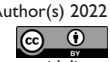
Article

new media & society
1–23



DOI: 10.1177/14614448221134493
journals.sagepub.com/home/nms


Who is afraid of dataveillance? Attitudes toward online surveillance in a cross-cultural and generational perspective

Veronika Kalmus
University of Tartu, Estonia

Göran Bolin
Södertörn University, Sweden

Rita Figueiras
Universidade Católica Portuguesa, Portugal

Abstract

This article compares surveillance-related experiences and attitudes of two generations of media users in countries with different historical surveillance regimes (Estonia, Portugal, and Sweden) and analyzes the predictors of the attitudes toward contemporary surveillance. A large-scale online survey ($N = 3221$) reveals that attitudes toward online state and corporate surveillance are interrelated; the two attitudinal components are, however, generation-specific, having different predictors. Tolerance toward state surveillance is more characteristic of the older group, being predicted by trustful and obedient attitudes toward state authorities and institutions. Tolerance toward corporate dataveillance is more characteristic of the younger group, being predicted by active and self-confident media use. While the socio-historical context molds the intergenerational gaps in surveillance-related experiences and attitudes, individual-level experiences of state surveillance do not predict tolerance toward either type of contemporary surveillance, suggesting that global techno-cultural developments are probably more powerful factors than past experiences in forming generation-specific attitudes.

Corresponding author:
Göran Bolin, Media and Communication Studies, Södertörn University, 141 89 Huddinge, Sweden.
Email: goran.bolin@sh.se

Keywords
Authoritarianism, cross-cultural analysis, datafication, dataveillance, generations, surveillance, trust

Introduction

In the age of social media and "surveillance capitalism" (Zuboff, 2015), state surveillance and corporate "big data" surveillance (Andrejevic and Gates, 2014) through social media have converged technologically (Trottier and Lyon, 2012). With the spread of smartphones, laptops, and other mobile and personal media, the areas of the life-worlds of citizens that can be subsumed by monitoring practices have multiplied, including information about *when, where*, and *with whom* citizens and consumers engage in communication (Andrejevic, 2007). The very same online technologies are used to both "capture the digital consumer" (Bolin, 2011) and monitor state security (Giroux, 2015; Haggerty and Ericson, 2000). Recent research suggests that the attitudes of citizens toward surveillance by social media companies are mixed, where media users, on the one hand, are skeptical, or even cynical (Lutz et al., 2020), but at the same time do very little in terms of protecting themselves through, for example, privacy settings (Jansson, 2012; Leckner, 2018; Obar and Oeldorf-Hirsch, 2020; Turow et al., 2015), the phenomenon that Barnes (2006) calls the "privacy paradox."

Most previous studies on social media surveillance are conducted in long-time liberal democracies with limited experiences of explicit and intrusive state surveillance (exceptions are, for example, Liu, 2022; Martin et al., 2019, 2020). An unanswered question, then, is whether citizens with experiences of such surveillance practices differ from those without. What role does the historical legacy of totalitarianism or authoritarianism vis-à-vis global techno-cultural developments, embodied in generational experiences and values, play in the formation of attitudes toward contemporary state and corporate surveillance? To answer the question, this article presents results from an original cross-cultural study among two generations with different experiences of state surveillance in three European countries.

To represent distinct historical *surveillance regimes*—the sum of the strategies and technologies of surveillance in each cultural setting—we chose Estonia, Portugal, and Sweden. Estonia was occupied by the Soviet Union from 1939 until regaining independence in 1991. During these years, Estonia was subsumed by the *totalitarian* regime of the Soviet Union, characterized by the surveillance apparatus that was omnipotent and omnipresent in all spheres of society and "included the regime's dreaded secret police with its vast powers of surveillance, arrest and detention" (Kasekamp, 2010: 130). The contemporary surveillance regime is, in contrast, loose and liberal, with state institutions investing heavily into earning and maintaining public trust, for instance, by implementing a data tracker, through which citizens can see which organizations have used their data and request more information about those practices when needed (see Männiste, 2022). These efforts have resulted, particularly, in Estonian e-governance and digital services being widely trusted by the public (see Ehin et al., 2022).

