. Citizens defined smart CCTV as a type of 'objective' measure, as it seems to undertake some sort of 'objective observation' of abnormal, external situations.

> Some other participant emphasised that CCTV play a role of an 'objective witness' of anomalous situations. Footages can be checked afterwards to obtain reliable information and to help clarify circumstances and identify suspects.
> (Discussion Table no. 1, facilitator's reflections)

Citizens supported the idea that the recordings of these cameras offer a real and indisputable picture of possible criminal acts, and these images can work as an objective source of evidence. Yet, they mostly mentioned traditional CCTV systems, rather than smart systems, at the time of mentioning positive aspects of this kind of technology.

> With respect to cameras' effectiveness, Asunta's case was mentioned—the little girl from Galicia who was possible to identify in certain private vehicles thanks to the recordings made by some cameras.
> (Discussion Table no. 21, facilitator's reflections)

Despite CCTV's ability to serve as a reliable source of evidence, citizens also point out its inability to be used as a preventive measure and to be used to trigger an immediate intervention.

> Cameras do not offer immediate aid. Although aid is not provided when the problem occurs, people start discussing how surveillance cameras can also offer evidence of the perpetuated crime.
> (Discussion Table no. 16, facilitator's reflections)

In fact, CCTV appears to be absolutely ineffective from a victim's perspective, as it does not stop crime from occurring and its use is usually restricted to very limited areas.

> – I wonder where cameras were when I was attacked. I mean, who decides where they are installed and according to which criteria they are installed in one place and not in another one?
> – Cameras do not act as a deterrent; cameras are just there to identify people…
> – This is true… but they should also have a deterrent effect or better to employ more policemen who have much a stronger deterrent character.
>
> (Discussion Table no. 8, reported speeches of three participants)

The ability to provide evidence is considered the cameras' main advantage. Yet citizens are aware that cameras are useful only under strict regulatory supervision.

> At the end, CCTV systems are just silent and inert witnesses watching a situation. It offers footage as evidence of what has occurred. Yet the effects and real consequences of its use depend entirely on the functioning of the judicial system and on the application of criminal law. These were recurrent ideas.
> (Discussion Table no. 15, facilitator's reflections)

Citizens believe that the effectiveness of cameras cannot be appreciated in the 'here and now' but, rather 'before' the criminal action is perpetrated, due to their dissuasive power, or 'after' the crime has occurred, since recordings can be helpful both to look for portrayed criminals or as evidence in a trial. Nonetheless, citizens are also aware of the potential risks and misuses of the technology. For instance, they were sceptical about adding a 'smart' software component to traditional CCTV systems.

> Regarding technological challenges, what algorithms can do is still very limited and adding a human element is fundamental to prevent errors. However, this human element also raises concerns: CCTV systems can be 'manipulated, intentionally or unintentionally.' Who watch the watchers? Who control the cameras? These questions represented key issues for some participants. Recorded footage can occasionally even end up on internet, which implies a serious risk.
> (Discussion Table no. 15, facilitator's reflections)

Participants worried also about the potential discriminatory effects of relying on 'smart' systems. 72% of participants agree or strongly agree with the statement "Smart CCTV worries me because it could result in my behaviour being misinterpreted."

> Another participant pointed out as a negative element the fact that CCTV systems 'put people in boxes' by indicating someone as a criminal.
> (Discussion Table no. 2, facilitator's reflections)

CCTVs were also questioned on a civil rights ground. Concerns about individual privacy and freedom were by no means confined to just one table discussion: 75% of participants strongly agree or agree with the statement "Smart CCTV worries me because it could violate my fundamental human rights."

> Some participants expressed their disagreement with the idea of using CCTV as a social control element, for example with the purpose of monitoring who is participating in a demonstration and expressed their concerns about the potential negative consequences this practice may have on their personal lives. They also stressed the need to know who hold these footages and for what purpose they are used. […] They oppose the use of CCTV in

> more private places and one of the participant said that smart CCTV undermines 'the right to be a free person.'
> (Discussion Table no. 1, facilitator's reflections)

In the pursuit of a difficult balance between acceptable and inacceptable uses of CCTVs, citizens clearly stated that only public authorities should implement, control and operate smart CCTV systems in order to guarantee their effectiveness. Public authorities should also control and manage the storage of the images recorded, and use transparent procedures.

