Theoretical/research paper

P | U | S

Public Understanding of Science
1–17

DOI: 10.1177/0963662517702321
journals.sagepub.com/home/pus
SAGE

Beyond the security paradox: Ten criteria for a socially informed security policy

Vincenzo Pavone
Institute of Public Goods and Policies (IPP) – Consejo Superior de Investigaciones Científicas (CCHS-CSIC), Spain

Kirstie Ball
University of St Andrews, UK

Sara Degli Esposti
Universitat Oberta de Catalunya, Spain

Sally Dibb
Coventry University, UK

Elvira Santiago-Gómez
Universidade da Coruña, Spain

Abstract
This article investigates the normative and procedural criteria adopted by European citizens to assess the acceptability of surveillance-oriented security technologies. It draws on qualitative data gathered at 12 citizen summits in nine European countries. The analysis identifies 10 criteria, generated by citizens themselves, for a socially informed security policy. These criteria not only reveal the conditions, purposes and operation rules that would make current European security policies and technologies more consistent with citizens' priorities. They also cast light on an interesting paradox: although people feel safe in their daily lives, they believe security could, and should, be improved.

Keywords
acceptability, privacy, public participation, security, technology

Corresponding author:
Vincenzo Pavone, Institute of Public Goods and Policies (IPP) – Consejo Superior de Investigaciones Científicas (CCHS-CSIC), Calle Albasanz, 26-28, Madrid 28037, Spain.
Email: vincenzo.pavone@csic.es

1. Introduction

Over the past 20 years, but especially since 9/11, security policies in Western societies have increasingly adopted pre-emptive measures which are reliant on surveillance-oriented security technologies (SOSTs). This shift has had controversial consequences, with scholars highlighting a variety of concerns they associate with pre-emptive security and surveillance practices (De Goede, 2014; De Goede and Randalls, 2009; Hoijtink, 2014; Pavone and Degli Esposti, 2012). As new SOSTs facilitate the collection, storage, processing and combination of personal data by security agencies and commercial organisations, their impact on established civil and political rights (Friedewald et al., 2010), social sorting (Lyon, 2007b; Strauss and Nentwich, 2013) and individual privacy (Lyon, 2002)[1] has been criticised.

With so many concerns raised by technologies over which citizens have little control, it would be reasonable to expect Public Engagement with Science (PES) studies to have scrutinised how people assess these technologies and their implementation. However, SOSTs have so far received relatively little attention (Martin and Donovan, 2014; Pavone and Degli Esposti, 2012). Inspired by an unquestioned acceptance of the trade-off between privacy and security, early studies have rather considered the extent to which citizens are willing to trade their privacy in exchange for greater security (Bowyer, 2004; Jain et al., 2005; Strickland and Hunt, 2005). More recent studies have focused on the decision-making process involved in the development and implementation of SOSTs (Friedewald et al., 2017; Hempel et al., 2013; Van Lieshout et al., 2013; Wright et al., 2014; Wright and Friedewald, 2013).

This study hopes to contribute to this line of inquiry by focusing on an interesting paradox: although people feel safe in their daily lives, they believe security could, and should, be improved. Evidence of this paradox can be found in *Eurobarometer 432: Europeans' attitudes towards security* (European Commission (EC), 2015). The report indicates that although the large majority of respondents consider their countries secure places (89%; $n = 28{,}082$) and agree on saying that their immediate neighbourhood, city, town or village are safe places to live in (82%), a large percentage of them think that security agencies are not doing enough to fight crimes such as corruption (52%), human trafficking (47%), money laundering (46%), drug trafficking (41%) or cybercrime (40%), and that citizens (79%) and citizens' associations (64%) could also help and play a role in safeguarding public security. Furthermore, the majority of European citizens (55%) consider that fundamental rights and freedoms have been restricted as a result of current security policies. This negative perception of the effect of security policies on individual freedoms seems to be worse in 2015 than it was in 2011, when only 48% considered their liberties to have been restricted for reasons related to the fight of crime and terrorism (EC, 2014). These findings suggest that current security policies and solutions are somehow perceived as inadequate by citizens, whose demands, opinions and perceptions need to be further explored and included in future security policies. In pursuing this objective, PES studies can stimulate productive and insightful discussion about the politics and purposes of science and technology (Stirling, 2008). They also have a role in producing new and socially responsible knowledge that can underpin innovation (Owen et al., 2012), governance (Macnaghten and Chilvers, 2014) and policy-making (Hagendijk and Irwin, 2006; Jasanoff, 2003).

Through the adoption of an adapted version of the citizen summit methodology, this article analyses the multiple ways in which citizens interpret security and privacy and assess and evaluate SOSTs. Drawing from qualitative data gathered at 12 citizen summits in nine European countries, this article presents 10 general criteria used by citizens to assess the adequacy of SOSTs. On one hand, the analysis confirms the appropriateness of policy actions undertaken in the area of data protection; on the other hand, it also suggests alternative normative and procedural principles,

which could be adopted in the design, deployment and management of security technologies and that can increase the acceptability of future security solutions.

2. Exploring SOSTs from a public engagement perspective

Over the past 20 years, the concept of security has undergone multiple reformulations. It has shifted from territorial integrity and national sovereignty to human security and, after 9/11, to a new concept of homeland security. New security policies have particularly encouraged pre-emptive security measures, enacted through the development of data-intensive security technologies and public–private security collaboration. These measures have been introduced within policy frameworks which justify the restriction of individual privacy and freedom – a matter of political concern (Beck and Lau, 2005; Cohen, 2014; Friedewald et al., 2010; Lyon, 1994, 2007a; Richards, 2012). Some scholars argue that new holistic security policies suffer from a democratic deficit (Eriksen et al., 2003; Tonra, 2011; Zwolski, 2012); they also tend to reduce democratic scrutiny in other policy domains by framing social problems as security problems (Balzacq, 2008, 2010; Huysmans, 2000, 2006; Loader, 2002). Several studies have shown how the security agenda increasingly constructs migration, crime and social integration as existential threats, addressing them in very narrow security terms and shifting attention away from the role played by social, political and economic factors (Boswell, 2007; Dover, 2008; Karyotis, 2011; Léonard, 2010).

Security solutions which rely heavily on digital surveillance have been especially criticised for different reasons. First, they privilege pre-emptive approaches based on pattern discovery over forms of targeted and historically motivated tracking (Lyon, 2014). Furthermore, their impact on crime reduction is contested (Welsh et al., 2015) and can encourage crime displacement (Johnson et al., 2012). Finally, more recent studies of privacy concerns demonstrate that most people feel resigned and powerless when confronted with the current reality of mass dataveillance (Degli Esposti, 2014; Turow et al., 2015).

