



RESEARCH
ARTICLE



OPEN
ACCESS



PEER
REVIEWED

Developing the Citizen Summit Method: Understanding citizens' views on digital surveillance technologies

Sally Dobb *Manchester Metropolitan University*

Kirstie Ball *University of St Andrews Business School*

Sara Degli-Esposti *Institute of Philosophy of the Spanish Research Council (CSIC)*

DOI: <https://doi.org/10.14763/2025.4.2045>

Published: 18 November 2025

Received: 6 March 2025 **Accepted:** 29 July 2025

Funding: FP7 Security, Grant/Award Number: SurPRISE (Surveillance, Privacy, Security) Grant Award Number FP7-SEC-2011-285492.

Competing Interests: The author has declared that no competing interests exist that have influenced the text.

Licence: This is an open-access article distributed under the terms of the Creative Commons Attribution 3.0 License (Germany) which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. <https://creativecommons.org/licenses/by/3.0/de/deed.en>
Copyright remains with the author(s).

Citation: Dobb, S., Ball, K., & Degli-Esposti, S. (2025). Developing the Citizen Summit Method: Understanding citizens' views on digital surveillance technologies. *Internet Policy Review*, 14(4). <https://doi.org/10.14763/2025.4.2045>

Keywords: Mixed-methods, Citizen summit, Deliberative methods, Participatory methods, Surveillance

Abstract: This article demonstrates how the citizen summit was transformed into the 'Citizen Summit Method' (CSM). Citizen summits are growing in popularity in policymaking. In their original form they are used as participatory fora to engage voters in deliberating matters of political and social importance. In their redesigned form, they retain their deliberative character while delivering high quality scientific data for use in policymaking and research. Interdisciplinarity was central to the CSM redesign, which involved the theoretical integration of interdisciplinary constructs into a theoretically derived model. The model ran through the CSMs different elements and ensured they cross-referenced each other, with the resulting research delivering in-depth and nuanced evidence about citizens' views. The CSM was explored in an international study of citizens' views on Digital Surveillance Technologies and whether they would be prepared to trade off privacy for security. The results showed that citizens did not perform a security–privacy trade-off and that institutional trustworthiness determined their support or opposition to digital surveillance. The CSM has huge potential for application in internet governance, where citizens are affected by many complex, high-risk policy and regulatory challenges. Options for intersectoral collaboration are discussed as well as the limitations of the CSM.

This paper is part of **The craft of interdisciplinary research and methods in public interest cybersecurity, privacy, and digital rights governance**, a special issue of *Internet Policy Review*, guest-edited by Adam Molnar, Diarmaid Harkin, and Urs Hengartner.

ACKNOWLEDGEMENTS

The authors would like to acknowledge the contributions made to this research by Jacob Lora Skjødt and Nanna Engberg Kristensen, who were collaborators at the Danish Board of Technology Foundation at the time the research was conducted.

Introduction

Citizen summits are growing in popularity in policymaking. In their original form policymakers used this participatory forum to poll opinions and engage voters in deliberating matters of political and social importance. Summits have proven effective in engaging publics on issues such as climate change (Jun & Bryer, 2017; Bedsted et al., 2011), immigration policy, health care, environmental issues and the economy (Badger & Quealy, 2019), and have contributed to democratic reform (Fung, 2015). In urban planning, they have addressed the democratic deficit, ensured diverse public input into policy matters and supported the development of citizens' civic skills (Durrant & Cohen, 2023; Grönlund et al., 2022; Beauvais & Warren, 2019). Yet, in their original form, the quality of the scientific evidence citizen summits produce has been criticised (Macnaghten et al., 2005; Sturgis, 2014; Sturgis & Allum, 2004).

This article sets out several methodological enhancements to the original citizen summit format that retain its deliberative benefits while enabling higher-quality scientific evidence to be gathered. These enhancements rely on careful theoretical integration of interdisciplinary perspectives on the phenomena being investigated. This new Citizen Summit Method (CSM) adopts a robust mixed methods approach which can enable interdisciplinary and inter-sectoral research teams to improve their understanding of public responses to policy interventions. The new CSM was developed during a large project in which citizens across nine countries in the European Union (EU) deliberated about the acceptability of using digital surveillance technologies (DSTs) to protect national security. Each event enjoyed a high level of local political support which enhanced their legitimacy.

The new CSM has huge potential for application in internet policy, where citizens are affected by many complex, high-risk policy and regulatory challenges. While the research reported in this article addresses surveillance, a topic within the remit of internet policy (Hintz & Dencik, 2016; Gstrein, 2020), there are many other areas to consider. Examples include online safety (Neudert, 2023), digital inclusion (Carmi & Yates, 2020; Quyoum et al., 2025), and ensuring free and fair democratic elections (Bennett & Lyon, 2019; Bakir, 2021). The privacy and human rights risks for citizens in these policy areas demand high-quality evidence concerning their impact on democratic rights and processes. Given the diverse multi-stakeholder nature and distributed decision-making structure of internet governance (Radu et al., 2024), deliberative research that garners citizens' views can create a robust representative evidence base to drive effective policymaking.

The article begins by describing the study context for developing the method, then it describes the original citizen summit approach before explaining the enhancements made by the new CSM. Finally, the CSM's ability to support informed debate and generate policy recommendations, as well as its limitations and the need for further development, are considered.

1. The study context

The study that developed the CSM gathered citizens' views on how national security and human rights can be protected in a digitised world. Terror attacks across Europe have led to the legal sanctioning and procurement of DSTs, such as smart Closed Circuit Television (CCTV), geolocation tracking, and enhanced communications surveillance as solutions to homeland and international security challenges. These measures polarise opinion among the public, who are expected to trade off their privacy in exchange for promised increased security (European Agenda on Security, 2015).

All DSTs present security benefits and privacy risks (Siegrist & Cvetkovich 2000), yet the idea of a security–privacy trade-off rests on an incentivistic logic which assumes citizens will accept a DST if they believe the security benefits outweigh the privacy risks (Acquisti et al., 2015). This acontextual argument has been criticised for presenting privacy and security as abstract categories rather than as enacted social practices emerging from the interaction between people and their social and institutional contexts (Pavone & Esposti, 2012; Dourish & Anderson, 2006). Prior empirical work has also failed to challenge this trade-off assumption (Strickland & Hunt, 2005) and revealed the need for the complex issues underlying privacy concerns and public scepticism towards DSTs to be better understood (Ball et

al., 2019).

In practice, citizens have little control over whether their data are gathered for national security purposes and the changing institutional context is likely to influence their attitudes toward DSTs (Acquisti et al., 2016; Nissenbaum, 2009). This study captured these underlying dynamics to reveal whether European publics really were ‘trading off’ privacy for security or had other priorities. The CSM was developed to examine citizens’ views on these issues, internationally at scale, by studying the acceptability of DSTs and attitudes towards the security agencies that deploy them (Solove, 2011).

2. Citizen summits: origins of the Citizen Summit Method

Citizen summits originated in the United States’ local government (Moynihan, 2003). In 1999, the new mayor of Washington D.C. worked with the Office of Neighborhood Action and AmericaSpeaks to create a new model of public participation that could contribute to district strategic planning. The 3,000 citizens who attended reviewed a draft strategic plan prepared by the Office of Neighborhood Action. Grouped on tables of ten, they spent over seven hours discussing city-wide priorities, using a networked laptop computer and wireless polling keypads to vote on questions posed at different points in the summit. Trained facilitators helped to promote dialogue and keep the conversations focused. The voting results were immediately displayed on large screens at the front of the room. Following the discussion, each group agreed a message to share through the networked laptop, to which the mayor was able to respond during the summit.

This original citizen summit approach is able to mobilise democratic participation, raise awareness about issues of public importance, engage citizens in open debate to make recommendations directly to policymakers, and facilitate immediate feedback from both policymakers and fellow citizens. These are the hallmarks of deliberative research, in which there is capacity to share and weigh up different arguments, before reaching a decision and making policy recommendations (Leshner, 2003; Wilsdon & Willis, 2004).