> All agreed in saying that it was absolutely necessary to make available clear information about what happen to CCTV footage, how it is used and who has access to this information.
> (Discussion Table no. 2, facilitator's reflections)

Deep Packet Inspection (DPI)

Compared to smart CCTVs, Deep Packet Inspection (DPI) was welcomed with greater distrust and criticism, as it was generally considered to be a very intrusive technology, whose implementation and modalities of operation raised remarkable concerns. The participants were especially concerned with the high degree of arbitrariness when it comes to who, what, where and why DPI operators choose to monitor and track.

> In comparison with CCTV, DPI is perceived as a much more threatening kind of measure: while cameras monitor you at a particular time, with DPI you are constantly and entirely under surveillance. This is far more intrusive.
> (Discussion Table no. 2, facilitator's reflections)

DPI clearly is a technology that requires some sort of judgement to define what are the communications, actions, words or images that may be associated to risky behaviours.

> What do we define as anomalous behaviour and as a consequence worth to be monitored? Somebody said: "Surveillance criteria don't make sense at all: what is an abnormal pattern?"
> (Discussion Table no. 21, facilitator's reflections)

In addition, monitoring through DPI implies a form of targeted surveillance, as it is mostly orientated towards private spaces of communications and virtual social interactions. This specific aspect of DPI not only triggered extensive debate, it also encouraged the participants to claim that citizens should take some degree of responsibility for their activities on the web.

> Lack of awareness. The debates focused on everyone's responsibility to control what they do on internet. There is a strong need to know more and be more cautious.
> (Discussion Table no. 21, facilitator's reflections)

Nonetheless, the participants admitted that DPI could be very useful to contrast serious crimes like terrorism or child pornography. In contrast with smart CCTVs, DPI was perceived to act in the immediate time, in the present of the 'here and now'. Doubts were also not absent, though, not only because terrorists are perceived to be more sophisticated than how they are generally described.

> Some participants said that DPI cannot be considered an effective tool to locate terrorists because they are far more 'sophisticated' and not 'so idiot' to speak about the organisation of a crime in explicit terms through internet.
> (Discussion Table no. 1, facilitator's reflections)

> 'Terrorists will bypass these checks' 'How many terrorists have been caught by using DPI?' 'they question everybody's privacy just to catch one person' 'as long as they catch at least one.' 'Yes, but you must believe in what they tell you has been done.'
> (Discussion Table no. 4, facilitator's reflections)

The major problem, though, proceeded from the fact that DPI monitors in real time what is perceived as a fundamentally private space, i.e. our online activities, which participants suggest should be protected exactly in the same way our mail communications are protected. Moreover, being ubiquitous and beyond reach as to when it operates, where and for how long, DPI seemed to affect citizens' private space and privacy in an unpredictable way. DPI leaves people vulnerable and with no choice about whether or not to be monitored. During table discussions, this consideration was often contrasted with the features of CCTV systems, whose location and operation in both public and private spaces is always announced, giving citizens the possibility to avoid places and buildings where CCTVs are installed, if they wish to do so.

> This is very intrusive. "It's like someone entering into your house." There is also nothing to be done to defend oneself: passwords, cryptography, etc. nothing works, 'they can see everything.' To prevent this from occurring 'one should go away from this world and be permanently disconnected.'
> (Discussion Table no. 2, facilitator's reflections)

Participants criticised also the fear-based approach used not only to increase their feeling of insecurity, but also to manipulate their opinion in order to make SOSTs more acceptable. A participant compared the ubiquitous use of DPI to the indiscriminate use of antibiotics.

> With DPI it is used the same fear approach that is applied by pharmaceutical companies seeking to introduce doses of antibiotics into manufactured food as a disease prevention strategy.
> (Discussion Table no. 12, facilitator's reflections)

Looking at the future, participants worried that, even when SOSTs were used in an acceptable and controlled way, they could be easily abused to follow the interests of powerful political elites and/or other commercial actors.

> 'You are on sale.' 'There is somebody making money selling your data.'
> (Discussion Table no. 4, facilitator's reflections)

> This is not surveillance but massive collection of data. We don't know who is doing this and for whom is working. In the film we saw China and the Arab countries as examples, but we don't know to what extent this is carried out in Europe. I use different browsers and tools to check who is tracking me. All private firms are monitoring us.
> (Discussion Table no. 5, facilitator's reflections)

Participants expressed clear interest in knowing not only how technologies are used and regulated today, but also how they will be used and regulated in the future. That is why citizens demanded clear limitations on the use of SOSTs, more information on the rules under which surveillance acts are performed.