Despite the relevancy of the topic and the need to investigate public assessment of security technologies, most studies in the area suffer the limitations of having replicated policymaker discourses concerning the existence of a trade-off between privacy and security (Strickland and Hunt, 2005). In framing security and privacy as interchangeable goods, these studies have not explored, for instance, whether security technologies actually address citizens' security needs and priorities (Jain et al., 2005), how privacy is conceptualised or whether citizens actually frame the latter in opposition to security (Strickland and Hunt, 2005). Furthermore, these studies have contributed to perpetuate security policies that considerably reduce privacy without offering significant gains in security (Mitchener-Nissen, 2014; Pavone et al., 2016). In fact, studies based on the privacy-security trade-off inevitably require citizens to decide which liberties could be sacrificed to meet security needs (Bowyer, 2004).

This article tries to overcome these shortcomings by applying an adapted version of a specific type of public engagement method, the citizen summit (Bedsted et al., 2011). Public engagement exercises have proved effective in increasing democratic participation and raising awareness. However, they have also been criticised as the data gathered are often not sufficiently robust to feed scientific research and guide policy development (Sturgis, 2014; Sturgis and Allum, 2004). In this respect, public opinion surveys have been more successful in collecting reliable quantitative data, but their success came at the expense of public participation and debate (Macnaghten et al., 2005). Moreover, survey methods tend to gather opinions related to a predetermined set of options and scenarios, while the conceptual and analytical dimensions that underpin these opinions remain out of sight and alternative views can be marginalised. Not unexpectedly, only a few studies within this literature have specifically explored the social, ethical and cultural criteria

adopted by different publics to assess the acceptability of technologies and innovations, such as future energy options (Butler et al., 2015; Zoellner et al., 2008), waste management (Garnett and Cooper, 2014), health policy issues (Street et al., 2014) or electricity grid options (Schweizer and Bovet, 2016).

Innovative public participation methods adopted in the study of surveillance technologies allow to create new space for discussion and negotiation, where divergences and conflicts are not silenced (Hempel et al., 2013). New societal impact assessment methodologies, for instance, feature ethical dilemma scenarios to assess the ethical, social and other implications of SOSTs (Wright et al., 2014; Wright and Friedewald, 2013). On this basis, attempts have been also made to develop decision support systems capable of reconciling security and privacy (Van Lieshout et al., 2013).

In our study, the citizen summit, a traditional public engagement method, has been specifically revised to allow participants to frame the issue of how to assess the acceptability of SOSTs in their own terms and express informed opinions after having had the chance of discussing the topic with other people attending the event. This new version of the citizen summit combines informed engagement with deliberative participation, enabling a two-way exchange of knowledge and expertise: from scientific experts and/or policymakers to citizens, and from citizens to experts and/or policymakers. Reconciling public participation and deliberation with the needs to gather reliable scientific data, our study casts light on the normative and procedural criteria adopted by European citizens in assessing the acceptability of three specific SOSTs, which are deep packet inspection (DPI), geolocalization through smart phones and smart closed-circuit television (CCTV).

3. Data gathering procedure and analysis

This study applies an adapted version of the citizen summit method to collect both quantitative and qualitative data. Between January and March 2014, 12 summits took place in nine European Union (EU) countries,[2] each of which was attended by around 200 participants (see Table 1). The recruitment strategy was inspired by the principles of maximum variation sampling (Creswell, 2013). In order to achieve the broadest variety of opinions, each country's sample represented the local socio-demographic breakdown.[3]

In order to make sure that participants were familiar with the use, functions, benefits and limits of the SOSTs under consideration, they had received an information magazine, which includes a summary of the European Security policy, and focused on the use, functions, benefits and limits of the SOSTs[4] under consideration, prior to attending the event. A short film about each SOST was also shown at the summit.[5]

Each summit was a daylong event which was divided into three sessions. Upon arrival, participants were placed in discussion groups. Each summit featured approximately 25 discussion groups, each comprising eight participants, a note-taker and a facilitator. In the two first sessions, participants viewed one of the documentary films, discussed the content in their table groups and then answered questions in plenary using an audience response system. Then, they made policy recommendations concerning security solutions during the third session. The facilitators ensured that the discussion flowed and that all participants expressed their views, while the note-takers wrote down the main arguments discussed by their groups. During each summit, participants discussed two of the three SOSTs explained in the magazine they received before the event (see Table 1).

Four types of qualitative data were gathered: (1) a summary of the participants' discussions as documented by note-takers sitting at each table, including some verbatim quotes; (2) the verbatim transcription of each group's recommendations collected on a standard template by table facilitators; (3) the verbatim transcription of the summit postcards on which participants were encouraged to voice more detailed opinions or dissent;[6] and (4) project reports written by national research

Table 1. Number of citizen summit participants per country.

Country	Invited/registered	Participants	Date and location	SOSTs
Denmark	227	169	18 January, Aarhus	GEO and sCCTV
Hungary	257	215	25 January, Budapest	DPI and GEO
Norway	186	126	1 February, Oslo	DPI and GEO
Spain	220	185	1 February, Madrid	sCCTV and DPI
Italy	250	193	8 February, Florence	sCCTV and DPI
Austria	260	234	22 February, Vienna	DPI and GEO
United Kingdom	400	214	1 and 15 March, Birmingham	GEO and sCCTV
Switzerland	330	254	8 March, Zürich; 22 March, Iverdu; 29 March, Lugano	GEO and sCCTV
Germany	221	190	29 March, Kiel	GEO and sCCTV

SOSTs: surveillance-oriented security technologies; GEO: geolocalization; sCCTV: smart closed-circuit television; DPI: deep packet inspection.

partners, which included details on national controversies related to privacy and security themes and other cultural and contextual information in addition to specific information on the participatory event. The data were analysed using thematic data analysis, which is a flexible method for identifying, analysing and reporting themes within qualitative data (Marshall and Rossman, 2011). An inductive logic was followed. Initially, themes were identified from the analysis of all qualitative data gathered in each country. This approach allowed the identification of recurrent topics in the main arguments expressed by participants in their discussions and in their recommendations. Recurrent themes were identified and grouped within categories called criteria. In the analysis, researchers paid attention to those principles used by citizens when deciding whether or not they consider the security measures to be acceptable. Criteria indicate standards on which a particular judgement or a decision is based; these criteria encompass the legal, ethical, economic and procedural standards consciously used by citizens to explain their views about the acceptability of SOSTs. Drawing from these citizen summits, some scholars have addressed national-specific and technology-specific criteria, providing interesting insights into national approaches to security (Degli Esposti et al., 2017; Degli Esposti and Santiago, 2015). This study, however, specifically addresses European security policy; the main focus, thus, is on the criteria that emerged consistently in all of the countries and which applied to the three technologies. These criteria had been identified first at the country level, and then they were compared across the countries. As a result of the comparison, we identified 10 of these criteria that featured in all of the countries studied. It is these common criteria which form the basis of the discussion in this article. These criteria contribute to a fine-grained exploration of what norms and procedures the participants adopted when assessing the deployment of security technologies. They provide a cogent portrait of how participants experience, frame and assess the SOSTs that are used to enhance European security policy. They also offer a distinctive picture of how participants would revise these security measures if given a chance to shape European security policy.

