PAR PUBLIC ADMINISTRATION REVIEW

Sara Degli Esposti
Consejo Superior de Investigaciones Científicas (CSIC)
Kirstie Ball
University of St Andrews
Sally Dibb
Coventry University

Research Article

What's In It For Us? Benevolence, National Security, and Digital Surveillance

Abstract: *This article challenges suggestions that citizens should accept digital surveillance technologies (DSTs) and trade their privacy for better security. Drawing on data from nine EU countries, this research shows that citizens' support for DSTs varies not only depending on the way their data are used but also depending on their views of the security agency operating them. Using an institutional trustworthiness lens, this research investigates three DST cases—smart CCTV, smartphone location tracking, and deep packet inspection—that present escalating degrees of privacy risk to citizens. The findings show that the perceived benevolence of security agencies is essential to acceptability in all three cases. For DSTs with greater privacy risk, questions of competence and integrity enter citizens' assessments.*

Evidence for Practice

- Citizens are not necessarily willing to trade privacy for security, as is often assumed.
- For citizens to accept digital surveillance technologies, these technologies must be deployed in ways that reflect benevolence and incorporate community interests.
- For citizens to accept more intrusive digital surveillance technologies, security agencies need to demonstrate integrity and their ability to deliver security benefits.
- Participatory democratic processes can establish the shared values that underpin the use of digital surveillance for security purposes.

Digital Surveillance Technologies (DSTs) are widely used by security agencies[1] in Europe and in the United States to fight crime and terror (Bigo 2016). National governments have often justified digital surveillance to the public on the basis that it is reasonable to trade individual privacy for better national security, dismissing those who oppose DST use as having "something to hide" (Solove 2011). This article challenges this assumption using an institutional trustworthiness lens. It shows that citizens' evaluations of DSTs vary not only depending on how the DST uses their data but also depending on their views of the security agency itself.

Following recent data breach scandals, public concerns about how security agencies generate and use citizens' data suggest that an investigation of this issue is overdue. This article places data use at the heart of its research design, using the concept of data vulnerability to distinguish three DST cases: smart CCTV (sCCTV), smartphone location tracking (SLT), and deep packet inspection (DPI). Data vulnerability refers to the extent to which citizens believe that they will experience harms from how the data generated by DSTs are used (Martin, Borah, and Palmatier 2017). Each of the DSTs examined presents different levels of data vulnerability.

This article finds that the three institutional trustworthiness subscales—benevolence, competence, and integrity—influence the extent to which citizens support or oppose different DSTs, according to the data vulnerabilities they generate. The perceived benevolence of security agencies is essential to citizen perceptions of DST support in all three cases. For the DSTs that provoke greater data vulnerability (i.e., SLT and DPI), questions of competence and integrity enter citizens' assessments. Those who oppose their adoption are particularly concerned about security agencies' integrity (West and Bowman 2016). Quantile regression is used to examine the relationship between the trustworthiness subscales and citizens' perceptions of these DSTs, as it helps unpack the differing views of those who support and those who oppose the technologies. Thus, the study contributes to earlier research examining citizen support for such intrusive technologies (Bromberg, Charbonneau, and Smith 2018) and the related ethical issues.

In addition to these theoretical contributions, the study makes two important methodological

Sara Degli Esposti is a Research Fellow in the *Institute of Public Goods and Policies* (IPP), part of the Spanish National Research Council (CSIC), Honorary Research Fellow in the *Centre for Business in Society*, Coventry University. and teaches Applied Statistics to law enforcement agents in the Security Degree of Nebrija University. She has both academic and professional experience in the field of information privacy, cybersecurity, and digital technology acceptance and is currently the Research Director of H2020 project TRESCA (no. 872855).
Email: sara.degli.esposti@csic.es

Kirstie Ball is a Professor in Management at the University of St Andrews. She is co-director and founder of CRISP, the *Centre for Research into Information, Surveillance and Privacy*, a joint research center between St Andrews, Edinburgh, Stirling and Essex Universities. She is also Research Fellow at the *Surveillance Studies Centre*, Queen's University, Canada and Visiting Professor at the *Centre for Business in Society* at Coventry University. Her research specialisms are surveillance, privacy, and employee monitoring.
Email: kirstie.ball@st-andrews.ac.uk

Sally Dibb is a Professor of Marketing in the *Centre for Business in Society* at Coventry University. Her research explores the role of data in addressing societal and business challenges and has been supported by a range of UK and European funding streams. Sally is a visiting Professor at The Open University and the University of St Andrews. She has served twice as a panel member for the United Kingdom Research Excellence Framework.
Email: sally.dibb@coventry.ac.uk

Public Administration Review,
Vol. 00, Iss. 00, pp. 1–12. © 2021 The Authors. Public Administration Review published by Wiley Periodicals LLC. on behalf of The American Society for Public Administration.
DOI: 10.1111/puar.13362.

contributions. First, it demonstrates the utility of quantile regression as a way of moving beyond average perceptions to reveal the patterns behind polarized views and the factors underpinning them. Second, it responds to the need for increased contextual accuracy in trustworthiness research by adopting a between-case methodology that distinguishes the cases using the concept of data vulnerability (Cvetkovich and Nakayachi 2007).

The next section establishes the theoretical basis for the study and presents the research propositions. The first subsection considers institutional trustworthiness and the public acceptance of DSTs, and the second focuses on data vulnerabilities. A section on methods follows, detailing the cases, research approach, measures, and participant profiles. The last sections discuss the research results and present the implications for policy and practice.

Literature Review and Propositions

All DSTs present security benefits and privacy risks (Siegrist and Cvetkovich 2002). This article questions whether the institutional trustworthiness of security agencies influences citizen support of DSTs given these benefits and risks. The idea of a security–privacy trade-off assumes that citizens will accept a DST if they believe the security benefits outweigh the privacy risks. A major criticism of this argument is that it is a-contextual. It presents privacy and security as abstract categories rather than enacted social practices emerging from the interaction between people and their social and institutional contexts (Dourish and Anderson 2006). Prior empirical studies have challenged this assumption and explored its dynamics (Cayford, Pieters, and van Gelder 2019; Pavone and Degli Esposti 2012; van den Broek et al. 2017). These studies show that the public does not engage in a trade-off, but rather expects the proposed solution to offer both privacy and security. As part of this assessment, institutional trustworthiness plays a key role in raising public support for DSTs, as a recognized component of the national security institutional context at a macro level (Ball et al. 2018). The importance of building trust in law enforcement agencies and in the intelligence community has also been recognized among practitioners (Anderson 2015). This study adds to this line of inquiry, by shedding light on the contribution of the three subcomponents of institutional trustworthiness on public support for using DSTs for national security.

Institutional trustworthiness refers to beliefs about a third party that facilitate "a willingness to depend on [that] party in a situation of risk" (Akter, D'Ambra, and Ray 2011, 100). This definition suggests that there are two aspects of institutional trustworthiness to consider. The first is how the concept's basis, measured by its three subcomponents, varies in its relationship to citizens' evaluations of different DSTs. The second is how the risks associated with DST deployment shape this variation. Using concepts from the public administration and organization literature streams to frame the citizen–institution relationship in the security domain these two aspects of the research question are now considered.

Institutional Trustworthiness and DSTs

Within the significant corpus of public administration research which addresses trust in government (Kim and Lee 2012), the institutional trustworthiness of security agencies has not been examined in any detail. Assessing the concept in the context of DST deployment frames different DSTs as manifestations of security policy. Conceptually, institutional trustworthiness explores the connection between the citizen and the institution, enabling citizens to evaluate institutions and what they stand for (Jackson et al. 2012). Such evaluations go beyond politically entrenched reactions to particular governments or personalities (Levi and Stoker 2000). They are generalized assessments about existing authority structures, public policies, or institutional reforms. Citizens' trustworthiness assessments of institutions thus reflect deeply held, long-term beliefs, dissatisfactions, or concerns and are based on their experiences of the political system of which they are a part.

Examining the relationship between DST deployment and the trustworthiness of security agencies helps indicate the bases on which citizens deem DSTs and, thus, security policy acceptable. This is important for two reasons. First, assessments of low trustworthiness arising from the use of intrusive DSTs have the potential to undermine not only citizens' perceived security and safety but also the functioning of national security as a whole. This issue is especially acute following recent surveillance scandals[2] and the sheer diversity and opacity of nonstate actors in the "security-industrial complex" (White 2012). Second, digital security surveillance targeting particular populations is at odds with conceptions of national security as a public good that benefits all in society and on which many other governance systems rest (Loader and Walker 2007).