Participants' trust in operating and regulating actors was limited and contextualised: their confidence depended on whether the purpose for which the technology was implemented was actually respected and on what were the rules and principles governing the operations of those in charge of controlling the system, as well as the presence of accountability procedures. Trust and confidence in institutional actors and authorities seemed also to be a terrain for continuous negotiations.

> There is nothing new to be invented. If usually police needs a court order to act, on the internet the same legal requirements should be applied to safeguard our privacy. Technology is used against citizens. They must comply with what written in the Convention on Human Rights!
> (Discussion Table no. 5, facilitator's reflections)

Participants were aware that the implementation of new security technologies was part of a legitimate strategy for lowering the costs of security, but they still were more in favour of investing in personnel, e.g. policemen, judges and security operators. Needless to say, participants insisted that it would be a better and alternative strategy to invest in the real causes of insecurity: lack of education and employment, which are the most important causes of social exclusion.

> What would you suggest? Eradicate insecurity causes: invest in education and generate new jobs: unemployment is a main source of insecurity.
> (Discussion Table no. 5, facilitator's reflections)

Yet, if security had to be necessarily improved by means of security technologies, participants claimed the need for updated legislation, able to cope with the new reality of this century and its new threats. Legislation should be designed, approved and respected at European level, but without neglecting regional differences.

> What is your recommendation? A global comprehensive legislation able to increase transparency and public awareness.
> (Discussion Table no. 6, facilitator's reflections)

Within this new governance system, control mechanisms must be transparent and citizens should receive clear information about the use and rules of security technologies.

> Creation of a system, a network, a set of powerful communication campaigns with the aim of providing clear and easy to understand information to the public to let people know where they need to go if they want to complain, who people should contact to make a request and finally to let people know how they could claim back their personal information if at some point they need it (in a judicial trial or to face an accusation).
> (Discussion Table no. 9, facilitator's reflections)

Participants also proposed the creation of a new figure, a mediator, able to help citizens connect with the authorities responsible for the use and regulation of these technologies, in order to have access at all times to their personal information, to where, when and why their privacy has been legally infringed and to what are their rights in case of abuse.

> What would you suggest? 'Creation at regional or national level of a technological public advocate, a figure similar to the Ombudsman.'
> (Discussion Table no. 9, facilitator's reflections)

Finally, with regards to the trade-off, effectively half of participants approached security and liberty as a zero-sum game: they said to consider that these SOSTs were both security enhancing and privacy infringing (51%). Yet, only a small portion of them was actually willing to give up their liberty in exchange for an increased level of security. The other half did not adopt the trade-off approach, and believed that these technologies were highly intrusive but not really effective (26%), or, quite to the contrary, consider these technologies very effective in terms of improving security, but not privacy infringing (11%). Finally, a very small group of participants were indecisive and did not see any security gain or privacy harm (2%).

Smart CCTV	Deep Packet Inspection (DPI)
Objective evidence of criminal activity	Subjective evidence of criminal activity
Visible use of the device	Invisible use of the device
Proved security outcomes	Unknown security outcomes
Human-mediated form of surveillance	Technology-driven form of surveillance
Third-party responsible to provide information	Personal responsibility to find information on how the technology works
Used to fight petty crime	Used to fight serious crime

Table 7*: Comparison between smart CCTV and DPI*

6. Conclusion

Smart CCTV systems are perceived in Spain differently depending on its private or public use. Citizens are more critical towards the private use of CCTV cameras, which are considered intrusive, while quite supportive of the use of cameras in public locations. Security cameras in private establishments protect the owners of eventual theft and assault, but not ordinary citizens. The main purpose of private cameras seems to be controlling consumers' purchasing habits rather than the security of either objects or people. DPI is perceived as a measure more used to pursue economic goals than to increase public security.

Traditional CCTVs receive more support than smart CCTV. Smart CCTV systems located in private residential areas are considered typical examples of measures conceived to protect wealthy families and their belongings: these cameras are perceived to increase separation between rich and poor people, and increase social inequalities. While traditional CCTV systems are considered fairly equitable forms of surveillance, it is not clear when, by whom, and for what reasons people are monitored by means of DPI. The fundamental lack of transparency and information around DPI raises serious concerns among citizens. The 'algorithmic' components of both smart CCTV and DPI also worry participants. It is not clear what are the rules establishing what it is defined normal or what is considered to be abnormal behaviour. The autonomous decisions taken by algorithms also raise and leave unanswered important questions about fairness and equality. Certainly, this preliminary recognition of Surprise Citizen Summit results leaves many questions open, asking for a more in-depth analysis of both quantitative and qualitative results. For example, most people are concerned about terrorism and consider it one of the major problems of the contemporary world, yet very few citizens believe they may be victims of a terrorist attack and see the need of investing in surveillance measures.