4. Towards a socially informed approach to security

This article argues that a socially informed approach to the public understanding of security policy needs to go beyond questions of the security/privacy trade-off and address the emerging security paradox. Inspired by the trade-off, previous studies missed the opportunity to surface more rich and nuanced views. In fact, the results of this study demonstrate variability in the notions of privacy and

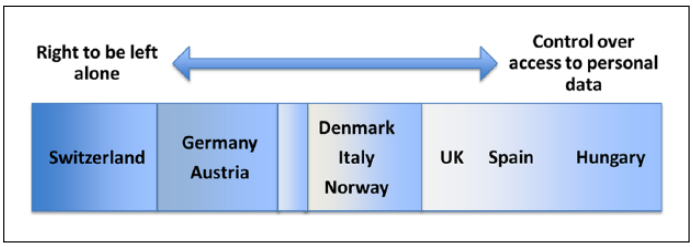

Figure 1. Defining privacy.

security in European comparative perspective, which have not been captured by previous work. Security, for instance, was sometimes understood as personal security, and other times as national security – two aspects of security which do not necessarily converge (Pavone et al., 2016). While the Hungarian and Spanish participants considered SOSTs to be more acceptable if used to improve national security, German and Austrian participants considered their use acceptable only if they increased personal security. Other countries adopted an intermediate position in which SOSTs were considered acceptable as long as they increase both national security and personal safety. However, only smart CCTV was considered effective in improving personal safety, while geolocalization and DPI were considered acceptable only to safeguard national security (Strauss, 2015).

Variation of meaning was also observed in relation to the concept of privacy. Participants in Switzerland, Germany and Austria tended to frame privacy as a right to be left alone, as expressed by a note-taker in Germany:

> Citizens feel a chilling effect on their behaviour, deriving from the wish to be left alone. Many citizens at the summit said that they perceive the increasing use of new SOSTs as the rise of a big brother creating an atmosphere of mistrust already experienced in the German history.

In contrast, participants in Spain and Hungary were more inclined to frame privacy in terms of control over personal data, as expressed in the following note-taker's reflection in Spain:

> […] whilst many participants asked for severe punishment for the security agencies and the commercial actors who break the law, they also asked for a more thorough control over who, why and for what purposes, accesses their information. At the same time, they also asked for better and more extensive access to their own data, wherever they may be stored in order to increase control of their data and their own information.

Participants in other countries adopted an intermediate position, with the United Kingdom positioned closer to Spain and Hungary, and Italy and the Nordic Countries in the middle (see Figure 1).

Furthermore, our study confirms the existence of the paradox emerged in the Eurobarometer (EU Commission, 2015). It was not surprising to find that a large majority of study participants said that they felt safe in their daily life (69%) and considered that their countries were safe places in which to live (66%). Despite feeling safe, the majority of study participants said that SOSTs should be routinely implemented to improve national security (59%), even though they are concerned that the use of SOSTs is eroding their privacy (67%). They suggested that alternative approaches to security, which do not involve surveillance technologies, should be given priority (69%). However, the qualitative methods deployed by the article to capture and analyse participants' criteria to assess SOSTs reveal that there are more nuances to the participants' views and provide interesting insights about the security paradox. The rest of the discussion is, thus, devoted

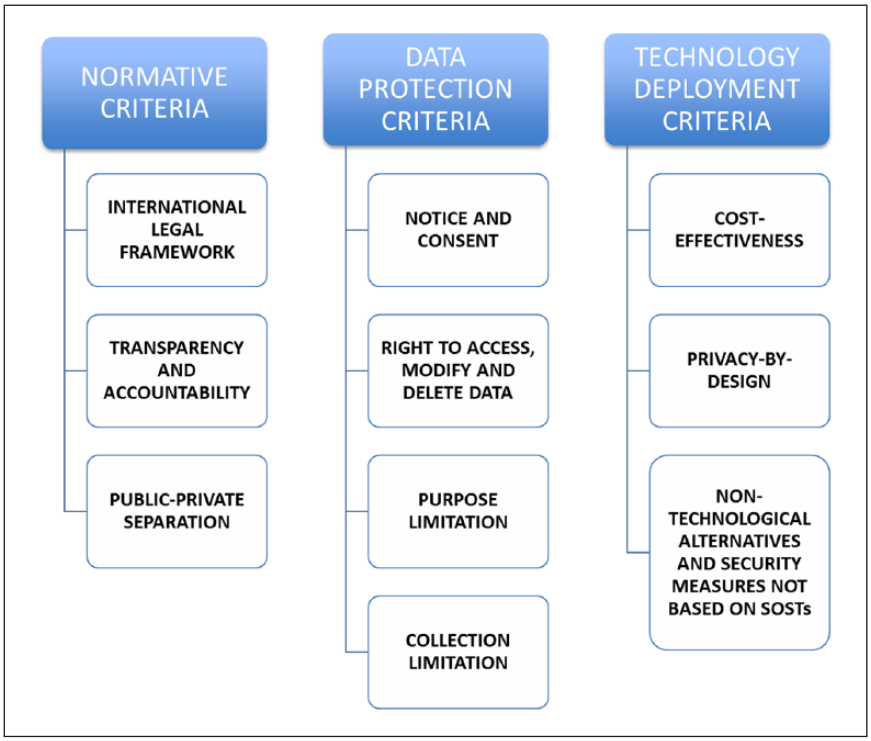

Figure 2. List of criteria.

to the presentation of 10 criteria, which have been identified in all countries where the participatory events were organised.