Portugal lived under a right-wing dictatorship from 1926 up to 1974. During these years, strategies of intimidation, demobilization, and repression, headed by the political

police with the help of a network of informants (civilians), promoted a culture of denunciation and values of resignation and obedience in the society (Pimentel, 2007). Fundamental rights of data privacy were anticipated by the Portuguese constitution (1976), and a set of laws on data protection preceded the European Union's General Data Protection Regulation (GDPR) (Bacelar de Gouveia, 2021). However, the expansion of the contemporary surveillance regime is fueling public debate. COVID lockdowns opened a discussion around the conflicting values of privacy and safety, and the increasing use of CCTV, police body cams, and drones by law enforcement units is questioned. Most notoriously, in 2022, the Portuguese data protection authority prohibited the telecom providers from retaining geolocation and traffic data of their clients, and access to that data without restrictions by criminal investigation authorities (Comissão Nacional de Proteçãode Dados [CNPD], 2022).

To contrast these two past totalitarian/authoritarian surveillance regimes with a yardstick, we chose Sweden as a representative of long-time *liberal democracy*. As many liberal democracies, Sweden has a specific surveillance regime, with, for example, increased presence of CCTV in public places since the mid-1990s that triggered public debate (Flyghed, 2006; Priks, 2015). The law passed in 2008 to increase the ability for surveillance of all telephone and Internet traffic passing over the Swedish territory was also fiercely debated (Bjereld and Oscarsson, 2009). Already before the GDPR, Sweden had a similar data protection regulation.

Besides socio-historical contexts and generational mindsets, other socio-demographic and cognitive factors impact upon surveillance and privacy-related attitudes and practices (see Lutz et al., 2020; Svenonius and Björklund, 2018); they are, however, seldom employed in one study. A specific contribution of our analysis consists in offering a multi-dimensional explanation to tolerance toward online state and corporate surveillance by testing the significance of the generational belonging and the country context, and a set of predictors such as education, actual and mediated experiences of state surveillance, trust in people, state institutions and the media, privacy concerns and practices, pro-democratic versus pro-authoritarian attitudes, and indicators of Internet use and digital skills.

The aim of this article is to compare surveillance-related experiences and attitudes of two generations of media users in three countries, and to explore the relationships between the attitudes toward contemporary surveillance and their predictors, considering the socio-historical context of diverse surveillance regimes. Specifically, the research questions in the current study ask:

1. How do the generational belonging and the country context impact upon experiences of, and attitudes toward, surveillance, and the related attitudes toward state institutions and the media?
2. What are the main predictors of tolerance toward state and corporate surveillance in three different socio-historical contexts?

Our discussion will proceed in four parts. In the next section we will expound the concepts of state surveillance and dataveillance and frame our analysis within the context of previous research, focusing on the issues of privacy and trust, and the related attitudes. We will then introduce our survey methodology and present, in the third section of the

paper, findings related to cultural and generational differences, and patterns of relationships between key variables. We will conclude the paper by discussing the main findings and by pointing at some features to be taken up in future research.

State surveillance and dataveillance: issues of privacy and trust

State surveillance has, in the era of analogue media, often been associated with totalitarian communist regimes such as the Soviet dictatorship (Weiner and Rahi-Tamm, 2012). However, fascist, or right-wing authoritarian states have also had their surveillance apparatuses, seeking to monitor citizen behavior (see Costa Pinto and Adinolfi, 2014, about Portugal), just as long-term democracies historically have engaged in monitoring measures (Lyon, 2015). Research has focused on CCTV (Grass, 2004; Norris et al., 2003), but also on biometric surveillance, facial recognition, and so on (Gates, 2011; Introna and Wood, 2004), including liberal democracies such as Sweden (Gunnartz, 2006).

The convergence between state surveillance and dataveillance has been observed since decades (Gandy, 1993; Haggerty and Ericson, 2000) but became obvious to a wider public with the Snowden revelations in 2013 (Lyon, 2015), the Cambridge Analytica scandal in 2018 (Cadwalladr, 2018), and, most notoriously, China's Social Credit System (e.g. Werbach, 2021). Fears around the pervasiveness of surveillance technologies resurfaced with the Pegasus spyware scandal in 2021, where an international consortium of journalists revealed that for 10 years the Israeli surveillance company NSO helped governments around the world to steal information from targeted smartphones (data, photographs, conversations, and geolocation; Pîrvu, 2021).