Another interesting finding, supporting socio-cultural approaches to the analysis of risk, relates to the need of involving the public in the management of new risks and new threats of the 21st century. SOSTs should be regulated at the European level to ensure fairness of treatment to all Europeans, though national and regional peculiarities and demands should contribute to shape overarching policies. Moreover, in order to combine effectiveness and legitimacy, participants asked for the creation of an institutional mediator, able to create a permanent and effective communication between security agencies and public authorities, on the one hand, and civil society, on the other hand. The technology mediator is expected to ensure citizens access to their own data, and to inform citizens about their rights and duties and while also informing politicians and regulators of citizens' opinions, concerns and suggestions. Citizens seem also to be willing to contribute to the protection and preservation of their data, by contributing to the design of both public policies and new technologies. In addition, citizens want to participate actively in controlling infractions and abuses in the use of surveillance technologies. Through increased transparency and dialogue social trust in the authorities responsible for the use of SOSTs can be gained and ensured over time. Trust, in fact, need to be continuously negotiated and built through the existence and correct functioning of clear rules, transparent information and effective participatory practices.

References

Ball, K.S. 2009. "Exposure." *Information, Communication & Society* 12(5): 639-57.

Ceyhan, A. 2002. "Technologization of security: Management of uncertainty and risk in the age of biometrics." *Surveillance & Society* 5(2): 102-123.

Covello, V.T. 1983. "The perception of technological risks: A literature review." *Technological Forecasting and Social Change* (23): 285–97.

DBT 2015. *Citizen Participation*. Available at: http://www.tekno.dk/theme/citizen-participation/?lang=en

Douglas, M. 1992. *Risk and Blame: Essays in Cultural Theory*. London: Routledge.

Douglas, M., and A. Wildavsky. 1982. *Risk and culture: An essay on the selection of environmental and technological dangers*. Berkeley: University of California Press.

Felt, U., and B. Wynne. 2007. "Taking European knowledge society seriously." Luxembourg: DG for Research. EUR 22:700.

Festinger, L. 1957. *A Theory of Cognitive Dissonance*. Stanford: Stanford University Press.

Fischhoff, B. 1995. "Risk perception and communication unplugged: Twenty years of process." *Risk Analysis* 15(2): 137–45.

Fischhoff, B., S. Lichtenstein, P. Slovic, S.L. Derby, and S.L. Keeney. 1981. *Acceptable Risk*. Cambridge: Cambridge University Press.

Hempel, L., and E. Töpfer. 2004. CCTV in Europe. Final Report. The Urbaneye Working Papers Series, edited by 5th Framework Programme of the European Commission.

Hughes, S.S. 2012. "US Domestic Surveillance after 9/11: An Analysis of the Chilling Effect on First Amendment Rights in Cases Filed against the Terrorist Surveillance Program." *Canadian Journal of Law and Society* 27(3): 399-425.

Kahneman, D., and A. Tversky. 1979. "Prospect theory: An analysis of decision under risk." *Econometrica* 47(2): 263–91.

Kasperson, R. E., O. Renn, P. Slovic, H.S. Brown, J. Emel, R. Goble, J.X. Kasperson, and S. Ratick. 1988. "The social amplification of risk: a conceptual framework." *Risk Analysis* 8 (2): 177-187.

Kolluru, R.V., and D.G. Brooks. 1995. Integrated Risk Assessment and Strategic Management. In *Risk Assessment and Management Handbook. For Environmental, Health, and Safety Professionals*, eds R. Kolluru, S. Bartell, R. Pitblade and S. Stricoff, 2.1–2.23, New York: McGraw-Hill.

Kroener, I., and D. Neyland. 2012. "New technologies, security and surveillance." In *Routledge Handbook of Surveillance Studies*, edited by K.S. Ball, K.D. Haggerty, and D. Lyon. London: Routledge.

Lippert, R., and K. Walby. 2012. "Municipal corporate security and the intensification of urban surveillance." *Surveillance & Society* 9(3): 310-20.

Lopes, L.L. 1983. "Some thoughts on the psychological concept of risk." *Journal of Experimental Psychology: Human Perception and Performance* (9): 137–44.

Luce, R.D., and E.U. Weber. 1986. "An axiomatic theory of conjoint, expected risk." *Journal of Mathematical Psychology* (30): 188–205.