Despite their popular use in policy settings, several criticisms of the original summit method require it to be redesigned for use in academic or inter-sectoral settings, where policymakers and academics collaborate in deliberative research. These concerns include the extent to which the original method conforms to social scientific methodological principles and questions about the quality of the gath-

ered evidence (Macnaghten et al., 2005; Sturgis, 2014; Sturgis & Allum, 2004). Citizen summits primarily gather quantitative polling data with simple ‘yes/no’ responses rather than validated scales. The qualitative reasons behind these views are also typically not captured or fed into policy processes (Macnaghten et al., 2005). Participatory theorists have also expressed concern about the extent to which summits are truly participatory. The predesigned formats, procedures, and questions used appear more consultative in nature (Vaughn & Jacquez, 2020). Wider criticisms of deliberative research also apply, including questions about summits’ level of reflexivity (European Commission, 2008); whether theoretical and empirical questions are fully addressed (Jasanoff, 2005; Wynne, 2006); if social empowerment is an inevitable consequence (Harmon et al., 2013); who and how the involved publics are constituted (Felt & Fochler, 2010), and who decides what will be discussed (Stilgoe et al., 2014).

3. Using the CSM to study digital surveillance technologies

Using citizen summits to study public opinion robustly on the polarising issue of DSTs required several elements to be added to the original format. First, research questions, a theoretical model and key variables were identified by theoretically integrating the results of an interdisciplinary literature review. These formal insights underpinned and integrated all aspects of the research design and materials. Second, the CSM’s methodological components were redesigned for use in a deliberative plenary setting, while remaining scientifically robust. Established scales rather than the polling-style ‘yes/no’ questions used in the original summits were used. Third, unlike in the original summit approach, qualitative data were formally gathered to understand citizens’ reasoning on themes linked to the key variables identified through theoretical integration. These elements are set out in more detail below.

3.1 Integrating the methodological components

Citizen summits have four integrated methodological components (see Table 1): (i) *information materials* shared in advance to familiarise citizens with the issues being discussed; (ii) *video vignettes* used as stimulus material to engage citizens in the debate; (iii) the use of citizen *table groups*, supported by a table facilitator, to debate and make policy recommendations; and (iv) an *attitude survey* administered via an audience response system, using polling keypads to instantly capture and relay the data back to citizens, promoting vitality and participation to the proceedings.

In the new CSM these traditional summit components were deconstructed and re-integrated using theoretical integration logic (Poth & Shannon-Baker, 2022). A detailed theoretical model was developed to guide the overall research design and provide crucial connections linking each of the methods (see Figure 1). This theoretical integration took place during the study design and piloting stages to ensure each methodological component supported the others. Common constructs which connected the different methodological components were first identified and then embedded within each component (Poth & Shannon-Baker, 2022; Alavi et al., 2018; Tunarosa & Glyn, 2017).

The interdisciplinary research team whose expertise spanned Science and Technology Studies (STS), Surveillance Studies, Law and Management Studies, first conducted a wide-ranging literature review to identify relevant phenomena of interest which might represent, influence or intervene in the security-privacy trade off. This review integrated constructs and dimensions from across the team's disciplinary interests, as shown in table 2. A further literature review then identified the consequences of the phenomena under investigation and the relationships between them were mapped (Fisher et al., 2021a; Fisher et al., 2021b). For example, those with higher general concerns about security threats and positive general views on DSTs could be more likely to believe DSTs were effective and hence more likely to accept them. The resulting theoretical model, shown in Figure 1, featured the public acceptability of DSTs as the dependent variable (see Table 2), which refers to the extent to which citizens approve of the DST and believe it should be routinely implemented (Sanquist et al., 2008).

The theoretical model explored how the public acceptability of DSTs was influenced by a range of constructs, including: general familiarity with, and attitudes towards, technology; familiarity/attitudes towards different DSTs; perceived intrusiveness/effectiveness of these technologies; perceived temporal, spatial and social proximity of risks associated with their use; perceived trustworthiness of public bodies operating DSTs; and citizens' substantive privacy concerns. Variables concerning the technologies' perceived effectiveness and intrusiveness represented the different sides of the security-privacy trade-off. As these were attitudinal variables, they were not suitable for objectively measuring 'amounts' of security and privacy to be 'traded-off'; rather, they represented the balance of citizens' views on these issues. The subsequent analysis examined whether there was a direct relationship between perceived effectiveness and intrusiveness with the public acceptability of the different DSTs, or whether other variables were influential.

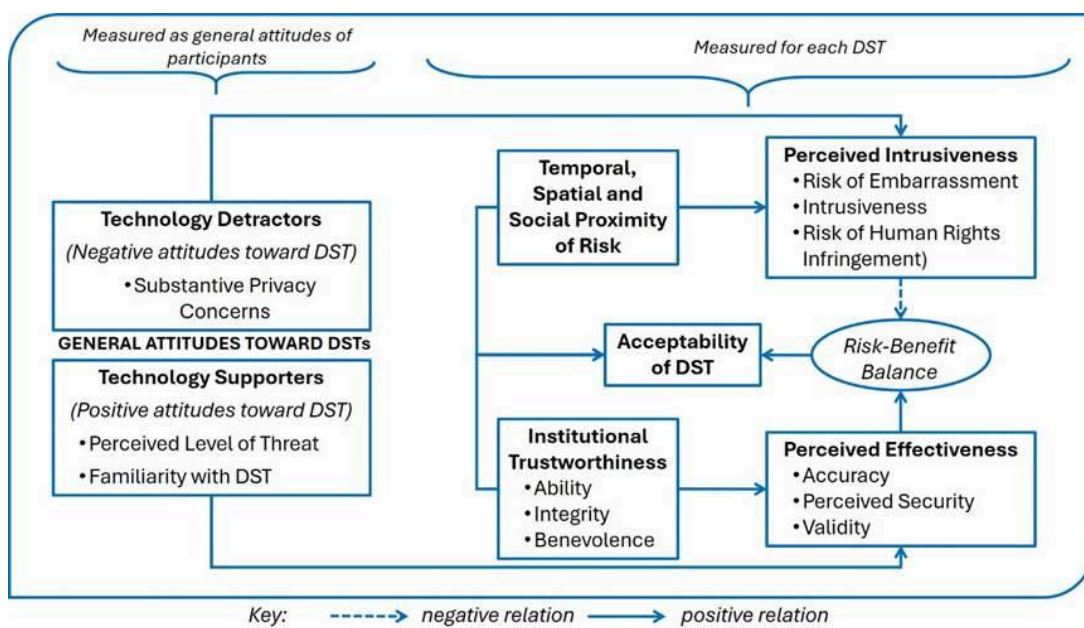


FIGURE 1: Theoretical model of the factors which influence the public acceptability of DST.

Understanding and observing these different constructs required their integration into the different data collection methods used in the summits, with relevant theoretical constructs becoming part of the attitude survey component of the method. Then, it was ensured that these core constructs featured in the table group debates and information materials (see Table 4). The video vignettes and information material were designed to describe these core constructs and set up the matters for debate in the table groups. All material was translated into each participating country's national language¹.

TABLE 1: Citizen summit features

<p>Information materials:</p> <ul style="list-style-type: none"> • Non-technical magazine or booklet that provides information about the issue to be debated, shared in advance of the summit; • Participants encouraged to read the document and bring it with them to the event if they wish; • Offers a balanced view of the issue, including evidence from all sides of the argument.
<p>Video vignettes:</p> <ul style="list-style-type: none"> • Designed to illustrate the phenomena in question, exploring the arguments in a balanced way to provoke debate;

1. The questionnaire was translated by local project partners into Danish, Hungarian, Norwegian, German, Italian, Spanish, Swiss German, Swiss French, Swiss Italian, and Austrian German.