5. Ten criteria for a socially informed security policy

From the analysis of the qualitative data gathered across the 12 citizen summits, a set of common criteria emerged. These criteria captured the circumstances and principles considered necessary by all participants to implement SOSTs in an acceptable way. They constitute the baseline from which European security policies should be built. The criteria are grouped into three core themes: the first relates to the normative and legal context in which SOSTs operate, the second relates to the fair management and protection of the data used by SOSTs and the third concerns SOSTs design and deployment. Sub-criteria are listed in Figure 2 and presented in detail in the following theme-specific sections.

Normative criteria

The acceptability of SOSTs was often linked to the normative context in which the technologies are operated. National and international regulations, transparency and private–public separation were fundamental criteria used by the large majority of participants to say *how* SOSTs should be managed.

International legal framework. Despite the technical challenges created by ubiquitous computing and trans-border data flow, regulation is still seen by citizens as a powerful mechanism to ensure

that technological risks are contained and managed (Falkner, 2012). International laws are considered necessary to limit the supranational ubiquitous, digital surveillance. Specific laws should also be introduced to reduce massive surveillance and limit the impact of SOSTs beyond national borders: 'we need a new and international legal frameworks … it is important … and even more an oversight body that could intervene if someone broke the law when using deep packet inspection in an illegal way' (Norwegian National Report, p. 17). Given the global nature of security threats and security strategies, the national fragmentation of regulations and data protection authorities was perceived as an obstacle to both security strategies and data protection:[7] 'Legal guarantees should safeguard citizens' rights in the entire EU region. A body at a EU-level must give out licenses to set up surveillance cameras, oversee accountability, and protection of personal data' (Recommendation, Hungarian Citizen Summit).

Transparency and accountability. Many participants perceived that SOSTs are used in situations in which information, transparency and responsibility are poor or missing. They suggested that SOSTs should only be introduced after providing detailed and accessible information about operation modes, operators, rules, domains and purposes to the public: 'the use of SOSTs is opaque, responsible authorities are not known to the public. We need the creation of national agencies to scrutinize both the use of surveillance-oriented technologies and the compliance with legal regulations' (Recommendation, Austrian Citizen Summit).

Citizens demanded more transparency about the actors involved in security operations, their role and level of accountability:

> Organizations, both private and governmental, which collect data, must be open about [data management]. They should state what kind of data they collect and why. Several groups made a concrete suggestion to create a 'My page', where one can see a list of everyone who have stored your personal data, and a log of when it is used. One should also be able to block certain actors from using your personal data. (Norwegian Country report, p. 27)

Information campaigns were proposed as a potential solution to generalised lack of knowledge of data protection legislation and as a way to enhance the overall security accountability chain. Such action would help ensure that clear responsibilities could be identified when things go wrong: 'Transparency here is absolutely essential: people want to know what data are being collected, who is responsible for them and what purposes they are intended for' (Swiss National Report, p. 36). The need to know who is behind security operations to foster accountability was widely recognised: 'We need a law of transparency, as much as we have a law on data protection' (Spanish National Report, p. 43). Furthermore, surveillance technologies should only be used when it is necessary: 'evidence is needed before initiating surveillance and greater transparency from companies and authorities on what the surveillance is used for' (Recommendation, Danish Citizen Summit).

Public–private separation. International regulations and transparency of operations were deemed crucial but not sufficient requirements. The involvement of private actors in security operations and in the management and use of SOSTs generated particular anxiety (Zedner, 2006). Participants did not trust for-profit organisations and were not happy to assign to them the responsibility to enact security measures and/or operate security technologies: 'citizens were also concerned about the actors which use surveillance-oriented security technologies, and many tables mentioned the need for oversight bodies to "watch the watchers"'. They suggested the establishment of such bodies on an international or European level[8] (Norwegian National Report, p. 26). Only public bodies

that are independent from political control were considered suitable to perform an oversight role: 'monitoring and protection of personal data must be conducted by public bodies. Outsourcing such services to the private sector should never be an option' (Postcard, Spanish Citizen Summit). People expressed additional concerns related to the use of data gathered by SOSTs for marketing purposes or about the release of people's data to security agencies. The outsourcing of the security function to private firms was considered especially problematic: 'No security services should be outsourced to private companies!' (Postcard, UK Citizen Summit). In circumstances where the involvement of private actors is absolutely necessary, stricter requirements were considered necessary to ensure transparency and accountability.

Data protection criteria

Although participants recognised that informing citizens about the installation and operation of SOSTs might be challenging in the security domain, characterised by high level of secrecy, they considered necessary to inform the public about how security agencies operate and respect people's rights. Information on how data protection rights, for instance, are safeguarded during police investigation can help diminish citizens' concerns about the data privacy. The purpose and conditions under which people's data were processed in security investigations represented a very relevant and controversial theme. Blanket surveillance was especially criticised not only for its impact on privacy and human rights but also for its effectiveness.

Notice and consent. A major source of concern for all participants was the fact of not being aware of being a subject of surveillance. They consider unacceptable that, because of new digital means, people can be constantly monitored without their knowledge:

> Conditions of data gathering must be defined: who, where, when, for what purposes can record data; how long and how they can store those data; who and under what conditions can access those data. Everybody should be enabled to access their own personal data recorded by these technologies. The population must be informed about all these – in a passive form, via leaflets, TV ads, etc., and in active forms. (Postcard, Hungarian Citizen Summit)

Citizens should be notified if they have been part of an investigation and opt-in consent forms should be used whenever possible. When opt-in frameworks are not viable, notification about when, and for what purpose, surveillance is operated needs to be given to help people become aware of these practices:

> Active information obligation for data collectors, public and private, means the citizen is not required to make a demand but rather that who collects data should be obliged to inform the concerned person; what is stored, how long and why at all! E.g. also in form of a yearly report of the data collecting entity, where it is publicly declared for which purpose and how much data is collected. (Recommendation, German Citizen Summit)

Right to access, modify and delete data. When the retrieval of personal data is required for security reasons, citizens considered they should be notified and have the right to access, modify or have their data removed after the investigation ends:

> Uncertainty lies in the fact that we are ignorant of which data are collected, who gathers them and how they are managed. The solution is a specific legislation on new technologies and surveillance. The establishment of a body controlling the use of the data and its processing and mechanisms that enable us to decide whether we want them to go public. (Recommendation, Spanish Citizen Summit)

> The problem I have with CCTV and DPI is who has access to all my information, where is it stored and how long for? Who accounts for it all? (Postcard, UK Citizen Summit)