Luther, C., and I. Radovic. 2012. "Perspectives on Privacy, Information Technology, and Company/Governmental Surveillance in Japan." *Surveillance & Society* 10(3/4): 263-75.

Lyon, D. 2001. *Surveillance society: Monitoring everyday life*. Buckingham, Philadelphia: Open University Press.

Lyon, D. 2014. "Surveillance, Snowden, and Big Data: Capacities, consequences, critique." *Big Data & Society* 1(2): 1-13.

Macnaghten, P., M.B. Kearnes, and B. Wynne. 2005. "Nanotechnology, governance, and public deliberation: what role for the social sciences?" *Science Communication* 27(2): 268.

Moynihan, D.P. 2003. "Normative and Instrumental Perspectives on Public Participation Citizen Summits in Washington, DC." *The American Review of Public Administration* 33(2): 164-188.

Pavone, V., and S. Degli Esposti. 2012. "Public assessment of new surveillance-oriented security technologies: Beyond the trade-off between privacy and security." *Public Understanding of Science* 21(July): 556-72.

Pavone, V., J. Goven, and R. Guarino. 2011. "From risk assessment to in-context trajectory evaluation-GMOs and their social implications." *Environmental Sciences Europe* 23(1): 3-13.

Pavone, V., C. Osuna, and S. Degli Esposti. 2011. "Invertir en ciencia y tecnología en tiempos de austeridad económica:¿que opinan los ciudadanos?" In: España: Percepción Social de la Ciencia y la Tecnología 2010, pp. 115-36. Madrid: Fundación Española para la Ciencia y la Tecnología, FECYT.

Rayner, S. 1992. "Cultural theory and risk analysis." In: *Social theories of risk*, edited by Sheldon Krimsky and Dominic Golding. Westport: Praeger.

Renn, O. 1998. "Three decades of risk research: accomplishments and new challenges." *Journal of Risk Research* 1(1): 49-71.

Renn, O., W. Burns, R.E. Kasperson, J.X. Kasperson, and P. Slovic. 1992. "The social amplication of risk: Theoretical foundations and empirical application." *Social Issues* 48(4): 137–60.

Sanquist, T.F., H.A. Mahy, C. Posse, and F. Morris. 2006. "Psychometric Survey Methods for Measuring Attitudes toward Homeland Security Systems and Personal Privacy." In: Proceedings of the Human Factors and Ergonomics Society Annual Meeting, pp. 1808-11.

Sanquist, T.F., H.A. Mahy, and F. Morris. 2008. "An Exploratory Risk Perception Study of Attitudes Toward Homeland Security Systems." *Risk Analysis: An International Journal* 28(4):1125-33.

Schmidt, M. 2004. "Investigating risk perception: A short introduction." In: M. Schmidt. *Loss of agro-biodiversity in Vavilov centers, with a special focus on the risks of genetically modified organisms (GMOs)*. PhD Thesis, Vienna, Austria. Available at: http://faculty.mercer.edu/butler_aj/documents/Intro_risk_perception_Schmidt_000.pdf

Sjöberg, L. 2000. "Factors in Risk Perception." *Risk Analysis* 20 (1): 1-12.

Slovic, P., ed. 2000. *The perception of risk, Risk, society, and policy series*. London: Earthscan Publications.

Slovic, P. 1987. "Perception of risk." *Science* 236(4799): 280–85.

Slovic, P., B. Fischhoff, and S. Lichtenstein. 1986. "The Psychometric Study of Risk Perception." In: *Risk Evaluation and Management*, edited by V. Covello, J. Menkes and J. Mumpower, 3-24. Springer: US.

Slovic, P., B. Fischhoff, and S. Lichtenstein. 1985. "Characterizing Perceived Risk." In: *Perilous progress: Managing the Hazards of Technology*, eds R.W. Kates, C. Hohenemser, and J.X. Kasperson, 91-125.Westview. Available at SSRN: http://ssrn.com/abstract=2185557

Strickland, L.S., and L.E. Hunt. 2005. "Technology, security, and individual privacy: New tools, new threats, and new public perceptions." *Journal of the American Society for Information Science and Technology* 56(3): 221-34.

Timan, T., and N. Oudshoorn. 2012. "Mobile cameras as new technologies of surveillance? How citizens experience the use of mobile cameras in public nightscapes." *Surveillance & Society* 10(2): 167-81.

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.

Wynne, B. 2006. "Public engagement as a means of restoring public trust in science,hitting the notes, but missing the music?" *Public Health Genomics* 9(3): 211-20.