Even before these scandals, there was a growing body of research into "social media surveillance" (Fuchs et al., 2011; Trottier, 2012, see a review in Bolin and Jerslev, 2018), and the new business models that build on the monitoring of media users (Bermejo, 2009; Bolin, 2011; Kosterich and Napoli, 2016; van Dijck et al., 2018). The everyday use of networked media technology has fostered a new data-driven regime integrated into the general operations of contemporary capitalism at every level, expanding its business models to the social world and to conventional industries (Figueiras, 2019), sometimes labeled *dataveillance*—a concept launched in computer science indicating "the systematic use of personal data systems in the investigation or monitoring of the actions or communications of one or more persons" (Clarke, 1988: 499), but reactivated for the social media world by van Dijck (2014), indicating the commercial equivalent to state surveillance. In this study, we align with the latter, narrower, conception, and juxtapose state surveillance (whether with or without the help of digital technology) with dataveillance as the type of surveillance adopted by commercial platform companies that build their business models on the extraction of data from online media users.

Attitudes toward dataveillance

Alongside a range of studies on the technological aspects of social media surveillance (e.g. Razaghpanah et al., 2018), audience researchers have focused on media user perceptions and attitudes. In the United States, Turow and colleagues have conducted

continuous surveys on attitudes among citizens on data mining, pointing to ambivalent feelings such as resignation (Draper and Turow, 2019; Turow et al., 2015, 2018). In Europe, Kennedy et al. (2015) have analyzed media users' attitudes toward social media data mining, asking users "to share their responses to these practices in their own words" (p. 2). Building their analysis on 10 focus group interviews each in Norway, Spain, and England, the main findings were that social media users were concerned with questions of "fairness," where some kinds of monitoring of their uses were considered "fair," considering the wider purpose of the data mining. Kennedy has followed up with a methodologically similar study of how media users relate to data visualizations, and how these users have developed a "feeling for numbers" (Kennedy and Hill, 2018).

The ambivalent attitudes among social media users toward surveillance or monitoring technologies have been described by Barnes (2006) as "a privacy paradox," where users worry about being monitored by surveillance technologies yet do little to protect themselves against the mapping of their behavior in online environments. Research has also established that media users tend to worry more about social privacy, that is, a concern that specific others can receive sensitive information, rather than institutional privacy where the social media algorithms are collecting data for the benefit of individually targeted advertising (Bergstrom, 2015; Bolin, 2018; Jansson, 2010, 2012; Nissenbaum, 2004; Raynes-Goldie, 2010).

The literature, furthermore, explains gaps between privacy preferences and privacy practices, pointing out that mismatches between stated preferences and actual behavior can be related to desirable trade-offs for benefits over privacy (Kesan et al., 2016; Turow et al., 2015), informational deficiencies (Furini and Tamanini, 2015), cultural backgrounds (Trepte et al., 2017), or negative privacy experiences (Sarakakis and Winter, 2017).

The concept of privacy paradox, furthermore, is associated with the underlying topic of the relation between trust and technology. Trust is rooted in knowledge, experience, and agency of citizens (Botsnam, 2017), and the cultural shifts brought by the digitalization process have impacted upon how societies produce trust both at the interpersonal and institutional level. State institutions and social media platforms are both organizations of trust production and distrust management (Bodó, 2021). They are embedded in specific logics of trust formation to shape their own trustworthiness, but "digital intermediation has transformed the traditional logics of institutional trust formation and created new trust-mediating services" (Bodó, 2021: 2668). This also raises the question of "trust *in* trust mediating technologies" (Bodó, 2021: 2681). Empirically, Masso and Männiste (2018) analyze the perceived personal and institutional dangers to privacy in an Estonian setting. They use representative survey data to explore linkages between people's privacy concerns, their Internet and social media use habits, and several indicators of trust, and suggest that trust in institutions may be one of the key variables to explain variations in privacy concerns. Mathieu and Hartley-Møller (2021) have empirically studied relations between trust, data protection, and privacy among Danish media users, revealing five "heuristics" that audiences had developed, and where the degree of trust hinged upon the characteristics of the media organization, previous media standards, the context of use and purpose, the experiences of datafication, and, finally, the understandings of datafication (p. 1). The authors highlight another paradox related to dataveillance: citizens trust least the datafied media they use most.