Purpose limitation. SOSTs should not be used for operating mass government surveillance, but only for targeting clearly defined threats and within the scope of specific investigations. 'Participants argued towards more control of surveillance activities and the demand for justified reasons for surveillance in order to target real suspects and criminals instead of the general public' (Austria National Report, p. 33). Mass surveillance was considered detrimental as it undermines citizens' perceived safety and their trust in security operators:

> By vast dragnet surveillance activities of governmental institutions, the trust in the state would get undermined because citizens perceive themselves subjected to a blanket suspicion. Broad surveillance measures involving large parts of the population are seen as disproportionate function or mission creep. (German National Report, p. 31)

Data collection limitation. Concerns were also expressed on the type of data gathered. Some types of data, such as those related to location or bodily appearance, were considered less sensitive than others, such as those related to personal communication. Similarly, information retrieved in public spaces, such as in public buildings or on the street, was considered less sensitive than the one gathered in private spaces, such as homes. In this respect, it is interesting to notice that the Internet tend to be seen as a private space rather than as a public space. Whenever possible, it was argued, security actions should target the least sensitive data in the least sensitive spaces, as this comment reveals: '[a]t some tables participants expressed that they found location as a less sensitive type of data than for example the content of their communication, which can be accessed through deep packet inspection' (Norway National Report, p. 28). Thus, the implementation of basic data management norms, such as EU data protection principles, was recognised by citizens as an important criterion determining the acceptability of SOSTs:

> We need clear rules concerning the limits on use and collection of personal data by technological means. In particular, it is necessary to establish rules concerning who may access personal data, for how long, under what conditions and for what purposes. (Recommendation, Italian Citizen Summit)

Technology deployment criteria

Concerns about the ways in which technologies are designed and deployed were also addressed by citizens. The cost of developing and implementing new surveillance devices was a highly relevant issue, which was discussed in conjunction with themes related to alternative security measures and solutions to complement or improve SOSTs, such as the adoption of privacy-by-design principles in the design phase.

Cost-effectiveness. Since tax payers' money is involved in the acquisition and deployment of SOSTs, it is not surprising that participants wanted to receive more information about the appropriateness, costs and impact of SOSTs: 'I have no problems with smart CCTV but the use of it, the running costs, the legitimacy and the effectiveness of it needs to be carefully monitored. And the watchers made accountable' (Postcard, UK Citizen Summit). As most of these technologies are developed, implemented and operated by public institutions, the presentation of exhaustive cost–benefit analyses was considered absolutely necessary – 'Is this cost effective? Very concerned about the future' (UK postcard). Others pointed out that SOSTs need to be supervised and operated by qualified staff – 'maintaining the human factor, that is to say, not replacing humans for robots in processes and their uses' (Spanish recommendation).

Privacy-by-design. The idea of privacy-by-design (Cavoukian, 2011) was mentioned as a possible solution to design privacy-preserving SOSTs and, thus, protect citizens' privacy: 'the concept of "privacy by design" was mentioned, hoping that future technology developers would use their knowledge to increase privacy, instead of increasing surveillance' (Norway National Report, p. 23). This idea was captured also in Italy: '… citizens' request for being in control of the personal data processed by SOSTs seems to support the idea of privacy by design currently proposed in policy circles' (Italian National Report, p. 41).

Alternative security approaches. In designing new security solutions, social, cultural and economic causes of crime and terrorism should never be forgotten (United Nations (UN), 2007), and humans should be considered part of the solutions, not only part of the problem. Participants also suggested that SOSTs should be used to support, not to replace, the work of human operators. SOSTs were more favourably seen as part of broader strategies able to tackle the social and economic causes of crime in a non-repressive way. Such strategies should adopt approaches which tackle social inequalities: 'a greater investment against poverty and inequality must be made. No doubt this would prevent a lot of insecurity problems' (Postcard, Spanish Citizen Summit).

The best scenario would be to see technology and social action to work in combination and witness the creation of an efficient, crime-preventing security strategy that respects human rights and works to eradicate the causes of crime in collaboration with local communities:

> When talking about alternatives, we have to keep in mind the characteristics of modern urban life, which can be characterized with alienation that can result in a decrease in social morals. At the same time, we can still observe the power of local communities in this area in smaller towns and villages. (Hungary National Report, p. 36)

> [We need] a clear estimation of the actual need to use these technologies and a realistic evaluation of the threat situation and of the real risks, and appropriately discreet use of security technologies. Alternatives should be sought and in the security sector greater value should be placed on the human factor, i.e. investigating authorities, than on the technologies. (Recommendation, Swiss Citizen Summit)

Alternative security approaches, such as those that reduce social inequalities and limit the surveillance of citizens and their personal data, were also mentioned. Suggestions included the following:

> i) addressing societal injustice and unease, taking care of the environment, investing in harmonious cohabitation, rather than targeting criminals; ii) protecting critical infrastructure at the source, addressing culturally-sensitive issues, such as tax evasion; iii) investing in neighbourhood patrols, or CCTV cameras. (Recommendation, Italian Citizen Summit)

A summary of all criteria identified and discussed in previous sections is reported in Table 2.

Conclusion

Increasing reliance on security policies that use SOSTs has sparked lively debate about their effectiveness, their consequences and their public acceptance. As a result of the increasing surveillance and of the progressive restriction of civil rights triggered by pre-emptive security polices based on SOSTs, several scholars have warned about the implications for democracy and for personal privacy. Surprisingly, however, comparatively few studies in the field of PES have explored how European citizens assess these technologies. An uncritical adoption of the trade-off between

Table 2. SOSTs are more acceptable if ….

Normative criteria	1. International legal framework	*… operated within international or European regulatory framework and under the control of sovra-national regulatory bodies.*
	2. Transparency and accountability	*… operated in a context where transparency about actors involved in security operations and accountability of security operators is guaranteed.*
	3. Public–private separation	*… operated only by public authorities and only for public benefits. The participation of private actors in security operations, such as when security agencies acquire banking data or Facebook data or when security functions are outsourced to private operators, therefore, must be avoided or strictly regulated.*
Data protection criteria	4. Notice and consent	*… citizens are informed and their use can be regulated through an opt-in approach. Whenever possible, their operation needs to be communicated to targeted individuals.*
	5. Right to access, modify and delete data	*… they allow monitored individuals to access, modify and remove their own data.*
	6. Purpose limitation	*… they do not pursue a blanket surveillance approach. After reasonable evidence is gathered, they should only address specific targets, at specific times, in specific spaces and for specific purposes. While their purposes may change, these changes need to be explicitly discussed and publicly approved.*
	7. Collection limitation	*… they target less sensitive data and space, whenever possible, according to criteria and purposes known by the public.*
Technology deployment criteria	8. Cost-effectiveness	*… their benefits largely outweigh their costs, especially in comparison with other non-technological, less intrusive, alternatives.*
	9. Privacy-by-design	*… they incorporate Privacy-by-Design principles.*
	10. Non-technological alternatives and security measures not based on surveillance	*… they work and operate in combination with non-technological measures and social strategies addressing the social and economic causes of insecurity. SOSTs should complement – never substitute – human action and judgement.*

privacy and security by these studies, moreover, has prevented the exploration of alternative frames of analysis, forcing participants in these studies to think how much privacy were they willing to give away in exchange for more security. As a result, scholarly studies have been unable so far to address an emerging security paradox: people keep asking for security improvements while they consider their life and their country safe. Mostly static views of citizens' opinions, these studies shed little light on the reasons and criteria underlying this security paradox.