- Enable abstract concepts, such as surveillance, privacy, and security to be brought to life;
- Support a sense of detachment, in which space and time are created for participants to critically reflect upon the issues;
- Provide participants with the opportunity to work through their views by discussing the films with others at the event.

Table groups:

- Tables of eight to ten individuals drawn from mixed socio-demographic groups;
- Format enables the participants to form opinions, share views and debate the issues;
- Interaction and engagement between these individuals and the recommendations which emerge differentiate summits from other mass participation methods;
- Unlike traditional focus groups, the discussion is deliberately free-flowing rather than choreographed according to a structured script;
- Table group facilitator is minimally involved in guiding the discussion but is crucial in capturing participants' recommendations.

Attitude survey:

- Attitude questions are administered via an audience response system that instantaneously captures the data;
- A head facilitator guides the event using a script to help contextualise the questions and provides feedback after each question to maintain interest;
- Each participant uses a clicker to indicate their response to questions displayed on a big screen, the answers from which can then be displayed;
- Certain technical constraints apply, such as limits to the number of questions; the need for short and clear wording; the use of scales that can readily be displayed on the central screen.

During this re-integration of the summit components, care was taken to foreground citizens' voices in the data gathering, while producing internationally comparable, mutually interdependent and individually robust quantitative and qualitative datasets. The questionnaire and table group discussion designs were adapted for this purpose, as were the information materials and video vignettes. These adaptations are described next.

TABLE 2: Elements contributing to the acceptability of DSTs

FAMILIARITY WITH DSTs: Extent to which a person is used to or familiar with a DST. Dimensions (3): awareness of a DST's existence and use; knowledge of how the technology works and is used; habituation – extent to which an individual is 'in touch' with and familiar with DSTs.

Sources: *STS literature*; Slovic et al. (1986); Covello (1983).

GENERAL ATTITUDES TOWARD DSTs: Extent to which someone is in favour of or against the use of technology to foster security. Dimensions (2): technology detractors, reflecting a generally negative belief about technology's ability to enhance security; technology supporters, reflecting a generally positive belief about technology's ability to enhance security.

Sources: *STS literature*; Gaskell et al. (2005).

PERCEIVED LEVEL OF THREAT: Extent to which someone feels endangered by malicious intent. Dimensions (2): personal security, reflecting the extent to which an individual feels safe; public security, reflecting the extent to which their context is safe
Sources: *Risk studies literature*; Bickerstaff et al. (2006); Irwin et al. (1999); Moffat et al. (2004); Sanquist et al. (2008).

PERCEIVED INTRUSIVENESS: Potential invasiveness of the security system and its degree of intrusiveness on individuals. Dimensions (3): the risk of embarrassment of making citizens feel ill-at-ease, uncomfortable, self-conscious or ashamed; the intrusiveness from forcing the system on citizens without invitation or permission; the perceived risk of human rights infringement.

PERCEIVED EFFECTIVENESS: Extent to which a DST is considered to achieve its security goal. Dimensions (3): accuracy with which it identifies risks and is error free; perceived security which results from its introduction; demonstrated validity in addressing the threat and using appropriate data.

Sources: *Risk studies literature*; Sanquist et al. (2008); Renn et al. (1992); Renn (1998); Sjöberg (2000).

TEMPORAL PROXIMITY: Extent to which future negative consequences may arise from a DST.

SOCIAL PROXIMITY: Whether a DST has a well-defined target or treats everyone as a suspect.

SPATIAL PROXIMITY: Extent to which a DST features in the day-to-day experience of a person

Sources: *Risk studies literature*; Bickerstaff et al. (2006); Irwin et al. (1999); Moffat et al. (2004); Sanquist et al. (2008).

INSTITUTIONAL TRUSTWORTHINESS: Extent to which an institution is considered trustworthy. Dimensions (3) include ability to achieve aims; integrity to act in good faith; and benevolence in relation to the citizen welfare.

Sources: *Organisation studies literature*; Mayer et al. (1995).

SUBSTANTIVE PRIVACY CONCERNS: DST's impact on individual privacy including:

PHYSICAL PRIVACY Dimensions (4) include intimacy - the safeguarding of a person's body, feelings and emotions; solitude - the ability to physically withdraw from social interaction; anonymity - the possibility of acting without being identified; reserve - the capacity to maintain confidential communications.

INFORMATION PRIVACY: Dimensions (4) collection - amount of personal data collected; unauthorised secondary use - personal data use for purposes other than for its collected purpose; improper access - personal information is voluntarily or accidentally disclosed to those who should not have access; errors - retention of/reliance on old, inaccurate personal data.

Sources: *Privacy studies literature*; Physical privacy concerns: Finn et al. (2013); Clarke (1997).

Information privacy concerns: Smith et al. (1996); Stone et al. (1983); Bélanger et al. (2002).

ACCEPTABILITY OF DST: The extent to which citizens approve of the DST and believe it should be routinely implemented.

Source: *Risk studies literature*; Sanquist et al., (2008).

3.2 Developing the questionnaire for a deliberative plenary setting

Applying the methods in plenary rather than a one-to-one setting had implications for the interaction between researchers and participants, the questions posed and how the data were gathered. Both quantitative and qualitative elements of the data collection were modified to ensure citizens' ease of participation and that the methods were theoretically mutually interdependent.

In the original citizen summits, the survey questions are displayed on a central screen, responses are recorded on keypads and immediate feedback is given on the same screen. This approach shows how participants' opinions are formed at various points in the event and is crucial to the participatory experience. However, these questions mainly seek simple 'yes', 'no' or 'don't know' answers, partly due to display limitations, but also because traditional summits poll opinions rather than test theoretical models using scaled questions.

For a more theoretically informed approach, the length and style of the survey

questions were modified. To avoid participant fatigue, the attitude survey was limited to around one hundred individual questions, split into shorter sections. Each question and its accompanying Likert scale needed to be clearly visible on the central display screen and easy to read aloud. This means those involving lengthy sentences, using complex or reverse scales, or those requiring trade-offs can be incomprehensible.

The questionnaire development followed an iterative process, involving multiple testing and piloting stages (Gomez et al., 2014). As the original scales were shown to be too complex to use at the summits, the research team rigorously refined these measures. Where possible, to ensure content and construct validity, they consulted with the original authors of the scales. Beginning with the existing scales three researchers iteratively reduced the number of scale items and refined the wording. Further testing was undertaken of the content and wording with other academic and security experts from the research team. The questionnaire, booklet and films were also piloted with members of the public. This rigorous testing of the questions, survey instrument and other materials across nine EU countries, underpins the method's reliability. Table 3 illustrates the process for the trustworthiness questions and shows the original literature scales and the final shortened versions.

TABLE 3: 'Before and after' question development – investigating trustworthiness

'Before': Scales on which the attitude survey questions were based²	
Existing scales include constructs related to how much the institution is trusted, its integrity, benevolence and the extent to which it is trusted.	
<i>Trust</i>	<ul style="list-style-type: none"> • I trust Institution A. • I feel that I would trust Institution A to deliver effective security services. • I feel that I would trust institution A's promises to maintain national security. • I feel that I would trust institution A's behavior to meet my expectations.
<i>Ability</i>	<ul style="list-style-type: none"> • Institution A is capable of meeting its responsibilities. • Institution A is known to be successful at what it tries to do. • Institution A does things competently.
<i>Benevolence</i>	<ul style="list-style-type: none"> • Institution A is concerned about the welfare of citizens. • Citizens' needs and desires are important to institution A. • Institution A will go out of its way to help citizens.
<i>Integrity</i>	

- Institution A would never deliberately take advantage of citizens.
- Institution A is guided by sound moral principles and codes of conduct.
- Institution A does not abuse its powers.