A few studies have focused on media user attitudes in non-democratic settings. Liu (2022) explored public opinion about the Chinese social credit system and found that political elites (party members) surprisingly were less likely to support the surveillance regime comprising the social credit system. Martin et al. (2019) analyzed attitudes toward Internet surveillance by governments and companies in five Arab countries (Saudi Arabia, Tunisia, Lebanon, Qatar, and the UAE), and found that Arab nationals were more concerned about surveillance by companies, while expatriates worried more about government surveillance. Martin et al. (2020) studied self-expression attitudes in relation to Internet surveillance and found that South Asian expatriates were more concerned about surveillance than Emiratis and Qataris.

In sum, the ambivalence among media users toward dataveillance is nuanced, complex, and varies among individuals and national contexts. While previous research includes comparative studies, combinations of cross-cultural and intergenerational analysis are missing. To fill this gap, we will compare attitudes toward online state and corporate surveillance across three countries and two generations and explore a set of contextually relevant variables as their predictors.

Data and methods

In our comparative study, we focus on two generational cohorts: those who were brought up and had their formative years under totalitarian or authoritarian conditions (in Estonia and Portugal), and a younger cohort who has not experienced the same oppressive regime. Generation theory suggests that people's worldviews form during the *formative years* of youth, roughly between the ages of 17 and 25 (Mannheim, 1952 [1928]; cf. Bolin, 2016). Since Portugal became a democracy earlier than Estonia, we had to define the older generational cohort based on Portugal.

The first generational cohort was born in 1946–1953, having had their formative years during the authoritarian regime in Portugal or the Soviet time in Estonia (or in liberal democracy in Sweden). This cohort was between 21 and 28 years old when Portugal left authoritarian rule. The second generational cohort consists of people born between 1988 and 1995, with their formative years in the post-totalitarian/post-authoritarian period in Estonia and Portugal. This cohort had not yet reached their formative years at the time of the regaining of Estonia's independence in 1991.

The quantitative survey was conducted online by the Enkätfabriken market research company in September–November 2020. The respondents were recruited from the web panels of the research company and its partner organizations in all three countries, with the aim of achieving maximum representativity regarding geographical location and gender. The planned sample size was 3000 (500 for each age group in each country), and the actual sample size was 3221 respondents (1094 in Sweden, 1083 in Estonia, and 1044 in Portugal). In Estonia, the survey was conducted in two languages, Estonian and Russian (86% of the respondents identified themselves as ethnic Estonians, and 12% as Russians). The questionnaire included 34 questions (with a total of 133 variable items), among them several novel and original indicators, developed by the authors to measure the key concepts of the research project. Our analysis is mainly based on aggregated index variables, composed by summing the

values of several indicators used in the survey. The indices had good or acceptable internal consistency (see Appendix 1).

The main dependent index variables are as follows:

- *Tolerance toward online state surveillance*, consisting of five indicators: I do not mind that state authorities have access to my data on social media; The state authorities have every right to monitor their citizens' online communication to prevent terrorist attacks; The state authorities have every right to monitor their citizens' online communication to prevent violent protests or riots; The state authorities have every right to monitor their citizens' online communication to prevent foreign intervention (e.g. in elections); The state authorities have every right to monitor their citizens' digitally (use drones, apps, geo-local positioning) to prevent the spread of diseases; all measured on the scale *1—fully disagree . . . 4—fully agree*;
- *Tolerance toward corporate dataveillance*, consisting of seven indicators (adapted from Ofcom, 2019): I do not mind that private corporations have access to my data on social media, measured on the scale *1—fully disagree . . . 4—fully agree*; I am happy for companies to collect and use my personal information if . . . I get a personalized service in return—like a weather update on my phone (based on my location); They use it to show me adverts or information that might be more relevant to me; They use it to send me relevant special offers/discounts for products/services they think I might like; They are clear about how they will use my information; I can choose to opt-out at any point, and they will stop using my data; They reassure me they will not share my information with other companies; measured on the scale *0—doesn't apply to me; 1—applies to me*.