Relying on revised version of the citizen summit method, this study gathered 10 criteria generally adopted by the participants to the summits in nine European countries to assess the acceptability of some current security technologies, such as smart CCTV, smart phone geolocalization and DPI. Using thematic data analysis, the article discovered different national interpretations of the concepts of privacy and security but detected the emergence of three shared groups of criteria related to (1) the normative and legal context in which SOSTs operate, (2) the protection of the data that SOSTs gather and process, and (3) the design and deployment of SOSTs.

A first key finding is that some of the criteria citizens use to assess the acceptability of SOSTs converge with the principles and criteria currently adopted by national and European security policies. Criterion 1, on international legal framework, for instance, is consistent with the most recent

Regulation (EU) 2016/679, which has established an international legal framework capable of overcoming the boundaries between national Data Protection regulations (EU Council and Parliament, 2016b). Criteria 4 and 5, on notice and consent and on access and management of personal data, are also reflected in more recent Directive (EU) 2016/680, which deals directly with data protection rules for security operators. Similarly, Europol's Data Protection framework compels the agency to comply with data protection principles and to inform affected citizens about the collection and use of their data (Drewer, 2012). Endorsing current implementation of the '*right to be forgotten*', the participants stressed the importance of removing and modifying the data gathered by security agencies once the investigation requiring its collection had ended.

Criteria 6 and 7, on purpose and collection limitation, are also consistent with a recent sentence of the European Court of Human Rights and European Court of Justice, which has ruled against mass surveillance in both the Russian and British contexts, respectively (European Court of Human Rights, 2015; European Court of Justice, 2016). Yet, citizens have also suggested that they should always be notified when under surveillance, *even if this might jeopardise security operations*. Finally, criterion 9 on privacy by design is also in line with recent EU efforts to introduce Privacy-by-Design principles (Danezis et al., 2014) in the General Data Protection Regulation (European Council and Parliament, 2016a).

However, some of the findings of this article suggest that there exist areas where citizens are not satisfied with current security policies and adopt (and suggest) different criteria of implementation and alternative measures. First, criterion 2 on transparency highlights that citizens still perceive a lack of transparency about operation modes, operators, rules, domains and purposes of public security agencies and private security actors. Second, criterion 8 on cost-effectiveness reveals that citizens consider that current SOSTs may not be as cost-effective and that they should complement, rather than replace, human intervention. Furthermore, criterion 3 on public–private separation reveals a mounting anxiety about the implication of private actors in security activities, which has not been sufficiently addressed by current security practices. Last but not least, criterion 10 on the implementation of alternative, non-technological security measures uncovers a deep dissatisfaction with current security policies and technologies not only because these are considered unfit to address the roots and causes of criminal actions but also because they are not operated in combination with non-technological security measures. As a result of these outcomes, the security paradox becomes more comprehensible: participants are not asking for an increased implementation of existing security measures but, rather, for a different implementation of existing and alternative security policies.

This study has important limitations, too. The results of the citizen summits do not proceed from a statistically representative sample of the population and have been organised around three specific security technologies. While the results cannot be immediately generalised to the countries and to other technologies, many of the criteria gathered, however, are sufficiently broad to be tested in future studies with different samples, countries and technologies. Despite these limitations, our study makes an important contribution to shed light on citizens' perceptions of SOSTs and confirms the important role that participative exercises can play in increasing our understanding of how people frame complex policy issues. Although more research is needed, our findings suggest that citizens' views can effectively help not only to understand the impact of security technologies but also to design socially informed security policies which respect civil liberties without losing their required effectiveness.

Acknowledgements

We would like to thank Pilar Caballero for her useful comments and suggestions on earlier drafts of the paper she shared with us when visiting the Institute of Public Goods and Policies (IPP) in 2016.

Funding

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This article is based on a research that has been funded by the EU project "SurPriSe: Surveillance, Privacy and Security: A large scale participatory assessment of criteria and factors determining acceptability and acceptance of security technologies in Europe", which received funding from the FP7 program, under the grant number: 285492.

Notes

1. Many of these concerns have been recently confirmed by the scandals and abuses revealed by whistleblowers such as Assange, Snowden and Manning in Landau (2013), Lyon (2014) and Bauman et al. (2014).
2. Each country organised one citizen summit except for Switzerland, which held three citizen summits, and the United Kingdom, which held two citizen summits.
3. For a detailed description of the method please refer Degli Esposti and Santiago (2015).
4. The magazine and an overview of the films can be found at: http://surprise-project.eu/wp-content/uploads/2014/04/SurPRISE-D4.3-Information-material-and-documentary-films.pdf
5. The films can be viewed at: http://surprise-project.eu/dissemination/information-material-from-the-participatory-events/
6. Both the summary of the arguments of the discussion groups and the recommendations and postcards were recorded in the original language of each citizen summit. Postcards and recommendations were translated into English. The main arguments from the discussion groups were analysed according to coding categories agreed among those who eventually wrote the different national reports, which were written and circulated among all of the partners in English.
7. The new European Union (EU) General Data Protection Regulation (GDPR) establishes the creation of such supranational authority.
8. Effectively, European and National security agencies have to comply with the new European Council and Parliament (2016a).

References

Balzacq T (2008) The policy tools of securitization: Information exchange, EU foreign and interior policies. *JCMS: Journal of Common Market Studies* 46: 75–100.

Balzacq T (2010) *Securitization Theory: How Security Problems Emerge and Dissolve*. London: Routledge.

Bauman Z, Bigo D, Esteves P, Guild E, Jabri V, Lyon D, et al. (2014) After Snowden: Rethinking the impact of surveillance. *International Political Sociology* 8: 121–144.

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: 525–557.