'After': Final questions used in the questionnaire

Questions about the trustworthiness of institutions that instigate or implement DST use.

Security agencies which use <name of DST>...

- are trustworthy;
- are competent at what they do;
- are concerned about the welfare of citizens as well as national security;
- do not abuse their power

3.3 Developing qualitative data collection in the table groups

Turning to the qualitative component, the table group discussions foregrounded citizen voices, open debate, and recommendations as independent qualitative data sources. They also added depth and context to the attitude survey findings. In the original summit method, the table group discussions enabled participants to form opinions and then vote in the plenary poll. For the new CSM, these discussions were modified according to focus group methodology, which can also be readily combined with other methods (Morgan, 1997). The ability of focus groups to explore “processes of attitude formation and the mechanisms involved in interrogating and modifying views” (Barbour, 2008, p. 32) was salient in revealing the reasoning behind the views in the questionnaire and the recommendations.

The trained facilitators ensured different views were exchanged by the diverse table groups, moderating the discussion to ensure consensus in the shared recommendations that were reached (Pinto da Costa, 2021). Although the facilitators did not ask prescribed questions, if the conversation faltered, they used a series of prompts reflecting the constructs in the video vignettes, information material and questionnaire (see Table 4). At the start of each discussion round and before the facilitator opened the debate, each participant completed a template about their views of the benefits and limitations of each DST.

TABLE 4: Extract from the facilitator briefing

The group discussions should allow the citizens to have an open debate inspiring each other with their respective views. This means that you as much as possible should allow the citizens to be in charge of where their discussions take them. Only if the discussion at your table is very narrow or if the citizens have a hard time keeping the discussion going you can prompt their discussion by asking them to comment on the following issues. The goal is **not** that every single one of the following issues is covered during the citizen dialogue but just to have a broad and nuanced debate:

- Why would a DST be effective? What does 'effective' mean?
- What alternatives are available?
- In what way is privacy compromised?
- What are its security benefits?
- What are the consequences if public institutions/private companies use the DST?
- What is this DST doing to society? What kind of society is developing?
- How does it affect the participants' own life, if at all?
- Who is making money and benefiting in an economic sense from these DSTS?
- Laws and regulation: do they work?
- What are the ethical implications (i.e. who or what is harmed)?
- Human rights implications (freedom of speech/movement/association etc.)?

Qualitative data sources included notes taken by table facilitators and dedicated note-takers who captured the argument flow and wrote down memorable quotes. The facilitators also shared written reflections after the event with the research team. These qualitative data were joined with other qualitative data sources generated in the discussions. Participants were encouraged to note their individual thoughts on postcards and 'post' them into a post-box located in the room. At the end of the discussion round, each table group produced a reasoned policy recommendation on a pre-prepared template, which also featured in the project report to the European Commission.

Each qualitative component was transcribed for thematic analysis in NVivo. These data were then coded and analysed to identify recurrent themes and explore the main arguments used (Marshall & Rossman, 2011). Although the amount of background noise precluded verbatim recording of the discussions, this challenge could be addressed by future technological advancement.

3.4 Information materials

The information materials informed participants about the technical features of the DSTs and considered current and potential privacy and security controversies associated with their use. The material was initially written in plain English and was subsequently translated as required by the different study countries. It included an overview of surveillance, privacy, and security informed by academic, legal, and journalistic resources and was illustrated with real-world examples. The purpose, function, benefits, and limitations of each DST in relation to these security and privacy implications were also considered as a way of stimulating debate.

The document progressed through four rounds of internal review to ensure an engaging format, easily digestible information, and well-balanced arguments. One

round of external review involved the project's advisory board, with three rounds of piloting with citizens. The content was proof-read and edited by a professional magazine editor, before being converted into a magazine by graphic designers. The booklet³, which was well-illustrated and prepared to the highest production standards, was mailed to participants before the summits with a letter encouraging them to peruse the content.

3.5 Short films (video vignettes)

The research team collaborated on producing the video vignettes, which integrated the same constructs as the survey and the information materials. Video vignettes are appropriate to use in settings which involve challenging situations, extreme emotions, or questions of ethics or human rights (Caro et al., 2012) and using films favourably compares to similar phenomena when experienced first-hand (Eifler, 2007). An iterative approach driven by theory was taken to the production process. Following Johnson (2000), constructs from the research model underpinning the questionnaire were used as the basis for the film-making.

Experts from industry, regulatory bodies, security bodies, campaign organisations, and academia were interviewed on camera about the uses, benefits, and limitations of each DST to create twelve one-hour interviews. Three seven-minute films were produced, each focusing on one of the DSTs. Content analysis of the interviews was used to distill source material for each film. The films were documentary in style, used high production values and were created by a small company with extensive experience of producing television for the BBC. Five rounds of editing of the raw interviews took place, reducing one hour and 45 minutes of material to seven minutes for each film. Images were then added and copyright clearances obtained. Piloting the films⁴ revealed the need for different national conventions for subtitling or voice overs. Some countries (e.g. Germany, Denmark) accepted subtitles in their respective national languages but in others (e.g. Italy), voice overs had to be recorded. The organisation of summits using the new CSM approach is discussed next, focusing on the specific case of the UK summit.

4. Running the summits

Twelve summits were organised in nine EU countries in North-West Europe (Denmark, Norway, and the UK), Central Europe (Austria, Germany, and Switzerland), and

3. A copy can be provided by the corresponding author on request.

4. DPI film: https://www.youtube.com/watch?v=C_YO-LHOkRQ&feature=youtu.be; SCCTV film: <https://www.youtube.com/watch?v=OaP3L8S0R3A>

Southern Europe (Hungary, Italy, and Spain). In each country, participants' views were sought on two DSTs from a group of three: Smart Closed-Circuit Television (CCTV), Smartphone Location Tracking (SLT), and Deep Packet Inspection (DPI). To ensure equal coverage of all DSTs across the project, the nine countries were grouped into three clusters using Hofstede's cross-cultural framework (Hofstede, 2001) as a guide (see also Grimmelikhuijsen et al., 2013). As Table 5 shows, the DSTs were then considered in at least two of the three countries in each cluster⁵.

TABLE 5: Allocation of DSTs to summit countries

	DST		
	SMART CCTV	DPI	SMARTPHONE LOCATION TRACKING
UK	✓	✓	
Norway	✓		✓
Denmark		✓	✓
Spain	✓		✓
Italy	✓	✓	
Hungary		✓	✓
Germany	✓		✓
Austria	✓	✓	
Switzerland		✓	✓
Total countries	6	6	6
Total participants	1,200	1,200	1,200

3.1 Organisation of the UK summits

The UK summits focused on Smart CCTV and DPI. Since the early 1990s, the UK has used video-based CCTV systems extensively in public spaces, with a further wave of expansion from 2010 of digital or smart CCTV, where a camera collects digital images and matches them to known images in a database. DPI is used by companies, intelligence services, and governments to read the content of communications sent via the internet (Wehner, 2013). At the time of the study, controver-

5. The range of views about security found across the nine countries can be found at https://www.researchgate.net/profile/Elvira-Santiago-Gomez/publication/273399132_Key_Factors_affecting_public_acceptance_and_acceptability_of_SOSTs/links/550038170cf260c99e8f888c/Key-Factors-affecting-public-acceptance-and-acceptability-of-SOSTs.pdf.

sies had emerged over these technologies' use, including in the wake of the Snowden revelations, when internet or surveillance facilitated by DPI led to concerns about privacy.

The summits took place in the UK's second largest city of Birmingham in central England, which is the administrative headquarters of the West Midlands metropolitan county and a major manufacturing, engineering, commercial, and service centre. The city is served by an international airport and has a strong cultural and educational tradition, with four universities located there. The multicultural diversity of its citizens, which is highly representative of ethnically rich Britain, made Birmingham a suitable location. The city has also been at the heart of debate about DSTs, with a public outcry following the dense installation of Automatic Number Plate Recognition (ANPR) cameras in a predominantly Muslim area of the city in 2010 (Isakjee & Allen, 2013).