Other variables reported in this analysis are as follows:

- Age group: 0—*younger*; 1—*older*;
- *Experiences of state surveillance*, consisting of two indicators: Do you know anyone in [Sweden/Portugal/Estonia] who . . . has carried out his or her political or religious practices (reading books, listening to the radio, attending meetings) in secret to prevent negative consequences; . . . has been prevented from doing something (going abroad, entering a university, getting a particular job) due to the authorities' knowledge about his or her past, the family history, political views, etc.; *0—no; 1—no one in person, but I have heard such stories; 2—yes*;
- *Mediated experiences of state surveillance*, consisting of two indicators: Have you seen any movies, series, or documentaries, or read any books or articles about state surveillance; Have you heard any jokes or rumors about state surveillance; *0—no; 1—yes, 1 or 2; 2—yes, several*;
- *Importance of privacy*: seven indicators of aspects of privacy the respondent considers important in daily interactions—both online and offline (adapted from Pew Research Center, 2014); *1—not at all important . . . 4—very important*;

- *Support for freedom of expression*, consisting of two indicators (based on Finkel et al., 1999): All people should have a right to express their opinions; Media (e.g. TV, newspapers, websites) should have the right to criticize politicians and the government; *1—strongly disagree . . . 5—strongly agree*;
- *Support for a strong state*, consisting of two indicators (based on Funke, 2005): Our country needs a strong government that will move us in the right direction; Instead of needing "civil rights and freedoms" our country needs one thing only: law and order; *1—strongly disagree . . . 5—strongly agree*;
- *Trust in state institutions*: eight indicators of state institutions the respondent trusts (from the survey Me. The World. The Media, 2014; see Masso et al., 2020); *1—not at all . . . 5—completely*;
- *Trust in the media*: five indicators of media channels (including social media) the respondent trusts (from Me. The World. The Media, 2014); *1—not at all . . . 5—completely*;
- *Functional diversity of Internet use*: 17 indicators of the types of websites or apps the respondent uses (based on Me. The World. The Media, 2014; updated by the authors); *1—never . . . 6—every day*;
- *Digital skills*: 10 indicators of digital skills the respondent possesses (from EU Kids Online, 2017; see Smahel et al., 2020); *1—not at all true of me . . . 5—very true of me*;
- *Mobile device usage skills*: ten indicators of activities the respondent can do on a smartphone or tablet (from EU Kids Online, 2017); *0—no; 1—yes*.

First, we used univariate analysis of variance (factorial ANOVA) to compare the mean values of six key index variables across the age groups and the countries. The index variables were shortened (normalized) to comparable 4- or 5-point scales prior to the analysis. Second, we explored relationships between the dependent variables (attitudes toward online state surveillance and corporate dataveillance) and age, education, experiences of surveillance, trust, political attitudes, and digital media usage and skills by using a series of linear regression analyses. Due to many independent variables (17) in our initial models, we applied Bonferroni correction to estimate the significance of predictors more conservatively and included in the final models only those predictors that were significant at $p < .001$ in at least one country.

Results

Comparison of the countries and generation groups

We start our analysis from *experiences of state surveillance* (Figure 1). The factorial ANOVA demonstrated significant differences between the countries ($F = 66.89$, $p < .001$) and age groups ($F = 15.61$, $p < .001$), and the interaction between country and age was also significant ($F = 76.74$, $p < .001$). The older generations in Estonia and Portugal reported more experiences of state surveillance in their social networks, compared to their younger counterparts. The experiences of elderly Portuguese and Estonians also surpassed those of both generation groups in Sweden. Younger Swedes reported