Although public administration scholars have not specifically focused on security agencies, previous research has examined citizens' perceptions of civil servants' trustworthiness and the effects of trust on public support for public administration initiatives. For example, trust in local government is an important predictor of support for initiatives such as zoning (Cooper, Gibbs Knotts, and Brennan 2008). Trust between citizens and security agencies fosters mutual cooperation and public acceptance of DSTs in matters of crime and security. For example, previous studies have demonstrated that citizens, including those living in communities from which terrorists seek support, are more inclined to cooperate with police officers they perceive to be competent, honest, and benevolent (Tyler and Fagan 2008). Thus, citizens assess the competence and warmth of bureaucrats and react accordingly (de Boer 2020).

Other studies, which address citizens' acceptance of body worn cameras (Bromberg, Charbonneau, and Smith 2018) and drones (West and Bowman 2016), show that ethical concerns around DSTs trigger demands for reassurance on the trustworthiness of DST operators. To be deemed trustworthy, an institution needs to show caring commitment to act in the interests of citizens, an ability to do the job well, and a capacity to act with integrity. According to Mayer, Davis, and Schoorman (1995), benevolence, competence, and integrity are interpreted as three contrasting belief systems with which citizens evaluate the trustworthiness of institutions. Exploring how each of these belief systems applies to the deployment of DSTs breaks important new ground in the study of national security.

Benevolence. Benevolence-based trustworthiness assessments are premised on the public's belief that the security agency understands the community it is serving and is willing to act in its interests (Tyler 2005). In this sense, the DST is deployed to protect all in society, however, defined. In law enforcement research, for example, this normative belief system is founded on a collective understanding of group interests and a shared commitment to social order between citizens and police, which motivates police to protect the interests of the community (Jackson et al. 2012). A benevolence-based trustworthiness assessment also indicates that citizens believe law enforcement agencies are interested in the well-being of the community and that their resources are distributed fairly across society (Tyler and Fagan 2008). Low benevolence could result in the agency being deemed as acting opportunistically in the interests of a few privileged parties, rather than protecting the public as a whole. Furthermore, low benevolence could signal perceived relational failure, in that the institution has failed to anticipate how stakeholders would view their intentions (Frederickson and Hart 1985). One example of the importance of benevolence is demonstrated by the observation that when the ethnic makeup of police officers reflects the diversity of the communities served—a phenomenon dubbed "black in blue"—law enforcement agencies tend to be perceived as having greater legitimacy than otherwise (Sounman 2017; Tyler, Schulhofer, and Huq 2010). The prevalence of group-based targeting in digital security surveillance potentially places benevolence at the core of citizens' concerns about the use of DSTs—a phenomenon exemplified by the experience of "flying while Muslim" (Blackwood, Hopkins, and Reicher 2015).

Competence. Citizens' trustworthiness assessments of security agencies premised on competence rest on an instrumentally rational belief system, in which citizens seek maximum utility from the DST deployment (Meško and Tankebe 2014). Citizens thus prioritize competence out of self-interest. Instrumental rationality is also the belief system that underpins the security–privacy trade-off (Solove 2011). In the law enforcement context, citizens judge agencies as competent if they perceive that they control crime effectively. Research reports international variation in the importance of competence-based trustworthiness assessments of agencies such as the police. Eastern cultures consider competence more important in their assessments, as do postcolonial societies where institutions are emerging from authoritarianism and corruption (Tankebe 2008). Nonetheless, in such cases competence tends only to dominate in the short term (Meško and Tankebe 2014), as trustworthiness has a basis beyond performance indicators. Longer-term trustworthiness rests on the normative dimensions of benevolence and integrity, which indicate principled authority. In practical terms, low competence indicates perceived operational failure, which may stem from political, social, legal, or economic changes to actions carried out by suppliers; poor strategic decision making; or low technical capability (Grimmelikhuijsen and Meijer 2014).

Integrity. Trustworthiness assessments based on integrity are premised on the public's belief that the institution adheres to an acceptable set of moral values (Hough et al. 2010). Low integrity indicates that citizens perceive an institution as having failed to act according to an appropriate set of values. In integrity-based trustworthiness assessments, citizens are concerned with whether the security agencies share their views about right and wrong, has the same moral compass (known as "value congruence"), and will not abuse its power. If citizens believe that law enforcement agencies are acting morally, the power bestowed on it is justified. These beliefs are influenced by the consistency of the institution's past actions, credible communications, and whether the citizen and the institution share a strong sense of justice. Stance taking is therefore important: deploying a DST that provokes a human rights risk has a bearing on how the public assesses the security agency's integrity. A particular DST can thus signal security agencies' moral and other priorities, and the greater the risk, the greater is the requirement for moral action (Simpson, Harrell, and Willer 2013).

These three belief systems clearly have contrasting foundations: a normative group orientation, instrumental rationality, and a normative moral orientation. Tyler (2005) argues that lasting satisfaction with law enforcement and crime control rests on normative rather than instrumental belief systems, but they also work in tandem. Here, as indicated in the following proposition, these systems are assumed to exert a separate but correlated influence on citizens' views of DSTs.

> **Proposition 1:** Perceived benevolence, competence, and integrity of the security agent will have a separate and distinct positive impact on the acceptability of each of the DST cases.

DSTs and Data Vulnerabilities

Returning to Akter, D'Ambra, and Ray's (2011) definition and the second aspect of the research question, this section considers the risks involved in the relationship between the citizen and the security agency. Although trustworthiness and risk appear mutually interdependent, one way to separate them is to investigate the vulnerability, or felt risk, that citizens experience because of DST deployment. Vulnerability refers to citizens' perception of their potential susceptibility to harm resulting from a particular risk (Martin, Borah, and Palmatier 2017).

As security methods become more "data intensive, data vulnerabilities"—vulnerability to data collection risks, data misuse risks, and subsequent human rights violations—become part of the trustworthiness assessment. Data collection risks include personal exposure, the excessive collection of sensitive information, and malicious use of personal information (Smith, Milberg, and Burke 1996). Data misuse risks include control over data sharing and use by third parties, breaches of confidentiality, unauthorized disclosure, and the dissemination of false information (Solove 2008). Human rights violations involve reduced freedom of speech, association, or expression and self-determination (Sanquist, Mahy, and Morris 2008). Moreover, according to privacy scholars (Nissenbaum 2009), the contexts within which data processing occurs bear their own social norms as to what is deemed acceptable. Therefore, some variation is expected in trustworthiness assessments, as the risks associated with data collection and use vary by the DSTs used. Trustworthiness scholars also confirm the importance of context specificity. Meaningful trustworthiness assessments must be made with respect to specific episodes in particular locales, between closely defined sections of the population, and in relation to the actions of specific institutions (Cvetkovich and Nakayachi 2007).

In addition to specifying context according to the DST risks as set out in the previous paragraph, this research also tests whether trustworthiness assessments vary depending on whether citizens support or oppose their use. As such, the propositions are explored in the context of three contrasting DSTs, each of which present differing data vulnerabilities to the public and may be either supported or opposed. The differences between the DST cases are now explored in terms of their data vulnerabilities to explore how their level of intrusiveness influences citizens' assessments of security agency trustworthiness. One additional assumption is made within the context of the three DSTs studied, as follows:

> **Proposition 2:** The basis of trustworthiness assessments will vary between the DST cases because of the different data vulnerabilities associated with each. Perceived data vulnerabilities will negatively influence people's views on the acceptability of each DST.

Cases and Method

DSTs and Data Vulnerabilities

This article features three DSTs that security agencies use. Each forms an empirical case, for which a context-specific description is set out and used for testing. The DSTs are smart CCTV (sCCTV), smartphone location tracking (SLT), and deep packet inspection (DPI). Each DST is deployed in a wide range of local, national, and international security settings, and each is supplied and supported by a network of technology contractors from the private sector (for more details, see appendix A).

sCCTV is used by homeland security agencies such as the police and national border forces to identify suspicious behavior in specific public spaces, such as airports and roads. Applications of sCCTV range from automatic detection of criminal behavior, to identification of search-listed criminals or unwanted individuals, to the prosecution of traffic offenders (Möllers and Hälterlein 2013). Security agencies use SLT, which can be performed through carrier-assisted surveillance, among other things (Pell and Soghoian 2013), to locate, follow, monitor, and gather evidence on suspects. SLT is used by security services and law enforcement agencies to glean information about the location and movements of the phone user over time. This technology is applied in the investigation of many different types of security threat, from traffic offenses to terror attacks. Finally, DPI is routinely used by security agencies internationally, such as the National Security Agency (NSA) and Government Communications Headquarters (GCHQ), to examine the content of Internet communications to identify criminal activity such as the distribution of child pornography, hate speech, or terrorism (Porcedda 2013). In the United Kingdom, as well as in other countries, a warrant is required to examine the contents of online communications.