Bedsted B, Gram S, Klüver L, Rask M, Worthington R, Lammi M, et al. (2011) The story of Wwviews. In: Rask M, Worthington R and Lammi M (eds) *Citizen Participation in Global Environmental Governance*. Oxon, UK: Earthscan, pp. 30–41.

Boswell C (2007) *The Securitisation of Migration: A Risky Strategy for European States*. Copenhagen: Danish Institute for International Studies (DIIS).

Bowyer KW (2004) Face recognition technology: Security versus privacy. *IEEE Technology and Society Magazine* 23: 9–19.

Butler C, Demski C, Parkhill K, Pidgeon N and Spence A (2015) Public values for energy futures: Framing, indeterminacy and policy making. *Energy Policy* 87: 665–672.

Cavoukian A (2011) Privacy by design in law, policy and practice: A white paper for regulators, decision-makers and policy-makers. Information and Privacy Commissioner, Toronto, Ontario, Canada, August.

Cohen ED (2014) *Technology of Oppression: Preserving Freedom and Dignity in an Age of Mass, Warrantless Surveillance*. New York, NY: Palgrave Macmillan.

Creswell JW (2013) *Educational Research: Planning, Conducting, and Evaluating Quantitative and Qualitative Research*. Upper Saddle River, NJ: Pearson.

Danezis G, Domingo-Ferrer J, Hansen M, Hoepman J-H, Le Métayer D, Tirtea R, et al. (2014) *Privacy and Data Protection by Design – From Policy to Engineering*. Creta: ENISA.

De Goede M (2014) The politics of privacy in the age of preemptive security. *International Political Sociology* 8: 100–104.

De Goede M and Randalls S (2009) Precaution, preemption: Arts and technologies of the actionable future. *Environment and Planning D: Society and Space* 27: 859–878.

Degli Esposti S (2014) When big data meets dataveillance: The hidden side of analytics. *Surveillance & Society* 12: 209.

Degli Esposti S and Santiago E (2015) Acceptable surveillance-orientated security technologies: Insights from the SurPRISE project. *Surveillance & Society* 13: 437–457.

Degli Esposti S, Pavone V and Santiago E (2017) Aligning security and privacy: The case of deep packet inspection. In: Čas J, Bellanova R, Burgess JP, Friedewald M and Peissl W (eds) *Surveillance, Privacy and Security: Citizens' Perspectives*. London: Routledge, pp. 71–90.

Dover R (2008) Towards a common EU immigration policy: A securitization too far. *European Integration* 30: 113–130.

Drewer D and Ellermann J (2012) Europol's data protection framework as an asset in the fight against cybercrime. *ERA Forum* 13: 381–395.

Eriksen EO, Joerges C, Neyer J and Advanced Research on the Europeanisation of the Nation-State (2003) *European Governance, Deliberation and the Quest for Democratisation*. Oslo: ARENA.

European Commission (EC) (2014) *Special Eurobarometer 380: Awareness of Home Affairs*. Directorate-General for Communication. Brussels: EU Press.

European Commission (EC) (2015a) *Eurobarometer "Europeans' Attitude Towards Security." 53: EU Commission, DG Communication*. Brussels: EU Press.

European Commission (EC) (2015b) Special Eurobarometer 432 'Europeans' attitudes towards security'. *Survey co-ordinated by the European Commission, Directorate-General for Communication (DG COMM 'Strategy, Corporate Communication Actions and Eurobarometer' Unit)*. Brussels: EU Press.

European Council and Parliament (2016a) *General Data Protection Regulation*. Brussels: EU Press, pp. 1–88.

European Council and Parliament (2016b) DIRECTIVE (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, Brussels: EU Press, pp. 1–43.

European Court of Human Rights, sentence on Case Roman Zakharov v. Russia, 4 December 2015; European Court of Justice, Sentence of the 21st of December 2016 on case (C-698/15).

European Court of Justice (2016) Sentence of the 21st of December 2016 on case (C-698/15).

Falkner R and Jaspers N (2012) Regulating nanotechnologies: Risk, uncertainty and the global governance gap. *Global Environmental Politics* 12(1): 30–55.

Friedewald M, Burgess JP, Ças J, Bellanova R and Peissl W (2017) *Surveillance, Privacy and Security: Citizens' Perspectives*. London: Routledge.

Friedewald M, Wright D, Gutwirth S and Mordini E (2010) Privacy, data protection and emerging sciences and technologies: Towards a common framework. *Innovation – The European Journal of Social Science Research* 23: 61–67.

Garnett K and Cooper T (2014) Effective dialogue: Enhanced public engagement as a legitimising tool for municipal waste management decision-making. *Waste Management* 34: 2709–2726.

Hagendijk R and Irwin A (2006) Public deliberation and governance: Engaging with science and technology in contemporary Europe. *Minerva* 44: 167–184.

Hempel L, Ostermeier L, Schaaf T and Vedder D (2013) Towards a social impact assessment of security technologies: A bottom-up approach. *Science and Public Policy* 40: 740–754.

Hoijtink M (2014) Capitalizing on emergence: The 'new' civil security market in Europe. *Security Dialogue* 45: 458–475.

Huysmans J (2000) The European Union and the securitization of migration. *JCMS: Journal of Common Market Studies* 38: 751–777.

Huysmans J (2006) *The Politics of Insecurity: Fear, Migration and Asylum in the EU*. New York, NY: Routledge.

Jain AK, Ross A and Uludag U (2005) Biometric template security: Challenges and solutions. In: *Proceedings of European signal processing conference (EUSIPCO)*, Florence, 4–8 September, pp. 469–472. New York: IEEE.

Jasanoff S (2003) Technologies of humility: Citizen participation in governing science. *Minerva* 41: 223–244.

Johnson SD, Guerette RT and Bowers KJ (2012) Crime displacement and diffusion of benefits. In: Welsh BC and Farrington DP (eds) *The Oxford Handbook of Crime Prevention*. New York: Oxford University Press, pp. 337–353.

Karyotis G (2011) The fallacy of securitizing migration: Elite rationality and unintended consequences. In: Lazaridis G (ed.) *Security, Insecurity, and Migration in Europe*. Aldershot: Ashgate, pp. 13–30.

Landau S (2013) Making sense from Snowden: What's significant in the NSA surveillance revelations. *IEEE Security & Privacy* 11: 54–63.

Léonard S (2010) EU border security and migration into the European Union: FRONTEX and securitisation through practices. *European Security* 19: 231–254.