3.2 Event sampling and recruitment

The two UK citizen summits took place in a city-centre hotel, with citizens recruited by a market research company. Some of those sampled were approached in a busy shopping mall in central Birmingham, others were drawn from the company's contact database or recruited by phone. The sample was strictly representative of the national demographic profiles in terms of age, gender, ethnicity, educational attainment, and occupation (Cresswell, 2013). This composition is designed to reflect the diverse views of the UK population, rather than of any specific group. Although not a representative random population sample, this approach supports a balanced and inclusive brainstorming exercise. The information magazine outlining the issues for discussion was sent to participants, along with the timetable, location, travel, and expenses details. Each participant was offered a £100 shopping voucher as an incentive for participation.

214 participants took part in the UK summits: 105 at the first event, and 109 at the second. 205 (97%) were British citizens. 25% of participants claimed to belong to a minority ethnic group, although some did not reveal their ethnicity. British society is highly multicultural and ethnic groups of South-East Asian or Black African origin account for 14% of the total population of England and Wales. 53% of participants were men and 47% were women; 39% had vocational qualifications, with 17% being university graduates. 47% were employed as managers or professionals, with 37% working in clerical, services, sales or technician roles. The remainder in paid work were employed in craft or trade roles, such as agricultural, fisheries or forestry workers, or were plant or machine operators or assemblers. 42% reported

earnings well below the average annual British salary, although this included retirees. Of the 13% who claimed to earn well over the average, 37% were university postgraduates, 35% were managers or senior officials, and 35% were professionals.

3.3 Registration, timetable, and responsibilities

The scale, length, and complexity of the summits required careful management, with formal training sessions prior to the event with briefing packs outlining each role and responsibility shared within the teams. Each summit required a team of circa 40 staff members, comprising three technical support roles, one head facilitator, one head prompter, one introductory speaker, two floor managers, circa 14 table facilitators and 14 note takers, and three handling registration.

The day-long event was organised into several segments, during which citizens viewed the short films, discussed the content in their table group, answered questions using the voting system, and then listened to feedback in plenary (see timetable in Table 6). Participants were registered, given a unique registration code and issued with a remote-control keypad for use with the audience response system. They were allocated to table groups of eight or nine participants, mixed in terms of age, gender, education, and occupational level. Participants were encouraged to spend a few minutes introducing themselves and chatting informally with others at their table, promoting an informal atmosphere and helping to kick-start subsequent discussion.

During the introduction session, the head facilitator described the summit purpose and reviewed the practical arrangements. A short speech by a popular local media broadcaster helped to motivate those attending. Attendance by local or national policymakers or politicians lends legitimacy to the summit. The first voting session followed, in which participants answered questions about their views on security, privacy, and the use of security technologies. These responses benchmarked participants' initial views against which later views could be gauged.

TABLE 6: Summit format and timings

- Introduction [20 mins total]
 - Head Facilitator welcomes participants, explains the summit aims, format, expectations of participants, voting procedures, and practical arrangements.
 - A short motivational speech by a well-known local personality or politician.
- Preliminary Voting Session [30 mins total]
 - Voting on demographic questions with feedback (10 mins).
 - Round-the-table introductions (10 mins).

- Voting on benchmark questions on institutional trustworthiness, perceived level of threat, attitudes towards security technologies and privacy, with brief feedback (20 mins).
- DST Session 1 [90 mins total]
 - Screening of Smart CCTV film (15 mins).
 - Voting on initial Smart CCTV questions (10 mins).
 - Table discussions about Smart CCTV (45 mins).
 - Post-discussion Smart CCTV questions (20 mins).
- DST Session 2 [90 mins total]
 - Screening of DPI film (15 mins).
 - Voting on initial DPI questions (10 mins).
 - Table discussions about DPI (45 mins).
 - Post-discussion DPI questions (20 mins).
- Recommendations Session [45 mins total]
 - Table discussions to agree and write recommendations.
 - Brief feedback.
- Final Questions Session [40 mins total]
 - Voting on 14 general attitude questions with feedback (20 mins).
 - Voting on 8 additional demographic questions (10 mins).
 - Event evaluation questions (5 mins).
 - Closing remarks (5 minutes).
- End of Event

Two 90-minute sessions relating to each of the two DSTs followed. Each began by screening the short film, followed by a table group discussion. The discussion was deliberately free-flowing, and table moderators intervened only to move the conversation forward when needed, or to encourage those who were more reluctant to join in. Participants then used their clickers to answer questions about the DST featured in the film. After each question, the Head Facilitator shared the voting results via a central screen. To foster shared engagement and reinforce the value of citizens' views, some table groups shared their discussions with the rest of the room. The research team created a short film about the summits, which shows how they were administered, the experiences of the participants and the high level of political support they received.⁶

Discussion

The effectiveness of the CSM re-design is demonstrated in three ways: first, by the explanatory power of the mutually interdependent qualitative and quantitative datasets; second by the extent to which the redesigned summits engaged participants with DSTs and the issues raised; and finally, through the generation of constructive recommendations for policy.

6. <https://youtu.be/yIHp4ZUgaGE?feature=shared> (requires YouTube log in).

The new CSM generated nuanced quantitative data which could be subject to more sophisticated multivariate analysis. Accordingly, the relationships between key variables and citizens' reasoning behind it were connected and made visible, recorded, and analysed scientifically. In robustly exploring these relationships and gathering rich qualitative insights, the heterogeneity of different citizen voices and views were more clearly revealed (Ball et al., 2018; Esposti et al., 2021).

Although detailed discussion is beyond the scope of this article, headline findings from the UK summits and snapshots of the quantitative and qualitative data are reported below. These data reveal different heterogeneous responses in how surveillance is experienced. Current research, for example, suggests that ethnic minorities often feel heavily scrutinised and at greater risk of digital privacy harms, while others view DSTs as protective (Quyoun et al., 2025). The mixed-method design captures these contrasting perspectives, while quantile regression of the survey data moves beyond 'average views'. Overall it was found that institutional trustworthiness – rather than the privacy or security aspects of DSTs – crucially shapes whether citizens oppose or support digital surveillance. These relationships hold internationally: European citizens were not directly trading off privacy for security when deliberating about the acceptability of DSTs (Esposti et al., 2021).

The mutual interdependence between the qualitative and quantitative datasets underpinned the effectiveness of the theoretical integration of these mixed methods early in the research design process. The findings associated with Institutional Trustworthiness illustrate this point. The quantitative data gathered via the audience response system showed that 30% agreed that security agencies that use SCCTV are trustworthy, 31% considered them competent, 45% thought they were concerned about citizen welfare and national security, but only 16% considered these agencies did not abuse their power. The figures were similar for DPI, with 31% believing the agencies using this technology are trustworthy, 29% considered them competent, 41% thought they were concerned about citizen welfare and national security, and 12% believed they did not abuse their power. Table 7 summarises the UK summit's Institutional Trustworthiness results.