Each of these DSTs provokes varying degrees of data vulnerability in the way they expose citizens to data collection risks, data misuse risks, and subsequent human rights violations (see Table 1). First, the sensitivity of information collected by each DST is progressively more severe, with sCCTV being the least severe case because it operates in public spaces (Degli Esposti and Santiago-Gómez 2015) and DPI being the most severe. sCCTV collects images of vehicles and people, comparing them with similar images in a database and then identifying them before passing the details on to security agencies or the police. SLT collects smartphone information about people's movements and location, producing a plethora of metadata that reveal much about their and activities. DPI reveals the content of any communication sent through online means and also dissects network data to extract useful metadata.

Second, the visibility of these data collection to citizens progressively decreases, with sCCTV being the most visible and DPI the most opaque. Citizens thus have progressively less control over their exposure to surveillance. Although the software algorithms running in sCCTV systems are operationally obscure (Introna and Wood 2004), smartphones and sCCTV cameras are still publicly visible, and European data protection laws require citizens to be notified when sCCTV is in operation. In the case of SLT, and despite the various methods to locate these devices, many users know that they can disable geolocalization functions, switch off the phone, and remove the battery to avoid being

Table 1 Summary Characteristics of Each DST

		sCCTV	SLT	DPI
Potential application and security benefit		Most common use is Automatic Number Plate Recognition (ANPR) to identify vehicles that have been stolen, driven without tax or insurance, or committed a traffic offense.	Can be used to obtain evidence against suspected criminals, locate missing persons, and place people at the scene of a crime.	Originally developed to detect viruses and malware, but now also used to manage digital rights, target advertising, and identify dangerous or criminal activity online, such as the distribution of child pornography, hate speech, or terrorism.
Data vulnerability	What information is exposed?	A person's travel movements on roads, in airports, and in other public places available to unknown third parties.	All personal movements of someone carrying a smartphone potentially visible to unknown third parties.	All communications content of someone surfing the Internet potentially visible to unknown third parties.
	Option to control exposure?	In the EU, the presence of CCTV cameras in public space must be declared. Citizens can avoid areas with sCCTV.	It is possible to disable some location-based services and GPS capability on a smartphone, though alternative means exist to geolocate the phone.	Impossible to know when and where DPI is in operation; any communication is potentially subject to DPI.
	Human rights violation?	Discrimination against minority groups (e.g., Project Champion).	Violation of freedom of speech and right to protest (e.g., use of Twitter location data to track Occupy protestors).	Violation of freedom of speech, freedom of association, and right to protest (e.g., quashing dissent in the Arab Spring).

tracked. By contrast, Internet users have no way of knowing if DPI is in operation, unless they have considerable technical knowledge and are aware of the location of the security agency facilities that use it (Clement 2013).

Data

Citizen Summit Events

Data were gathered during 12 citizen summits held in nine European countries in the spring of 2014. In their original form, citizen summits are a forum for public engagement used to inform voters and poll opinions about matters of political and social importance (Migchelbrink and Van de Walle 2020; Moynihan 2003). Citizens invited to participate in these summits tend to represent the composition of the city, region or national context, in which the summit is organized. In Europe, the method was originally applied as part of a global project about biodiversity (Bedsted et al. 2015) because it enabled participants to share and deliberate over different arguments (Burchardt 2014), before reaching a decision about the issue being debated. Deliberative processes have therefore been used to address democratic deficit problems (Nabatchi 2010) and increase public participation in policy decisions (Dean 2017; Roberts 2004).

The type of citizen summit used here combines a participatory ethos with meticulously designed and tested data collection methods, to ensure that participants were familiar with the use, functions, benefits, and limits of each DST, before expressing their views. The individual data-gathering elements were framed to reflect the theoretical underpinning of the propositions (Tunarosa and Glynn 2017), and they confirm the utility of a multimethod approach to assessing public opinion on national security matters (Reddick, Chatfield, and Jaramillo 2015).

The day-long summits were divided into segments in which participants viewed documentary films, discussed the content while seated in table groups, and then answered questions in plenary sessions about their views. Several distinctive features were included to engage the public in debate. First, information about the three DSTs was sent to participants in advance. The information was contained in a magazine, written especially for the empirical work by the authors in an accessible style. The magazine was based on the information collected from a gray literature review and the key informant interviews and set up the contrasting case contexts a priori (Kreissl et al. 2013). The document progressed through four rounds of internal review before publication, to ensure that the information could be easily digested, the format was sufficiently engaging, and the arguments were well balanced. Four additional rounds of external review took place with the project's advisory board and were piloted with citizens.

Second, during the summit, participants viewed a short documentary film about each DST. The films featured extracts from the key informant interviews and information about data vulnerabilities, benefits, and discussion points about the DSTs gleaned from the literature review. Short films are an accepted method for relaying information in which questions with ethical or human rights implications are considered (Eifler 2007). Both the magazine and films, which are publicly available, were translated into 11 European languages.[3]

Third, participants were seated in table groups with a facilitator, to support rich debate that was recorded by a notetaker. Every summit had approximately 25 discussion groups, each with approximately eight participants, a notetaker, and a table facilitator. Participants were assigned to these groups to ensure maximum variation in sociodemographics across tables. This approach is intended to ensure a range of different views feed into the discussion. Qualitative insights generated by the mixed-methods design are reported in Pavone et al. (2017) and in Degli-Esposti and Santiago-Gómez (2015).

Fourth, opinions were gathered using an attitude survey and polling keypads, to enable instant quantitative data capture and instant feedback to the participants. Significant effort was made to ensure that the questionnaire was appropriate for use in a plenary voting setting, with the instrument progressing through four rounds of piloting. Questions were short and simple, with clear wording that avoided double negatives. Multi-item measures for single subscales would have been too repetitive, so a careful choice was made of the measures recorded using a five-point Likert scale. Questions were presented in a logical order so that the head facilitator could share the range of responses in the room. For more details about the questionnaire used see supporting information in Appendix S1.

DST Between-Case Design. The nine countries selected for the data collection cover North (Norway, Denmark, and United Kingdom), Central (Austria, Germany, and Switzerland), and Southern/Eastern (Italy, Hungary, and Spain) Europe. Countries were grouped into simple clusters to maximize contextual variability and to increase external validity. Because each citizen summit was time limited, two of the three DSTs were considered in each cluster, one in the morning session of the summit and one in the afternoon session. Two methods were used to assign cases to clusters and ensure maximum variability in the clusters. First, Hofstede's (2003) criteria (power distance, individualism, masculinity, uncertainty avoidance, long-term orientation, and indulgence) were used, as national culture can affect the relationship among trust in government, its antecedents (Grimmelikhuijsen et al. 2013), and internal dimensions (Schoorman, Mayer, and Davis 2007). Second, the findings of Eurostat survey (Eurostat 2013)—the most recent at the time of the research—helped maximize contextual variability with respect to perceived institutional trust. The country clusters and DSTs captured the variability in the level of trust these countries' citizens had in the police, the legal, and political system, and other people (see appendix A). Each cluster included a mix of high (e.g., Norway) and low (e.g., Spain) trust countries. Guided as closely as possible by the national sociodemographic mix in each participating country, citizens were recruited to ensure variability in sample composition with regard to gender, age, and educational level. Information on the demographic composition of each sample is reported in Table 2.