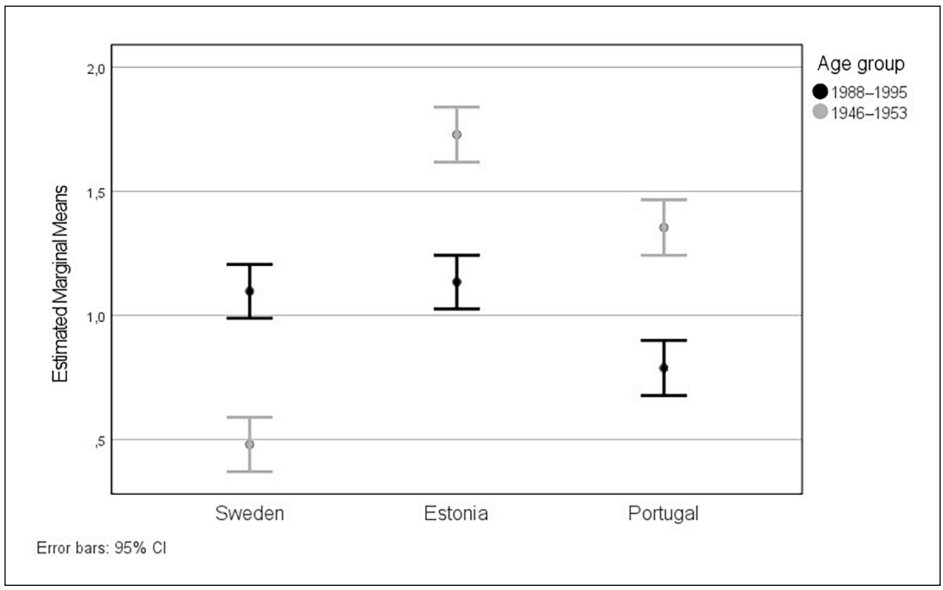


Figure 1. Experiences of state surveillance by countries and generation groups (estimated index means; 0—*lacking* . . . 4—*very high*).

significantly higher levels of experienced state surveillance, compared to their older compatriots. Younger Swedes, furthermore, demonstrated a higher level of *mediated experiences of state surveillance* (through films, documentaries, books, etc.) than older Swedes (Figure 2). Generational experience patterns regarding mediated state surveillance were completely different in two other countries, with the older age group in Portugal reporting more experiences through films, books, jokes, or rumors than the younger generation, while no intergenerational gap was revealed in Estonia. The country differences ($F = 44.88$) and the interaction between country and age group ($F = 52.83$) were significant at $p < .001$, with more mediated surveillance experiences reported in Estonia and Portugal.

Next, we examine trust as one of the key variables potentially explaining variations in attitudes toward privacy (Masso and Männiste, 2018) and surveillance. Figure 3 shows that the older generations in all three countries had a higher *trust in state institutions* compared to the younger cohorts ($F = 55.63$, $p < .001$). The levels of trust differed significantly between the countries ($F = 42.92$, $p < .001$), with Swedes, followed by Estonians, reporting higher trust in state institutions than Portuguese. The three countries differed significantly also regarding *trust in the media* (Figure 4), with Estonian respondents, followed by Swedish, surpassing the trust level of Portuguese ($F = 8.03$, $p < .001$). The pattern of intergenerational differences was mixed and statistically not significant.

When it comes to our main dependent variables, the older generation groups in all countries scored significantly higher than their younger compatriots ($F = 82.21$, $p < .001$) on *tolerance toward online state surveillance* (Figure 5). Differences between the

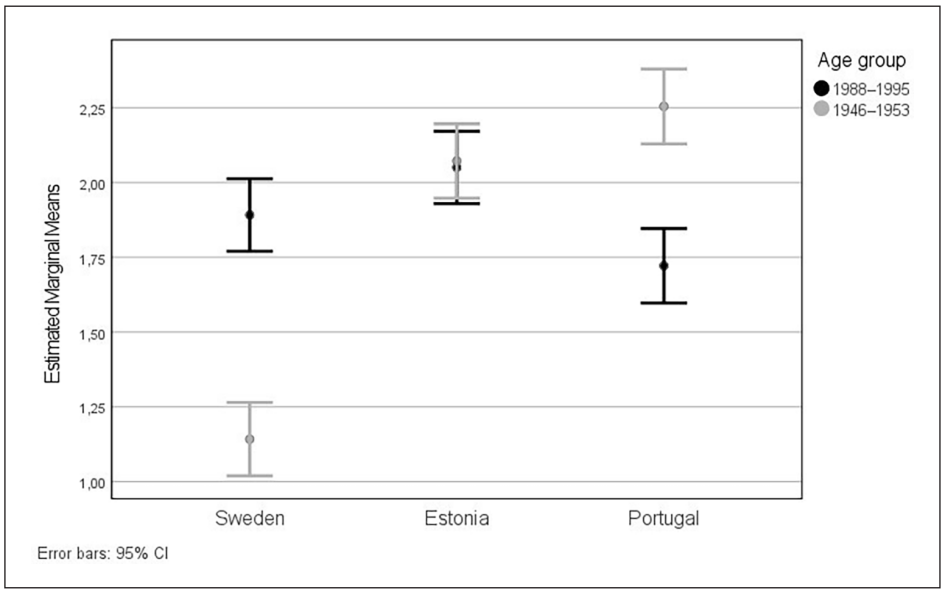


Figure 2. Mediated experiences of state surveillance by countries and generation groups (estimated index means; 0—*lacking* . . . 4—*very high*).