TABLE 7: Institutional Trustworthiness results from the UK summits

Smart CCTV: Institutional Trustworthiness	Agree %
Security agencies that use SCCTV are	30%
• Trustworthy	31%
	45%
	16%

<ul style="list-style-type: none"> • Competent • Concerned about citizen welfare as well as national security • Do not abuse their power 	
DPI: Institutional Trustworthiness	Agree %
Security agencies that use SCCTV are	
<ul style="list-style-type: none"> • Trustworthy • Competent • Concerned about citizen welfare as well as national security • Do not abuse their power 	31% 29% 41% 12%

The qualitative data gave richer insights into the factors which underpinned these citizen views, with one individual who commented that, *“Someone needs to tell us that it [the data] is really being used for security”* (Male, older); while another argued it *“needs to be made clearer to users who and what is looking at their activities etc. and for what reason”* (Postcard 10). In the same vein, one table group called for: *“the government and security forces to be more open with statistics showing how DPI has benefited us. How many interceptions have taken place?”* Another group complained about the *“... overall lack of communication by all agencies involved [and] lack of consistency between agencies and their procedures and poor response to incidents”*. In the words of one participant: *“...who are they [security agencies] and who do they answer to?”* (Male, older). The vast majority considered that access to this information should only be granted to security agencies or certain government departments, because: *“We need guarantees on who has our information, and we need accountability”* (Female, younger). Most were opposed to the involvement of private sector organisations in national security matters and did not want such firms to operate DSTs or manage the data, as this recommendation stated: *“Personal security has been compromised due to privatization of security services”*. Many wanted to avoid the information being exploited for other purposes, as this citizen emphasised: *“Private companies should not be involved in operating DSTs or have access to the information/data that is produced”*.

Turning now to participant engagement, while the UK participants expressed broad support for DSTs at the end of the summits, they had also scrutinised privacy issues in a new light. 90% believed DSTs help enhance national security. 79% said they had gained new insight into the topics discussed, with 62% believing that the summit generated valuable insights for politicians. Just under half said their attitudes towards DSTs had changed during the summit; with 30% becoming more negative and 15% more positive. These changing views were reflected in citizens’

comments about privacy and how these technologies could affect it. While fears about public privacy rose from 46% to 65%, concerns about personal privacy increased from 35% to 69%. Worries about the use of DPI were greater than about smart CCTV, perhaps because of the ubiquitous and familiar use of CCTV on the UK's streets. 77% of citizens considered Smart CCTV to be an effective security tool, 80% believed it improved national security, with 68% considering the level of intrusiveness associated with the technology were justified. DPI attracted greater criticism, with concerns that it might spy on everyone, irrespective of whether they were doing anything wrong. In the words of one citizen: *"DPI should only be used if you have been charged with a crime not just to look at what your habits are"* (Postcard 14). Table 8 summarises the UK summit's citizen engagement results.

TABLE 8: Citizen engagement results from the UK summits

Question	Agree %
Gained new insight into the topics discussed	79%
The summit generated valuable insights for politicians	62%
Attitude towards DSTs changed during the summit <ul style="list-style-type: none"> • More positive • More negative 	15% 30%
Concern for public privacy <ul style="list-style-type: none"> • At the start of the summit • At the end of the summit 	46% 65%
Concern for individual privacy <ul style="list-style-type: none"> • At the start of the summit • At the end of the summit 	35% 69%
Smart CCTV <ul style="list-style-type: none"> • Is an effective security tool • Improves national security • Levels of intrusiveness are justified 	77% 80% 68%
DPI <ul style="list-style-type: none"> • Is an effective security tool • Improves national security • Levels of intrusiveness are justified 	57% 66% 46%

The summit recommendations also reflected these concerns. Despite having high expectations of national security, British citizens are unwilling to forfeit their personal privacy. This nervousness about DSTs' privacy implications, which included concerns about who might access the data collected, how it might be used, and with what implications, reinforces the paradoxes of the security–privacy trade off. Participants were keen to see more governmental transparency about how information was used and called for greater openness about the benefits and risks of DSTs. They also referenced the need for better regulation and oversight of how DSTs are used. One table group recommended:

“The use of DSTs should be governed by transparent and easy to understand legislation. In order to ensure accountability an independent regulatory body should be established that has responsibility for overseeing the use of DSTs, and which sets rules about handling the gathering of information/data.”

Another recommendation was to: *“form a publicly elected independent either national or worldwide body who monitors and controls the security agencies. Report findings to the public so that we can see who is accessing our data and what they are using it for”*. Speaking specifically about Smart CCTV, one citizen made the following request: *“Do not let CCTV get too advanced so that we end up in 1984, big brother is watching you!”* (Postcard 71). Taken together, these findings show the CSM's capacity to capture quantitative data on citizens' views, in combination with qualitative insights into the thinking behind them.

Conclusion

This article has reported the methodological developments undertaken to create a robust CSM approach to study citizens' views on DSTs. The adaptations respond to concerns about the limitations of the original summit method (Macnaghten et al., 2005) and the dilemmas associated with deliberative methods and participation experiments (Roberts, 2004). Interdisciplinarity was central to the redesign, which involved the theoretical integration of interdisciplinary constructs concerning the acceptability of DSTs. Augmenting the original method with a theoretically derived model ensured the CSM's four methodological elements cross-referenced each other and could be modified, tested, and applied in deliberative plenary settings. By uncovering the factors shaping citizens' views the data clarified citizens' concerns beyond the security–privacy trade-off (Pavone et al., 2018). Recommendations were delivered to the European Commission in a series of country reports and an aggregated report which featured statistics and qualitative data analysis

(SurPRISE 2015).

The article provides a template for those seeking to pursue high quality deliberative policy research involving the public. We recommend wide ranging cross-disciplinary literature reviews to identify variables which may explain differences in public attitudes towards policy matters and generate deliberation about them. Inclusive dialogue about what those variables might be, involving both researchers and policymakers, should focus on the purpose of the research rather than on disciplinary boundaries. The selected variables and the relationship between them then need to be modelled and incorporated into the CSM's main elements: attitude survey, table group discussions, information materials, and short films. Exhaustive testing for the plenary deployment of data collection instruments is crucial. Subsequent analyses will then be able to explore heterogeneity in responses across citizen groups and the reasons for it.

While this article focused on the acceptability of DSTs and featured some technologies which have since been superseded, the CSM can be deployed where public deliberation of internet policy matters is warranted. The variables explored have relevance when considering internet policy areas including online safety, free and fair elections, and the digital divide as well as digital surveillance. In all of these cases, institutional trustworthiness, the impacts on security or implications for privacy or other human rights matters are relevant. Other variables can be added. Drawing on insights from urban planning and addressing the democratic deficit, the CSM method could more avowedly incorporate policymakers not only into the events themselves but also in research design and implementation as co-creative partners within intersectoral research teams. High level support from policymakers contributed to the success of the research described in this paper.

The CSM still has room to develop into an inclusive and deliberative tool which may generate robust evidence about some of the most complex issues of our times. The overt use of a theoretical model to integrate and mix the methods still risks marginalising the inductive element in data collection and interpretation, even though the table group element is more free form. In this way the CSM still tends towards the more consultative form of participatory research in that its conceptual boundaries are preset and not defined by the participants (Vaughn & Jacquez, 2020). To overcome this limitation, a further recommendation includes using the CSM as a component in longitudinal participatory research in which participants determine an agenda to be scaled up or implement their results in a wider participative policy process.