Measures. As in previous studies (Pavone and Degli Esposti 2012), the dependent variable—public acceptance of DSTs—was measured on a five-point Likert scale to capture the extent to which participants agreed with the following statement: "Overall I support the adoption of [DPI/sCCTV/SLT] as a national security measure." The independent variables were also measured on five-point Likert scales, using previously validated statements from other studies. Questionnaire items based on previous studies served to measure benevolence, competence, and integrity (McKnight, Choudhury, and

Table 2 DSTs Discussed in Each Country and Demographic Composition of Samples

	sCCTV	SLT	DPI
1. Denmark	✓	✓	
2. Germany	✓	✓	
3. Hungary	✓	✓	
4. Austria	✓		✓
5. UK	✓		✓
6. Spain	✓		✓
7. Norway		✓	✓
8. Switzerland		✓	✓
9. Italy		✓	✓
Women	48 percent	45 percent	48 percent
Age: 18–49 years	57 percent	50 percent	52 percent
Education before university	61 percent	48 percent	55 percent
Ethnic minority	17 percent	21 percent	24 percent
N	(1,229)	(1,088)	(1,125)

Kacmar 2002), as well as the level of intrusiveness and effectiveness of the surveillance technologies. In line with previous studies, the control variables included participants' age, gender, education level, understanding of DSTs' functionality, information privacy concerns (Smith, Milberg, and Burke 1996), DSTs' perceived security benefits (Sanquist, Mahy, and Morris 2008), and general perceived level of threat. Additional control variables measuring whether participants belonged to a minority ethnic group, had children living with them, and were familiar with sCCTV systems, smartphones, and the Internet were also introduced in the model.

The dependent variables, independent variables, and covariates in the model reflect individual attitudes—that is, settled ways of thinking or feeling about the issues (Greenwald 2014). As the focus is on measuring the perceptions of participants who had reviewed information about DSTs, relying on self-reported measures was deemed appropriate (MacKenzie and Podsakoff 2012). The public administration literature has criticized survey methods for exposure to common method bias, which can artificially inflate the results and produce false positives caused by correlated measurement errors. However, this problem arises when the independent variable is an individual attitude and the dependent variable is an organizational attribute (Jakobsen and Jensen 2015), so this study is not affected.

Quantile Regression. Quantile regression was used to identify the factors influencing the perceptions of citizens who support the adoption of DSTs versus those who oppose it. Quantile regression is a nonparametric extension of linear regression that models selected conditional quantiles as a function of predictors (Koenker 2005). While conventional regression focuses on the mean, quantile regression can describe the entire conditional distribution of the dependent variable (Hao and Naiman 2007). It has been used in economics to investigate the effect of years of schooling on observed wages, wage structure, and wage premiums for union members (Koenker 2005); in management and in other areas to test, for instance, the effect of various tourist spending factors on low, medium, and high spender behavior (Lew and Ng 2012).

In this study, quantile regression enables a comparison of the views of those who disagree or strongly disagree with the use of each DST, represented in the 25th quantile of the dependent variable distribution, with the views of those who agree or strongly agree, represented in the 75th quantile. By comparing the findings for the 25th and 75th quantiles, the effect of each trustworthiness dimension on the opinions of both opponents and supporters of each DST can be identified. Although a discrete scale measures the dependent variable, continuity is assumed in the dependent variable, based on the size of the sample.

Findings

The results are presented in two parts. In the first, the escalating degrees of data vulnerability associated with each DST are revealed, through the levels of reported participant agreement with alternative statements about the degree of intrusiveness and unease associated with each DST. In the second, the results of the quantile regression are presented.

Perceived Data Vulnerabilities and the Between-Case Design

Each DST presented citizens with escalating degrees of data vulnerability, expressed in terms of exposure of sensitive information, loss of control over that exposure, and perceived vulnerability to human rights violations. Figure 1 displays the level of agreement with the three statements used to measure data vulnerabilities and with statements about the degree of intrusiveness associated with each DST. The average values show an escalation in participants' concerns when discussing sCCTV, SLT, and DPI, respectively, confirming the basis of the between-case design. Citizens were concerned about the individual or collective human rights violations linked to the implementation of the DSTs, with DPI being especially of concern. They also worried about the unintended disclosure of sensitive, personal information, and their lack of control over this risk.

Quantile Regression Results

Quantile regression explored the propositions in each of the three DST cases. Table 3 shows the results for the 25th quantile, which represents the group of citizens more critical of each DST. Table 4 shows the quantile regression for the 75th quantile, which includes the group that is more favorable about using each DST. Coefficients significantly different from zero appear in bold in the tables. The exact *p*-value and significance level appear in the column labeled P > t.

The findings confirm between-case differences in trustworthiness assessments along its subscales, with benevolence being important for

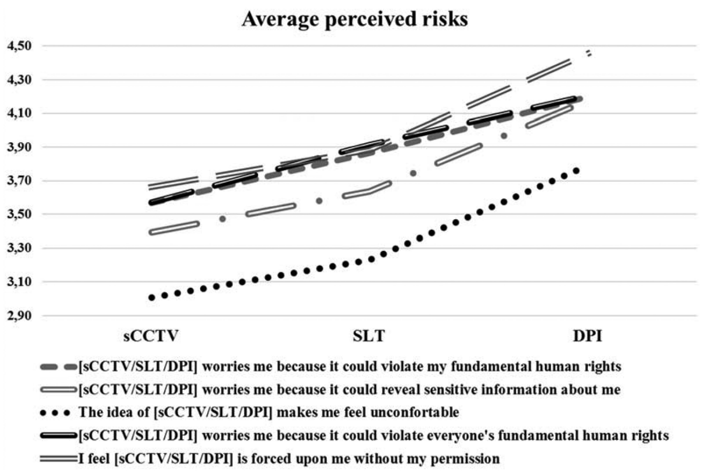

Figure 1 Perceived Degree of Data Vulnerability of Each DST on Average

Table 3 Results of the 25th Quantile Regression for the Three DSTs

25th Quantile (People Opposing the Adoption of [sCCTV/SLT/DPI] As a National Security Measure)	sCCTV			SLT			DPI		
	Coeff.	SE	P>t	Coeff.	SE	P>t	Coeff.	SE	P>t
Age	**.13**	*.03*	**.000**	**.08**	*.04*	**.026**	.02	*.04*	.588
Gender	.20	*.11*	.062	.05	*.10*	.633	**.22**	*.11*	**.038**
Minority ethnic group	.16	*.14*	.263	.09	*.13*	.488	.05	*.13*	.715
Children at home	.06	*.12*	.635	.04	*.11*	.736	**.24**	*.12*	**.040**
Education	.04	*.04*	.340	–.05	*.03*	.167	**–.08**	*.04*	**.027**
Familiarity with [CCTV/smartphone/internet]	.06	*.04*	.163	**.16**	*.05*	**.003**	–.02	*.07*	.727
Understanding of [sCCTV/SLT/DPI]	–.03	*.05*	.491	**–.17**	*.06*	**.006**	–.01	*.04*	.742
Feeling safe in daily life	–.10	*.06*	.103	–.03	*.06*	.656	–.04	*.06*	.528
Worries about online security	**.12**	*.05*	**.013**	.07	*.04*	.133	.03	*.05*	.581
[sCCTV/SLT/DPI] improves national security	**1.07**	*.12*	**.000**	**1.01**	*.11*	**.000**	**.81**	*.12*	**.000**
Concerns about excessive data collection	**–.15**	*.06*	**.012**	**–.20**	*.06*	**.001**	**–.13**	*.07*	**.041**
Concerns about unauthorized data sharing	.04	*.07*	.581	.04	*.07*	.561	.05	*.10*	.619
P1.a Benevolence	**.12**	*.06*	**.030**	**.18**	*.06*	**.004**	**.14**	*.06*	**.021**
P1.b Competence	**.18**	*.06*	**.005**	**.12**	*.06*	**.037**	**.15**	*.06*	**.018**
P1.c Integrity	.08	*.06*	.191	**.13**	*.06*	**.030**	**.17**	*.06*	**.006**
P2.a [sCCTV/SLT/DPI] revealing sensitive information	**–.21**	*.05*	**.000**	**–.15**	*.06*	**.009**	**–.17**	*.06*	**.006**
P2.b [sCCTV/SLT/DPI] is forced upon me	–.04	*.05*	.435	**–.10**	*.05*	**.038**	–.11	*.07*	.108
P2.c [sCCTV/SLT/DPI] could violate everyone's human rights	**–.23**	*.05*	**.000**	–.05	*.06*	.329	**–.18**	*.06*	**.002**
Constant term	2.37	*.59*	.000	2.37	*.58*	.000	3.11	*.72*	.000
Number of observations	513			503			501		
Pseudo-R^2	.49			.44			.38		

The significance is visible in column P > t.