Loader I (2002) Policing, securitization and democratization in Europe. *Criminology and Criminal Justice* 2: 125–153.

Lyon D (1994) *The Electronic Eye: The Rise of Surveillance Society-Computers and Social Control in Context*. Cambridge: Polity Press, John Wiley & Sons Publisher.

Lyon D (2002) Surveillance studies: Understanding visibility, mobility and the phenetic fix. *Surveillance & Society* 1: 1–7.

Lyon D (2007a) Surveillance, security and social sorting emerging research priorities. *International Criminal Justice Review* 17: 161–170.

Lyon D (2007b) *Surveillance Studies: An Overview*. Cambridge: Polity.

Lyon D (2014) Surveillance, Snowden, and big data: Capacities, consequences, critique. *Big Data & Society* 1: 1–13.

Macnaghten P and Chilvers J (2014) The future of science governance: Publics, policies, practices. *Environment and Planning C: Government and Policy* 32: 530–548.

Macnaghten P, Kearnes MB and Wynne B (2005) Nanotechnology, governance, and public deliberation: What role for the social sciences? *Science Communication* 27: 268–291.

Marshall C and Rossman GB (2011) *Designing Qualitative Research*. Thousand Oaks, CA: SAGE.

Martin AK and Donovan KP (2014) New surveillance technologies and their publics: A case of biometrics. *Public Understanding of Science*. Epub ahead of print 6 February. DOI:10.1177/0963662513514173.

Mitchener-Nissen T (2014) Failure to collectively assess surveillance-oriented security technologies will inevitably lead to an absolute surveillance society. *Surveillance & Society* 12: 73–88.

Owen R, Macnaghten P and Stilgoe J (2012) Responsible research and innovation: From science in society to science for society, with society. *Science and Public Policy* 39: 751–760.

Pavone V and Degli Esposti S (2012) Public assessment of new surveillance-oriented security technologies: Beyond the trade-off between privacy and security. *Public Understanding of Science* 21: 556–572.

Pavone V, Santiago Gomez E and Jaquet-Chifelle D-O (2016) A systemic approach to security: Beyond the tradeoff between security and liberty. *Democracy and Security* 12: 225–246.

Richards NM (2012) The dangers of surveillance. *Harvard Law Review* 126: 1934–1965.

Schweizer P-J and Bovet J (2016) The potential of public participation to facilitate infrastructure decision-making: Lessons from the German and European legal planning system for electricity grid expansion. *Utilities Policy* 42: 64–73.

Stirling A (2008) 'Opening up' and 'closing down' power, participation, and pluralism in the social appraisal of technology. *Science, Technology & Human Values* 33: 262–294.

Strauss S (2015) *Citizen Summits on Privacy, Security and Surveillance: Synthesis Report*. Vienna: ITA.

Strauss S and Nentwich M (2013) Social network sites, privacy and the blurring boundary between public and private spaces. *Science and Public Policy* 40: 724–732.

Street J, Duszynski K, Krawczyk S and Braunack-Mayer A (2014) The use of citizens' juries in health policy decision-making: A systematic review. *Social Science & Medicine* 109: 1–9.

Strickland LS and Hunt LE (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: 221–234.

Sturgis P (2014) On the limits of public engagement for the governance of emerging technologies. *Public Understanding of Science* 23: 38–42.

Sturgis P and Allum N (2004) Science in society: Re-evaluating the deficit model of public attitudes. *Public Understanding of Science* 13: 55–74.

Tonra B (2011) Democratic foundations of EU foreign policy: Narratives and the myth of EU exceptionalism. *Journal of European Public Policy* 18: 1190–1207.

Turow J, Hennessy M, Draper NA, (2015, June 26) *The Tradeoff Fallacy: How Marketers are Misrepresenting American Consumers and Opening Them Up to Exploitation*. Available at SSRN: https://ssrn.com/abstract=2820060 or http://dx.doi.org/10.2139/ssrn.2820060

United Nations (2006) *The United Nations Global Counter-Terrorism Strategy*. Geneva, UN: United Nations, pp. 1–9.

Van Lieshout M, Friedewald M, Wright D and Gutwirth S (2013) Reconciling privacy and security. *Innovation: The European Journal of Social Science Research* 26: 119–132.

Welsh BC, Farrington DP and Taheri SA (2015) Effectiveness and social costs of public area surveillance for crime prevention. *Annual Review of Law and Social Science* 11: 111–130.

Wright D, Finn R, Gellert R, Gutwirth S, Schütz P, Friedewald M, et al. (2014) Ethical dilemma scenarios and emerging technologies. *Technological Forecasting and Social Change* 87: 325–336.

Wright D and Friedewald M (2013) Integrating privacy and ethical impact assessments. *Science and Public Policy* 40: 755–766.

Zedner L (2006) Liquid security: Managing the market for crime control. *Criminology & Criminal Justice* 6(3): 267–288.

Zoellner J, Schweizer-Ries P and Wemheuer C (2008) Public acceptance of renewable energies: Results from case studies in Germany. *Energy Policy* 36: 4136–4141.

Zwolski K (2012) The EU and a holistic security approach after Lisbon: Competing norms and the power of the dominant discourse. *Journal of European Public Policy* 19: 988–1005.

Author biographies

Vincenzo Pavone is permanent research fellow, Institute of Public Goods and Policies (IPP), Consejo Superior de Investigaciones Científicas (CSIC). Combining political science and science and technology studies, his work critically addresses security technologies, liberty and democracy in the era of the security state.

Kirstie Ball is professor in Management at the School of Management, St Andrews University, and co-director of CRISP, the Centre for Research into Information, Surveillance and Privacy (www.crisp-surveillance.com). Her research, funded by ESRC, EPSRC, The Leverhulme Trust and EU FP 7, focuses on surveillance in and around organisations and surveillance in society.

Sara Degli Esposti has a PhD in Information Management from the Open University (UK) and is currently research fellow at the Internet Interdisciplinary Institute (IN3), Universitat Oberta de Catalunya (UOC). Her research focuses on privacy attitudes, compliance with European Union (EU) data protection law, cybersecurity, big data and smart technologies.

Sally Dibb is professor of Marketing and Society in the Centre for Business in Society, Coventry University. She has published extensively in the areas of consumer behaviour and marketing. Her inter-disciplinary research is underpinned by an interest in the role of data in addressing societal challenges.

Elvira Santiago-Gómez is lecturer in Communication and Public Opinion at the Faculty of Sociology, Universidade da Coruña, Spain. Her area of expertise is science and technology studies and her research specifically address public engagement and public assessment of science and technology controversies.