References

- Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, *347*(6221), 509–514. <https://doi.org/10.1126/science.aaa1465>
- Acquisti, A., Taylor, C., & Wagman, L. (2016). The economics of privacy. *Journal of Economic Literature*, *54*(2), 442–492. <https://doi.org/10.1257/jel.54.2.442>
- Akter, S., D'Ambra, J., & Ray, P. (2011). Trustworthiness in mHealth information services: An assessment of a hierarchical model with mediating and moderating effects using partial least squares (PLS). *Journal of the American Society for Information Science and Technology*, *62*(1), 100–116. <https://doi.org/10.1002/asi.21442>
- Alavi, M., Archibald, M., McMaster, R., Lopez, V., & Cleary, M. (2018). Aligning theory and methodology in mixed methods research: Before Design Theoretical Placement. *International Journal of Social Research Methodology*, *21*(5), 527–540. <https://doi.org/10.1080/13645579.2018.1435016>
- Arrindell, W. A. (2003). Culture's consequences: Comparing values, behaviors, institutions, and organizations across nations. *Behaviour Research and Therapy*, *41*(7), 861–862. [https://doi.org/10.1016/S0005-7967\(02\)00184-5](https://doi.org/10.1016/S0005-7967(02)00184-5)
- Badger, E., & Quealy, K. (2019). These 526 voters represent all of America. And they spent a weekend together. *The New York Times*. <https://www.nytimes.com/interactive/2019/10/02/upshot/these-526-voters-represent-america.html>
- Bakir, V. (2021). Media regulation and policy. In *Media studies. Text, production, context* (pp. 250–302). Routledge.
- Ball, K., Degli Esposti, S., Dibb, S., Pavone, V., & Santiago-Gomez, E. (2019). Institutional trustworthiness and national security governance: Evidence from six European countries. *Governance*, *32*(1), 103–121. <https://doi.org/10.1111/gove.12353>
- Barbour, R. (2007). *Doing Focus Groups*. SAGE Publications.
- Beauvais, E., & Warren, M. E. (2019). What can deliberative mini-publics contribute to democratic systems? *European Journal of Political Research*, *58*(3), 893–914. <https://doi.org/10.1111/1475-6765.12303>
- Bedsted, B., Gram, S., Klüver, L., Rask, M., Worthington, R., & Lammi, M. (2012). The story of WWViews. In *Citizen participation in global environmental governance* (pp. 30–41). Earthscan Publications.
- Belanger, F., Hiller, J. S., & Smith, W. J. (2002). Trustworthiness in electronic commerce: The role of privacy, security, and site attributes. *The Journal of Strategic Information Systems*, *11*(3–4), 245–270. [https://doi.org/10.1016/S0963-8687\(02\)00018-5](https://doi.org/10.1016/S0963-8687(02)00018-5)
- Bickerstaff, K., Simmons, P., & Pidgeon, N. (2006). *Public perceptions of risk, science and governance: Main findings of a qualitative study of six risk cases* [Working paper]. https://www.academia.edu/download/40320120/Public_Perceptions_of_Risk_Science_and_G20151123-31258-ak825b.pdf
- Caro, F. G., Yee, C., Levien, S., Gottlieb, A. S., Winter, J., McFadden, D. L., & Ho, T. H. (2012). Choosing among residential options: Results of a Vignette Experiment. *Research on Aging*, *34*(1), 3–33. [http](http://)

[s://doi.org/10.1177/0164027511404032](https://doi.org/10.1177/0164027511404032)

Clarke, R. V. (1995). Situational crime prevention. *Crime and Justice*, 19, 91–150. <https://doi.org/10.1086/449230>

Covello, V. T. (1983). The perception of technological risks: A literature review. *Technological Forecasting and Social Change*, 23(4), 285–297. [https://doi.org/10.1016/0040-1625\(83\)90032-X](https://doi.org/10.1016/0040-1625(83)90032-X)

Creswell, J. W. (2013). *Educational research: Planning, conducting, and evaluating quantitative and qualitative research*. Pearson Education Limited.

Degli Esposti, S., Ball, K., & Dibb, S. (2021). What's in it for us? Benevolence, national security, and digital surveillance. *Public Administration Review*, 81(5), 862–873. <https://doi.org/10.1111/puar.13362>

Dourish, P., & Anderson, K. (2006). Collective information practice: Exploring privacy and security as social and cultural phenomena. *Human-Computer Interaction*, 21(3), 319–342. https://doi.org/10.1207/s15327051hci2103_2

Durrant, D., & Cohen, T. (2023). Mini-publics as an innovation in spatial governance. *Environment and Planning C: Politics and Space*, 41(6), 1183–1199. <https://doi.org/10.1177/23996544231176392>

Eifler, S. (2007). Evaluating the validity of self-reported deviant behavior using Vignette Analyses. *Quality & Quantity*, 41(2), 303–318. <https://doi.org/10.1007/s11135-007-9093-3>

European Commission. (2015). *The European agenda on security*. <https://www.cepol.europa.eu/sites/default/files/european-agenda-security.pdf>

European Commission. Directorate-General for Research. (2008). *Public engagement in science: Report of the science in society session*. Publications Office. <https://data.europa.eu/doi/10.2777/20800>

Felt, U., & Fochler, M. (2010). Machineries for making publics: Inscribing and de-scribing publics in public engagement. *Minerva*, 48(3), 219–238. <https://doi.org/10.1007/s11024-010-9155-x>

Fisher, K. M., Shannon-Baker, P., Brooksher, K., & Greer, K. (2021). Characteristics of rural STEM clubs and implications for students with disabilities. *Special Education Research, Policy & Practice*, 5. <https://digitalcommons.georgiasouthern.edu/teach-elementary-facpubs/37/>

Fisher, K. M., Shannon-Baker, P., Greer, K., & Serianni, B. (2022). Perspectives of students with disabilities and their parents on influences and barriers to joining and staying in extracurricular STEM activities. *The Journal of Special Education*, 56(2), 110–120. <https://doi.org/10.1177/002246692111054109>

Fung, A. (2015). Putting the public back into governance: The challenges of citizen participation and its future. *Public Administration Review*, 75(4), 513–522. <https://doi.org/10.1111/puar.12361>

Gaskell, G., Eyck, T. T., Jackson, J., & Veltri, G. (2005). Imagining nanotechnology: Cultural support for technological innovation in Europe and the United States. *Public Understanding of Science*, 14(1), 81–90. <https://doi.org/10.1177/0963662505048949>

Gomes, E. S., Degli-Esposti, S., & Pavone, V. (2014). *Key factors affecting public acceptance and acceptability of SOSTs 2.4* (No. 2.4; SurPRISE Project Deliverable). https://www.researchgate.net/publication/273399132_Key_Factors_affecting_public_acceptance_and_acceptability_of_SOSTs

Grimmelikhuijsen, S., Porumbescu, G., Hong, B., & Im, T. (2013). The effect of transparency on trust

- in government: A cross-national comparative experiment. *Public Administration Review*, 73(4), 575–586. <https://doi.org/10.1111/puar.12047>
- Grönlund, K., Herne, K., Jäske, M., & Värttö, M. (2022). Can politicians and citizens deliberate together? Evidence from a local deliberative mini-public. *Scandinavian Political Studies*, 45(4), 410–432. <https://doi.org/10.1111/1467-9477.12231>
- Gstrein, O. J. (2020). Mapping power and jurisdiction on the internet through the lens of government-led surveillance. *Internet Policy Review*. <https://doi.org/10.14763/2020.3.1497>
- Gutwirth, S., Leenes, R., De Hert, P., & Poullet, Y. (Eds.). (2013). *European data protection: Coming of age*. Springer Netherlands. <https://link.springer.com/10.1007/978-94-007-5170-5>
- Harmon, S. H. E., Laurie, G., & Haddow, G. (2013). Governing risk, engaging publics and engendering trust: New horizons for law and social science? *Science and Public Policy*, 40(1), 25–33. <https://doi.org/10.1093/scipol/scs117>
- Hintz, A., & Dencik, L. (2016). The politics of surveillance policy: UK regulatory dynamics after Snowden. *Internet Policy Review*, 5(3). <https://doi.org/10.14763/2016.3.424>
- Irwin, A., Simmons, P., & Walker, G. (1999). Faulty environments and risk reasoning: The local understanding of industrial hazards. *Environment and Planning A: Economy and Space*, 31(7), 1311–1326. <https://doi.org/10.1068/a311311>
- Isakjee, A., & Allen, C. (2013). 'A catastrophic lack of inquisitiveness': A critical study of the impact and narrative of the Project Champion surveillance project in Birmingham. *Ethnicities*, 13(6), 751–770. <https://doi.org/10.1177/1468796813492488>
- Jasanoff, S. (2005). *Designs on nature: Science and democracy in Europe and the United States*. Princeton University Press.
- Johnson, B. (2000). Using video vignettes to evaluate children's personal safety knowledge: Methodological and ethical issues. *Child Abuse & Neglect*, 24(6), 811–827. [https://doi.org/10.1016/S0145-2134\(00\)00135-6](https://doi.org/10.1016/S0145-2134(00)00135-6)
- Jun, K.-N., & Bryer, T. (2017). Facilitating public participation in local governments in hard times. *The American Review of Public Administration*, 47(7), 840–856. <https://doi.org/10.1177/0275074016643587>
- Leshner, A. I. (2003). Public engagement with science. *Science*, 299(5609), 977–977. <https://doi.org/10.1126/science.299.5609.977>
- Macnaghten, P., Kearnes, M. B., & Wynne, B. (2005). Nanotechnology, governance, and public deliberation: What role for the social sciences? *Science Communication*, 27(2), 268–291. <https://doi.org/10.1177/1075547005281531>
- Marshall, C., & Rossman, G. (2011). *Designing qualitative research* (5th ed.). SAGE Publications, Ltd.
- Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *The Academy of Management Review*, 20(3), 709. <https://doi.org/10.2307/258792>
- Moffatt, S., Hoeldke, B., & Pless-Mulloli, T. (2003). Local environmental concerns among communities in North-East England and South Hessen, Germany: The influence of proximity to industry. *Journal of Risk Research*, 6(2), 125–144. <https://doi.org/10.1080/1366987032000078901>
- Monahan, T. (2006). *Surveillance and security*. Routledge. <https://www.taylorfrancis.com/books/9781>