Table 4 Results of the 75th Quantile Regression for the Three DSTs

75th Quantile (People Supporting the Adoption of [sCCTV/SLT/DPI] As a National Security Measure)	sCCTV			SLT			DPI		
	Coeff.	SE	P>t	Coeff.	SE	P>t	Coeff.	SE	P>t
Age	**.07**	*.04*	**.046**	.07	*.04*	.111	.04	*.04*	.387
Gender	.00	*.11*	.992	.06	*.12*	.643	.12	*.12*	.308
Minority ethnic group	–.07	*.15*	.651	.16	*.15*	.295	–.02	*.15*	.885
Children at home	–.04	*.13*	.732	.08	*.14*	.574	.19	*.14*	.169
Education	–.01	*.04*	.900	**–.11**	*.04*	**.010**	**–.11**	*.04*	**.009**
Familiarity with [CCTV/smartphone/internet]	.00	*.04*	.974	**.14**	*.07*	**.033**	–.08	*.08*	.299
Understanding of [sCCTV/SLT/DPI]	–.06	*.05*	.238	.08	*.08*	.276	.03	*.05*	.576
Feeling safe in daily life	**–.18**	*.06*	**.005**	.00	*.07*	.992	–.01	*.07*	.906
Worries about online security	**.11**	*.05*	**.034**	.08	*.05*	.117	.08	*.06*	.177
[sCCTV/SLT/DPI] improves national security	**.60**	*.13*	**.000**	**.51**	*.13*	**.000**	**.67**	*.13*	**.000**
Concerns about excessive data collection	**–.16**	*.06*	**.015**	**–.19**	*.07*	**.009**	–.13	*.08*	.097
Concerns about unauthorized data sharing	.07	*.08*	.365	.04	*.09*	.648	.10	*.11*	.381
P1.a Benevolence	**.18**	*.06*	**.003**	**.19**	*.08*	**.013**	**.22**	*.07*	**.001**
P1.b Competence	.09	*.07*	.190	**.19**	*.07*	**.009**	**.15**	*.07*	**.038**
P1.c Integrity	.01	*.06*	.915	.12	*.08*	.102	–.01	*.07*	.841
P2.a [sCCTV/SLT/DPI] revealing sensitive information	**–.13**	*.06*	**.018**	–.11	*.07*	.123	**–.21**	*.07*	**.003**
P2.b [sCCTV/SLT/DPI] is forced upon me	–.02	*.05*	.652	–.03	*.06*	.611	–.10	*.08*	.172
P2.c [sCCTV/SLT/DPI] could violate everyone's human rights	**–.13**	*.05*	**.019**	–.07	*.07*	.328	**–.14**	*.07*	**.036**
Constant term	4.65	*.62*	.000	2.28	*.71*	.002	4.41	*.83*	.000
Number of observations	513			503			501		
Pseudo-R^2	.22			.24			.14		

The significance is visible in column P > t.

all DSTs. Proposition 1, which suggests a positive relationship between security agencies' benevolence and DST acceptance, is confirmed across all DSTs and for all study participants. The positive effect of security agencies' perceived competence on citizens' willingness to accept each DST is confirmed in all cases but, in the case of sCCTV, only for the group of participants more favorable about this DST. Security agencies' integrity positively influences the views only of citizens more critical about the use of SLT and DPI. These results confirm citizens' need to be reassured about security agencies' competence and integrity when confronted with riskier DSTs.

Proposition 2, which establishes a negative effect of DST data vulnerabilities on their perceived acceptability, is also confirmed. However, the effect is significant only for the risk of revealing sensitive data and violating human rights for sCCTV and DPI. SLT seems more innocuous to citizens, perhaps because of their greater personal familiarity with smartphones. Nonetheless, more critical citizens are also less willing to accept SLT because of the perceived lack of control over geolocation functionalities.

In line with those who criticize the privacy–security trade-off (Solove 2011), participants acknowledge the effectiveness of using DSTs for security purposes, while also being concerned about the amount of data collected. Confirming previous studies (Sanquist, Mahy, and Morris 2008), Kendall rank correlation coefficients show that measures of privacy concerns and security benefits are inversely related. Measures of trustworthiness correlate positively with measures of security benefits and negatively with risk measures. However, correlation values were not sufficiently high to create multicollinearity in the regression model. The model shows good explanatory power with regard to the views of citizens who are more critical about each DST (pseudo-R^2 goodness-of-fit measure for the 25th quantile regression: sCCTV: 0.49; SLT: 0.44; DPI: 0.38), sufficient explanatory power in accounting for the opinions of those who are neither negative nor supportive (pseudo-R^2 for the median regression: sCCTV: 0.35; SLT: 0.32; DPI: 0.35), and low explanatory power in the case of those who support DST (pseudo-R2 goodness-of-fit measure for the 75th quantile regression: sCCTV: 0.22; SLT: 0.24; DPI: 0.14).

Discussion

This article examines the basis on which EU citizens support and oppose the use of digital surveillance to protect national security through an institutional trustworthiness lens across three DST cases, which present escalating degrees of privacy risk to citizens. The concept of data vulnerability was used to assess the degree of privacy risk felt by citizens in respect of each DST.

The paper's most important finding is that benevolence is central to the acceptance of DSTs regardless of data vulnerability levels. The findings highlight that for all DSTs to be accepted, security agencies need to act explicitly in the interests of the collectivity, the community and the group, rather than opportunistically and in a self-interested way. It also suggests that there is a shared responsibility for social order when using DSTs (Jackson et al. 2012). This finding underpinned the views of both those who supported and those who opposed the use of DSTs. It confirms that citizens' first question when any DST is used is likely to be "what's in it for us?"

The article also found that as data vulnerabilities increased, so did the range of institutional trustworthiness concerns, measured using the subscales. For DSTs considered more intrusive and risky, citizens also demand reassurance about security agencies' competence and integrity. Competence was important for those who supported and those who opposed the adoption of the two more intrusive DSTs: SLT and DPI. This finding confirms that citizens are likely to ask utilitarian, instrumentally rational questions about security agencies' ability to operate these DSTs efficiently and the extent to which tangible improvements in security will occur as data vulnerability increases (Meško and Tankebe 2014). If citizens believe that the security agency operates the DST competently, they are more likely to accept its adoption.

Integrity was also a basis of opposition to the same two DSTs, suggesting that opposition rests on questions about the responsible use of power that reflects shared moral norms and values (Hough et al. 2010). The breadth of the human rights' consequences discussed in the summit support materials indicates that these moral concerns may go beyond the issue of privacy to other areas, such as freedom of speech and autonomy. The findings indicate that assurances about the moral stance of a security agency are more likely to convince citizens who oppose the technology that it should be adopted.

The findings demonstrate that there are institutional dimensions to citizens' views on DSTs that extend beyond the security–privacy trade-off and challenge two common governmental tropes about the general public's opinions about national security surveillance. Decisions to support or oppose DSTs occur in a conceptual space beyond an individualized, instrumentally rational security–privacy trade-off. Each trustworthiness subscale—benevolence, competence, and integrity—was interpreted as a belief system based on contrasting foundations. The competence subscale is acknowledged to rest on instrumentally rational assessments and thus represents part of the security–privacy trade-off. The trade-off would suggest that the debate about DSTs begins and ends with competency. Yet concerns reflecting normative beliefs arise in parallel, with the normative concern of benevolence central for all assessments. The popular saying "nothing to hide, nothing to fear" is also challenged. Rather than showing that all those who oppose surveillance have "something to hide," these findings suggest that opposition may also stem from parallel concerns. These include whether security agencies are acting in the interests of the communities they serve and, where more privacy-intrusive DSTs are used, whether these agencies have the relevant capabilities and moral values. As Yamagishi, Kikuchi, and Kosugi (1999) argue, trustful people are not cultural dopes; they are vigilant and prudent as they process information about an actor's trustworthiness and nurture their "social intelligence" to detect signals of untrustworthiness.

Previous observations about the relative influence of benevolence, competence, and integrity in other settings are confirmed. The results uphold the importance of community interests with regard to benevolence (Sounman 2017). They also confirm the previous observation that when competence emerges as significant, it tends to be accompanied by one or more of the normative dimensions, rather than emerging on its own (Grimmelikhuijsen and Meijer 2014; Meško and Tankebe 2014). The emergence of integrity as the basis for opposition to SLT and DPI supports the views of Simpson, Harrell, and Willer (2013) and Grimmelikhuijsen and Meijer (2014), who note that as felt risk increases, so does the requirement for moral and principled action. It also reflects the importance of morality identified in studies of other surveillance technologies currently in use (Bromberg, Charbonneau, and Smith 2018; West and Bowman 2016).

The diverse ways the public engages with DSTs highlight several practical and policy questions. Increasing law enforcement agencies' trustworthiness may initially be thought to lie in the increased reporting of performance, reflecting the competence subscale. The findings show that policy implications can be generated using all three trustworthiness dimensions. Reflecting benevolence, promoting citizen participation in security agendas can promote congruence around community interests. A more nuanced picture of the outcomes of digital security surveillance for different groups may emerge, perhaps generating more inclusive, equitable, and sensitive applications. Efforts to improve transparency and to protect democratic rights in security settings will influence perceptions of integrity: whether the agency will "do the right thing" and not abuse its power. The democratic process can act to embrace feelings of opposition, avoidance, and resistance to privacy violations rather than outflank them, as the rhetoric of the trade-off and the "nothing to hide, nothing to fear" stance suggest.

The article also makes two methodological contributions. The between-case design exposes the influence of the trustworthiness assessment on DST acceptance in three cases, which show higher degrees of perceived data vulnerability. The design guarantees the robustness of results and foregrounds the consistent effect of benevolence across the three DST cases and for all groups of respondents. The second contribution is the use of quantile regression to attain further nuance, by highlighting similarities and differences in perceptions, between those who support and those who oppose digital surveillance. A great deal of policy making relies on finding solutions for the "average" citizen, without exploring in detail which arguments are relevant or irrelevant for which parts of the population. The quantile regression approach provides additional insights by focusing on polarized rather than average views.

Finally, this article has several limitations, which provide avenues for future research. First, while the results present an international picture, further research could consider how different DSTs within different states affect different communities. Second, the European Union is, as a research site, a relatively homogeneous social democratic political system. Replications of the research in authoritarian or recently postauthoritarian countries in transition arrangements may yield different findings. Third, as this research is quantitative in nature, more fine-grained research would reveal exactly how each individual belief system functions in its formation of public attitudes. Finally, as this was a cross-sectional rather than longitudinal study, the temporal dimension of the relationships should be explored in the future.

Conclusion

This article establishes that institutional trustworthiness dimensions—especially benevolence, but also competence and integrity—shape citizens' views on digital surveillance used in security operations. Digital surveillance is now a routine feature of national security measures. It offers security benefits but also provokes privacy risks because of the volume of captured and processed citizen data. Citizens experience these risks as data vulnerabilities linked to concerns about the exposure and sharing of their information and the associated human rights' implications. As long as digital surveillance remains a dominant feature of national security policy, national security agencies will need to reconcile its transformatory impact with public expectations of how they protect privacy and human rights and act with benevolence, competence, and integrity toward their citizens.

Notes

1. By 'security agencies' we mean the different government bodies which are responsible for maintaining security, law and order. This includes a nation's territorial police forces, special police forces, and border agencies. Although this research uses the term "security agencies," it is also acknowledged that a wide range of state and nonstate actors collaborate in the provision of national security, with security agencies at the center (see White 2012). In the citizen summits, participants explicitly identified the relevant security agencies in their national contexts when making their assessments.
2. Edward Snowden's revelations were especially noteworthy regarding the way in which security agencies collect and use people's data, with suspicions intensifying as new incidents have occurred. Recent examples include the alleged racist violence expressed by U.S. border patrol agents in a secret Facebook group (Thompson 2019) and the diffusion of security technologies into civilian domains, such as democratic elections (DCMS 2018).
3. Citizen summit information material is available at: http://surprise-project.eu/dissemination/information-material-from-the-participatory-events/.

References

Akter, Shahriar, John D'Ambra, and Pradeep Ray. 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): 100–16. https://doi.org/10.1002/asi.21442.

Anderson, David. 2015. A Question of Trust: Report of the Investigatory Powers Review. In: Report of the Independent Reviewer's review of the Data Retention and Investigatory Powers Act 2014.

Ball, Kirstie, Sara Degli Esposti, Sally Dibb, Vincenzo Pavone, and Elvira Santiago-Gómez. 2018. Institutional Trustworthiness and National Security Governance: Evidence from Six European Countries. *Governance* 32: 103–21. https://doi.org/10.1111/gove.12353.

Bedsted, Bjørn, Søren Gram, Marie Louise Jøergensen, and Lars Klüver. 2015. WWViews on Biodiversity: New Methodological Developments and Ambitions. In *Governing Biodiversity Through Democratic Deliberation*, edited by Mikko Rask and Richard Worthington, 27–40. New York: Routledge.

Bigo, Didier. 2016. Digital Surveillance and Everyday Democracy. In *The Routledge International Handbook of Criminology and Human Rights*, edited by Leanne Weber, Elaine Fishwick, and Marinella Marmo, 496–510. New York: Routledge.

Blackwood, Leda, Nick Hopkins, and Steve Reicher. 2015. 'Flying While Muslim': Citizenship and Misrecognition in the Airport. *Journal of Social and Political Psychology* 3(2): 148–70. https://doi.org/10.5964/jspp.v3i2.375.

de Boer, Noortje. 2020. How Do Citizens Assess Street-Level Bureaucrats' Warmth and Competence? A Typology and Test. *Public Administration Review* 80(4): 532–42. https://doi.org/10.1111/puar.13217.

Brandom, Russell. 2014. Egypt Launches Deep-Packet Inspection System. The Verge, Sep 17, 2014, 4:57pm EDT. https://www.theverge.com/2014/9/17/6350191/egypt-launches-deep-packet-inspection-with-help-from-an-american.

van den Broek, Tijs, Merel Ooms, Michael Friedewald, Marc van Lieshout, and Sven Rung. 2017. Privacy and Security: Citizens' Desires for an Equal Footing. In *Surveillance, Privacy and Security* 15–35. Routledge.

Bromberg, Daniel E., Étienne Charbonneau, and Andrew Smith. 2018. Body-Worn Cameras and Policing: A List Experiment of Citizen Overt and True Support. *Public Administration Review* 78(6): 883–91. https://doi.org/10.1111/puar.12924.

Burchardt, Tania. 2014. Deliberative Research as a Tool to Make Value Judgements. *Qualitative Research* 14(3): 353–70. https://doi.org/10.1177/1468794112469624.

Cayford, Michelle, Wolter Pieters, and P.H.A.J.M. van Gelder. 2019. Wanting it All—Public Perceptions of the Effectiveness, Cost, and Privacy of Surveillance Technology. *Journal of Information, Communication and Ethics in Society* 18(1): 10–27. https://doi.org/10.1108/JICES-11-2018-0087.

Clement, Andrew. 2013. "IXmaps—Tracking Your Personal Data Through the NSA's Warrantless Wiretapping Sites." 2013 IEEE International Symposium on Technology and Society (ISTAS), Toronto, ON, Canada. doi: https://doi.org/10.1109/ISTAS.2013.6613122.

Cooper, Christopher A., H. Gibbs Knotts, and Kathleen M. Brennan. 2008. The Importance of Trust in Government for Public Administration: The Case of Zoning. *Public Administration Review* 68(3): 459–68. https://doi.org/10.1111/j.1540-6210.2008.00882.x.

Cvetkovich, George, and Kazuya Nakayachi. 2007. Trust in a High-Concern Risk Controversy: A Comparison of Three Concepts. *Journal of Risk Research* 10(2): 223–37. https://doi.org/10.1080/13669870601122519.

DCMS. 2018. DCMS Committee Launches New Inquiry into the Growth of 'Immersive and Addictive Technologies'. Parliament.uk.

Dean, Rikki John. 2017. Beyond Radicalism and Resignation: The Competing Logics for Public Participation in Policy Decisions. *Policy & Politics* 45(2): 213–30. https://doi.org/10.1332/030557316X14531466517034.

Degli Esposti, Sara, and Elvira Santiago-Gómez. 2015. Acceptable Surveillance-Orientated Security Technologies: Insights from the SurPRISE Project. *Surveillance & Society* 13(3/4): 437–54. https://doi.org/10.24908/ss.v13i3/4.5400.

Dourish, Paul, and Ken Anderson. 2006. Collective Information Practice: Emploring Privacy and Security as Social and Cultural Phenomena. *Human-Computer Interaction* 21(3): 319–42. https://doi.org/10.1207/s15327051hci2103_2.

Eifler, Stefanie. 2007. Evaluating the Validity of Self-Reported Deviant Behavior Using Vignette Analyses. *Quality & Quantity* 41(2): 303–18. https://doi.org/10.1007/s11135-007-9093-3.

Eurostat. 2013. Average Rating of Trust by Domain, Sex, Age and Educational Attainment Level (Year 2013) Last update: 26-04-2019. http://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=ilc_pw03&lang=en.