135447281

Moran-Ellis, J., Alexander, V. D., Cronin, A., Dickinson, M., Fielding, J., Sloney, J., & Thomas, H. (2006). Triangulation and integration: Processes, claims and implications. *Qualitative Research*, 6(1), 45–59. <https://doi.org/10.1177/1468794106058870>

Morgan, D. (1998). *The focus group guidebook*. SAGE Publications, Inc. <https://sk.sagepub.com/books/the-focus-group-guidebook>

Moynihan, D. P. (2003). Normative and instrumental perspectives on public participation: Citizen summits in Washington, D.C. *The American Review of Public Administration*, 33(2), 164–188. <https://doi.org/10.1177/0275074003251379>

Nissenbaum, H. (2009). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press.

Pavone, V., Ball, K., Degli Esposti, S., Dibb, S., & Santiago-Gómez, E. (2018). Beyond the security paradox: Ten criteria for a socially informed security policy. *Public Understanding of Science*, 27(6), 638–654. <https://doi.org/10.1177/0963662517702321>

Pavone, V., & Esposti, S. D. (2012). Public assessment of new surveillance-oriented security technologies: Beyond the trade-off between privacy and security. *Public Understanding of Science*, 21(5), 556–572. <https://doi.org/10.1177/0963662510376886>

Pedersen, D. M. (1999). Model for types of privacy by privacy functions. *Journal of Environmental Psychology*, 19(4), 397–405. <https://doi.org/10.1006/jevp.1999.0140>

Pinto Da Costa, M. (2021). Conducting cross-cultural, multi-lingual and multi-country focus groups: Guidance for researchers. *International Journal of Qualitative Methods*, 20. <https://doi.org/10.1177/16094069211049929>

Poth, C. N., & Shannon-Baker, P. (2022). State of the methods: Leveraging design possibilities of qualitatively oriented mixed methods research. *International Journal of Qualitative Methods*, 21. <https://doi.org/10.1177/16094069221115302>

Quyoun, A., Wong, M., Ghosh, S., & Shahandashti, S. F. (2025). *Minoritised ethnic people's security and privacy concerns and responses towards essential online services*. arXiv. <https://doi.org/10.48550/ARXIV.2506.06062>

Radu, R., Nanni, R., & Shahin, J. (2024). New challenges in internet governance: Power shifts and contestation from “within”. *Telecommunications Policy*, 48(5), 102740. <https://doi.org/10.1016/j.telpol.2024.102740>

Renn, O. (1998). Three decades of risk research: Accomplishments and new challenges. *Journal of Risk Research*, 1(1), 49–71. <https://doi.org/10.1080/136698798377321>

Renn, O., Burns, W. J., Kasperson, J. X., Kasperson, R. E., & Slovic, P. (1992). The social amplification of risk: Theoretical foundations and empirical applications. *Journal of Social Issues*, 48(4), 137–160. <https://doi.org/10.1111/j.1540-4560.1992.tb01949.x>

Roberts, N. (2004). Public deliberation in an age of direct citizen participation. *The American Review of Public Administration*, 34(4), 315–353. <https://doi.org/10.1177/0275074004269288>

Sanquist, T. F., Mahy, H., & Morris, F. (2008). An exploratory risk perception study of attitudes toward homeland security systems. *Risk Analysis*, 28(4), 1125–1133. <https://doi.org/10.1111/j.1539-6924.2008.01069.x>

- Searle, R., Den Hartog, D. N., Weibel, A., Gillespie, N., Six, F., Hatzakis, T., & Skinner, D. (2011). Trust in the employer: The role of high-involvement work practices and procedural justice in European organizations. *The International Journal of Human Resource Management*, 22(5), 1069–1092. <https://doi.org/10.1080/09585192.2011.556782>
- Sjöberg, L. (2000). Factors in risk perception. *Risk Analysis*, 20(1), 1–12. <https://doi.org/10.1111/0272-4332.00001>
- Slovic, P., Fischhoff, B., & Lichtenstein, S. (1986). The psychometric study of risk perception. In V. T. Covello, J. Menkes, & J. Mumpower (Eds.), *Risk Evaluation and Management* (pp. 3–24). Springer US. http://link.springer.com/10.1007/978-1-4613-2103-3_1
- Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly*, 20(2), 167. <https://doi.org/10.2307/249477>
- Solove, D. J. (2011). *Nothing to hide: The false tradeoff between privacy and security*. Yale University Press.
- Stilgoe, J., Lock, S. J., & Wilsdon, J. (2014). Why should we promote public engagement with science? *Public Understanding of Science*, 23(1), 4–15. <https://doi.org/10.1177/0963662513518154>
- Stone, E. F., Gueuta, H. G., Gardner, D. G., & McClure, S. (1983). A field experiment comparing information-privacy values, beliefs, and attitudes across several types of organizations. *Journal of Applied Psychology*, 68(3), 459–468. <https://doi.org/10.1037/0021-9010.68.3.459>
- Strickland, L. S., & Hunt, L. E. (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), 221–234. <https://doi.org/10.1002/asi.20122>
- Sturgis, P. (2014). On the limits of public engagement for the governance of emerging technologies. *Public Understanding of Science*, 23(1), 38–42. <https://doi.org/10.1177/0963662512468657>
- Sturgis, P., & Allum, N. (2004). Science in society: Re-evaluating the deficit model of public attitudes. *Public Understanding of Science*, 13(1), 55–74. <https://doi.org/10.1177/0963662504042690>
- SurPRISE. (2015). *Final publishable summary report*. <https://cordis.europa.eu/docs/results/285/285492/final1-final-publishable-summary-report.pdf>
- Tunarosa, A., & Glynn, M. A. (2017). Strategies of integration in mixed methods research: Insights using relational algorithms. *Organizational Research Methods*, 20(2), 224–242. <https://doi.org/10.1177/1094428116637197>
- Vaughn, L. M., & Jacquez, F. (2020). Participatory research methods – Choice points in the research process. *Journal of Participatory Research Methods*, 1(1). <https://doi.org/10.35844/001c.13244>
- Wehner, C. (2013). *Deep packet inspection – Use cases, requirements and architectures*. EE Times. http://www.eetimes.com/document.asp?doc_id=1280856
- Wilsdon, J., & Willis, R. (2004). *See-through science: Why public engagement needs to move upstream*. Demos. <https://sussex.figshare.com/ndownloader/files/41126129/1>
- 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), 211–220. <https://doi.org/10.1159/000092659>

Published by



in cooperation with