Frederickson, H. George, and David K. Hart. 1985. The Public Service and the Patriotism of Benevolence. *Public Administration Review* 45(5): 547–53. https://doi.org/10.2307/3109929.

Fuchs, Christian. 2013. Societal and Ideological Impacts of Deep Packet Inspection Internet Surveillance. *Information, Communication & Society* 16(8): 1328–59. https://doi.org/10.1080/1369118X.2013.770544.

Greenwald, Anthony G. 2014. Why Are Attitudes Important? In *Attitude Structure and Function*, edited by Anthony R. Pratkanis, Steven J. Breckler, and Anthony G. Greenwald, 21–38. New York: Psychology Press.

Grimmelikhuijsen, Stephan G., and Albert J. Meijer. 2014. Effects of Transparency on the Perceived Trustworthiness of a Government Organization: Evidence from an Online Experiment. *Journal of Public Administration Research & Theory* 24(1): 137–57.

Grimmelikhuijsen, Stephan, Gregory Porumbescu, Boram Hong, and Tobin Im. 2013. The Effect of Transparency on Trust in Government: A Cross-National Comparative Experiment. *Public Administration Review* 73(4): 575–86. https://doi.org/10.1111/puar.12047.

Hao, Lingxin, and Daniel Q. Naiman. 2007. Quantile regression. In *Quantitative Applications in the Social Sciences*, Vol 149. London: Sage Publications.

Hofstede, Geert. 2003. *Culture's Consequences: Comparing Values, Behaviors, Institutions and Organizations across Nations*. London: SAGE.

Hough, Mike, Jonathan Jackson, Ben Bradford, Andy Myhill, and Paul Quinton. 2010. Procedural Justice, Trust, and Institutional Legitimacy. *Policing: A Journal of Policy and Practice* 4(3): 203–10. https://doi.org/10.1093/police/paq027.

Introna, Lucas, and David Wood. 2004. Picturing Algorithmic Surveillance: The Politics of Facial Recognition Systems. *Surveillance & Society* 2(2/3): 177–98. https://doi.org/10.24908/ss.v2i2/3.3373.

Jackson, Jonathan, Ben Bradford, Betsy Stanko, and Katrin Hohl. 2012. *Just Authority? Trust in the Police in England and Wales*. London: Willan, Taylor & Francis Group.

Jakobsen, Morten, and Rasmus Jensen. 2015. Common Method Bias in Public Management Studies. *International Public Management Journal* 18(1): 3–30. https://doi.org/10.1080/10967494.2014.997906.

Kim, Soonhee, and Jooho Lee. 2012. E-Participation, Transparency, and Trust in Local Government. *Public Administration Review* 72(6): 819–28. https://doi.org/10.1111/j.1540-6210.2012.02593.x.

Koenker, Roger. 2005. Quantile Regression. Edited by. In *Econometric Society Monographs*, Vol 38, edited by Andrew Chesher and Matthew Jackson. Cambridge, UK: Cambridge University Press.

Kreissl, Reinhard, Regina Berglez, Maria Grazia Procedda, Martin Scheinin, Matthias Vermeulen, and Eva Schlehahn. 2013. D 3.4 Exploring the Challenges: Synthesis Report. FP7 SurPRISE Project.

Levi, Margaret, and Laura Stoker. 2000. Political Trust and Trustworthiness. *Annual Review of Political Science* 3(1): 475–507. https://doi.org/10.1146/annurev.polisci.3.1.475.

Lew, Alan A., and Pin T. Ng. 2012. Using Quantile Regression to Understand Visitor Spending. *Journal of Travel Research* 51(3): 278–88. https://doi.org/10.1177/0047287511410319.

Lewis, Paul. 2010. Birmingham Stops Camera Surveillance in Muslim Areas. The Guardian, First published on Thu 17 Jun 2010 11.51 BST. https://www.theguardian.com/uk/2010/jun/17/birmingham-stops-spy-cameras-project.

Loader, Ian, and Neil Walker. 2007. *Civilizing Security*. Cambridge, MA: Cambridge University Press.

MacKenzie, S.B., and P.M. Podsakoff. 2012. Common Method Bias in Marketing: Causes, Mechanisms, and Procedural Remedies. *Journal of Retailing* 88: 542–55. https://doi.org/10.1016/j.jretai.2012.08.001.

Martin, Kelly D., Abhishek Borah, and Robert W. Palmatier. 2017. Data Privacy: Effects on Customer and Firm Performance. *Journal of Marketing* 81(1): 36–58. https://doi.org/10.1509/jm.15.0497.

Mayer, Roger C., James H. Davis, and F. David Schoorman. 1995. An Integrative Model of Organizational Trust. *Academy of Management Review* 20(3): 709–34. https://doi.org/10.5465/AMR.1995.9508080335.

McKnight, D. Harrison, Vivek Choudhury, and Charles Kacmar. 2002. Developing and Validating Trust Measures for e-Commerce: An Integrative Typology. *Information Systems Research* 13(3): 334–59. https://doi.org/10.1287/isre.13.3.334.81.

Meško, Gorazd, and Justice Tankebe. 2014. *Trust and Legitimacy in Criminal Justice: European Perspectives*. New York: Springer.

Migchelbrink, Koen, and Steven Van de Walle. 2020. When Will Public Officials Listen? A Vignette Experiment on the Effects of Input Legitimacy on Public Officials' Willingness to Use Public Participation. *Public Administration Review* 80(2): 271–80. https://doi.org/10.1111/puar.13138.

Möllers, Norma, and Jens Hälterlein. 2013. Privacy Issues in Public Discourse: The Case of "Smart" CCTV in Germany. *Innovation: The European Journal of Social Science Research* 26(1–2): 57–70. https://doi.org/10.1080/13511610.2013.723396.

Moynihan, Donald P. 2003. Normative and Instrumental Perspectives on Public Participation: Citizen Summits in Washington, D.C. *The American Review of Public Administration* 33(2): 164–88. https://doi.org/10.1177/0275074003251379.

Nabatchi, Tina. 2010. Addressing the Citizenship and Democratic Deficits: The Potential of Deliberative Democracy for Public Administration. *The American Review of Public Administration* 40(4): 376–99. https://doi.org/10.1177/0275074009356467.

Nissenbaum, Helen. 2009. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford, US: Stanford Law Books.

Pavone, Vincenzo, and Sara Degli Esposti. 2012. Public Assessment of New Surveillance-Oriented Security Technologies: Beyond the Trade-Off between Privacy and Security. *Public Understanding of Science* 21(July): 556–72. https://doi.org/10.1177/0963662510376886.

Pavone, Vincenzo, Kirstie Ball, Sara Degli Esposti, Sally Dibb, and Elvira Santiago-Gómez. 2017. Beyond the Security Paradox: Ten Criteria for a Socially Informed Security Policy. *Public Understanding of Science* 27(6): 638–54. https://doi.org/10.1177/0963662517702321.

Pell, Stephanie K., and Christopher Soghoian. 2013. A Lot More Than a Pen Register, and Less than a Wiretap: What the StingRay Teaches Us About How Congress Should Approach the Reform of Law Enforcement Surveillance Authorities. *Yale Journal of Law & Technology* 16(1): 134–71. https://doi.org/10.31228/osf.io/cwvk8.

Porcedda, Maria Grazia. 2013. Lessons from PRISM and Tempora: The Self-Contradictory Nature of the Fight against Cyberspace Crimes. Deep Packet Inspection as a Case Study. *Neue Kriminalpolitik* 25(4): 373–89.

Reddick, Christopher G., Akemi Takeoka Chatfield, and Patricia A. Jaramillo. 2015. Public Opinion on National Security Agency Surveillance Programs: A Multi-Method Approach. *Government Information Quarterly* 32(2): 129–41. https://doi.org/10.1016/j.giq.2015.01.003.

Roberts, Nancy. 2004. Public Deliberation in an Age of Direct Citizen Participation. *The American Review of Public Administration* 34(4): 315–53. https://doi.org/10.1177/0275074004269288.

Sanquist, Thomas F., Heidi Mahy, and Frederic Morris. 2008. An Exploratory Risk Perception Study of Attitudes toward Homeland Security Systems. *Risk Analysis* 28(4): 1125–33. https://doi.org/10.1111/j.1539-6924.2008.01069.x.

Schlehahn, Eva, Marit Hansen, Jaro Sterbik-Lamina, and Javier Sempere Samaniego. 2013. D 3.1—Report On Surveillance Technology And Privacy Enhancing Design. EU FP7 SurPRISE.

Schoorman, F. David, Roger C. Mayer, and James H. Davis. 2007. An Integrative Model of Organizational Trust: Past, Present, and Future. *Academy of Management Review* 32(2): 344–54. https://doi.org/10.5465/amr.2007.24348410.

Siegrist, Michael, and George Cvetkovich. 2002. Perception of Hazards: The Role of Social Trust and Knowledge. *Risk Analysis* 20(5): 713–20. https://doi.org/10.1111/0272-4332.205064.

Simpson, Brent, Ashley Harrell, and Robb Willer. 2013. Hidden Paths from Morality to Cooperation: Moral Judgments Promote Trust and Trustworthiness. *Social Forces* 91(4): 1529–48. https://doi.org/10.1093/sf/sot015.

Smith, H. Jeff, Sandra J. Milberg, and Sandra J. Burke. 1996. Information Privacy: Measuring Individuals' Concerns about Organizational Practices. *MIS Quarterly* 20(2): 167–96. https://doi.org/10.2307/249477.

Solove, Daniel J. 2008. Data Mining and the Security-Liberty Debate. *The University of Chicago Law Review* 75(1): 343–62. https://www.jstor.org/stable/20141911.

———. 2011. *Nothing to Hide: The False Tradeoff between Privacy and Security*. New Haven, CT: Yale University Press.

Sounman, Hong. 2017. Black in Blue: Racial Profiling and Representative Bureaucracy in Policing Revisited. *Journal of Public Administration Research & Theory* 27(4): 547–61. https://doi.org/10.1093/jopart/mux012.

Tankebe, Justice. 2008. Police Effectiveness and Police Trustworthiness in Ghana: An Empirical Appraisal. *Criminology & Criminal Justice* 8(2): 185–202. https://doi.org/10.1177/1748895808088994.

Thornton, Sara. 2010. Project Champion Review. Thames Valley Police.

Tunarosa, Andrea, and Mary Ann Glynn. 2017. Strategies of Integration in Mixed Methods Research: Insights Using Relational Algorithms. *Organizational Research Methods* 20(2): 224–42.

Tyler, Tom R. 2005. Policing in Black and White: Ethnic Group Differences in Trust and Confidence in the Police. *Police Quarterly* 8(3): 322–42. https://doi.org/10.1177/1098611104271105.

Tyler, Tom R., and Jeffrey Fagan. 2008. Legitimacy and Cooperation: Why Do People Help the Police Fight Crime in their Communities. *Ohio State Journal of Criminal Law* 6: 231–75.

Tyler, Tom R., Stephen Schulhofer, and Aziz Z. Huq. 2010. Legitimacy and Deterrence Effects in Counterterrorism Policing: A Study of Muslim Americans. *Law & Society Review* 44(2): 365–402. https://doi.org/10.1111/j.1540-5893.2010.00405.x.

Ungerleider, Neal. 2012. Occupy Sites Help Cops, Corps Track Occupiers. FastCompany, 25/04/2012.

West, Jonathan P., and James S. Bowman. 2016. The Domestic Use of Drones: An Ethical Analysis of Surveillance Issues. *Public Administration Review* 76(4): 649–59. https://doi.org/10.1111/puar.12506.

White, Adam. 2012. The New Political Economy of Private Security. *Theoretical Criminology* 16(1): 85–101. https://doi.org/10.1177/1362480611410903.

Yamagishi, Toshio, Masako Kikuchi, and Motoko Kosugi. 1999. Trust, Gullibility, and Social Intelligence. *Asian Journal of Social Psychology* 2(1): 145–61. https://doi.org/10.1111/1467-839X.00030.

Supporting Information

A supplemental appendix can be found in the online version of this article at http://onlinelibrary.wiley.com/journal/10.1111/(ISSN)1540-6210.

Appendix A

See Tables A1 and A2.

Table A1 DSTs Discussed in Each Country and Level Of Institutional Trust

		sCCTV	SLT	DPI	Trust in …[a]			
					Police	Legal System	Political System	Others
1.	Denmark	✓	✓		7.9	7.5	5.9	8.3
2.	Germany	✓	✓		6.4	5.3	4.9	5.5
3.	Hungary	✓	✓		5.7	5.1	4.5	5.3
4.	Austria	✓		✓	7.2	6.0	4.4	5.9
5.	UK	✓		✓	6.4	5.5	3.8	6.1
6.	Spain	✓		✓	5.4	3.1	1.9	6.3
7.	Norway		✓	✓	7.5	7.2	5.9	7.3
8.	Switzerland		✓	✓	7.4	7.0	6.6	6.4
9.	Italy		✓	✓	5.8	3.6	2.1	5.7

[a]Values indicate a weighted mean on an 11-point scale ranging from 0 = "no trust at all" to 10 = "complete trust". Source: Eurostat (2013).

Table A2 Detailed Descriptions of DST Cases

The descriptions were devised following a systematic review of the security and data protection gray literature, in conjunction with key informant interviews with 12 security industry experts, consultants, scholars, and regulators (Schlehahn et al. 2013).

- *Smart CCTV (sCCTV)* is used by homeland security agencies such as the police and national border forces to identify suspicious behavior in specific public spaces, such as airports and roads. Applications range from automatic detection of criminal behavior, to identification of search-listed criminal or unwanted individuals, to the prosecution of traffic offenders (Möllers and Hälterlein 2013). The most common use is Automatic Number Plate Recognition (ANPR) to identify vehicles that have been stolen, driven without tax or insurance, or committed traffic offenses. Vehicle license plate details or image are captured when they pass sCCTV. Citizens may not be aware at the time that this information has been captured, and there is a risk of images being misinterpreted and false positive identification occurring, should an individual's information be implicated in an investigation. Human rights vulnerabilities were manifested in a controversial UK case in which sCCTV cameras were installed in predominantly Muslim areas of Birmingham in 2010 under an antiterrorism program called "Project Champion" (Thornton 2010). In 2011, the British police in Birmingham, UK, had to remove ANPR cameras from three areas of the city that had a high Muslim population. The cameras were funded under Project Champion, but the cameras were promoted to the public on safety grounds. Community leaders and local members of parliament strongly objected to the cameras, and community relations were damaged. Two hundred cameras were installed but were never switched on. The project's failure and the loss of the cameras cost the police £300,000 (€351,414) (Lewis 2010).
- *Smartphone location tracking (SLT)*, which can be performed through carrier-assisted surveillance, among other things (Pell and Soghoian 2013), is used to locate, follow, monitor, and gather evidence of suspects. SLT is used by security services and law enforcement agencies to glean information about the location and movements of the phone user over time. It is used in investigations locally, nationally, and internationally for many different types of security threat, from traffic offenses to terror attacks. SLT can reveal citizens' movements and specific locations to a third party, should that information be shared. Anyone carrying a smartphone that is turned on and registering its location on cell towers, via apps and location-based services, can easily be tracked. Human rights vulnerabilities manifested by the policing of the Occupy movement in Germany and the United States, where location data were used to track protestors (Ungerleider 2012). The Occupy movement is an international social-political movement protesting against economic inequality and promoting participatory democracy. It began with a group of veterans setting up camp in New York in September 2011, but through coordination on social media and other methods has spread to cities around the world.
- *Deep packet inspection (DPI)* is routinely used by security agencies internationally to examine the content of Internet communications to identify criminal activity. Agencies, such as the NSA and GCHQ, use DPI to identify malicious activity online, such as the distribution of child pornography, hate speech, or terrorism (Porcedda 2013). All electronic communications can be subject to DPI, raising immediate information privacy concerns with every electronic communication. This technology is opaque, making it impossible for citizens to know when and where their communication data are monitored. DPI is banned in Europe, but all messages that travel through servers based in the United States, where it is unregulated, are subject to it. DPI raises privacy concerns as it renders all unencrypted online communication visible to unknown third parties, should those communications travel across their networks. Human rights vulnerabilities have manifested from DPI, which has been linked to online censorship around the world and to several politically repressive regimes. Documentary evidence suggests that DPI was used to monitor political opponents of the Syrian government (Fuchs 2013), and it was allegedly used by the Libyan and Egyptian governments to crush dissent in the Arab Spring (Brandom 2014). The A*rab Spring* was a series of prodemocracy *protests and uprisings* that took place in several largely Muslim countries, including Tunisia, Morocco, Syria, Libya, Egypt, and Bahrain, beginning in the spring of 2011.