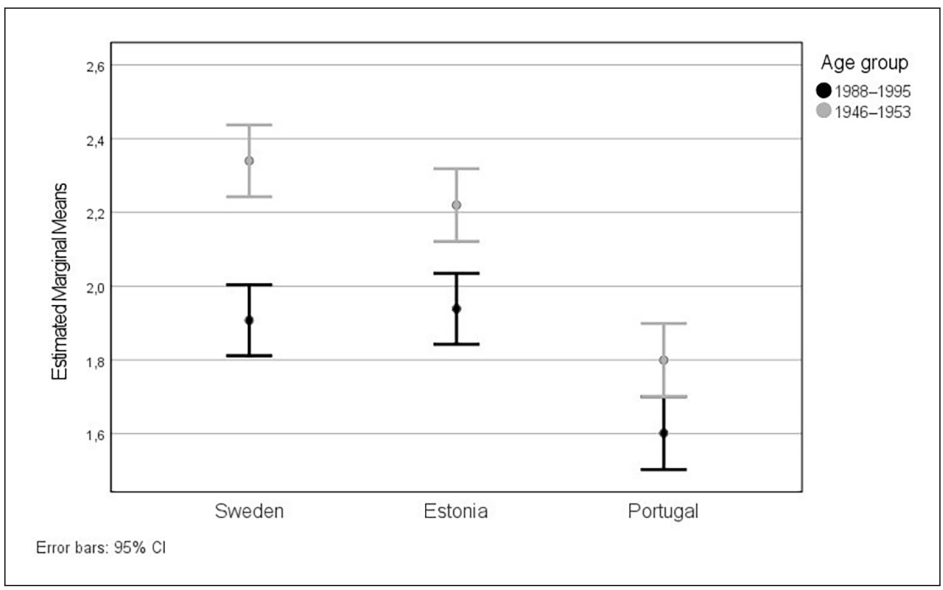


Figure 3. Trust in state institutions by countries and generation groups (estimated index means; 0—*lacking* . . . 4—*very high*).

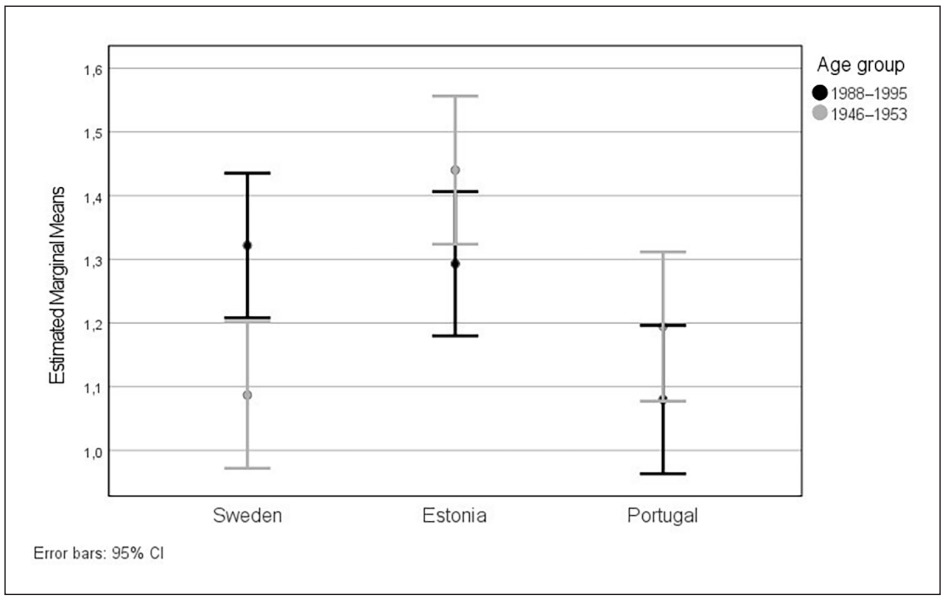


Figure 4. Trust in the media by countries and generation groups (estimated index means; 0—*lacking* . . . 4—*very high*).

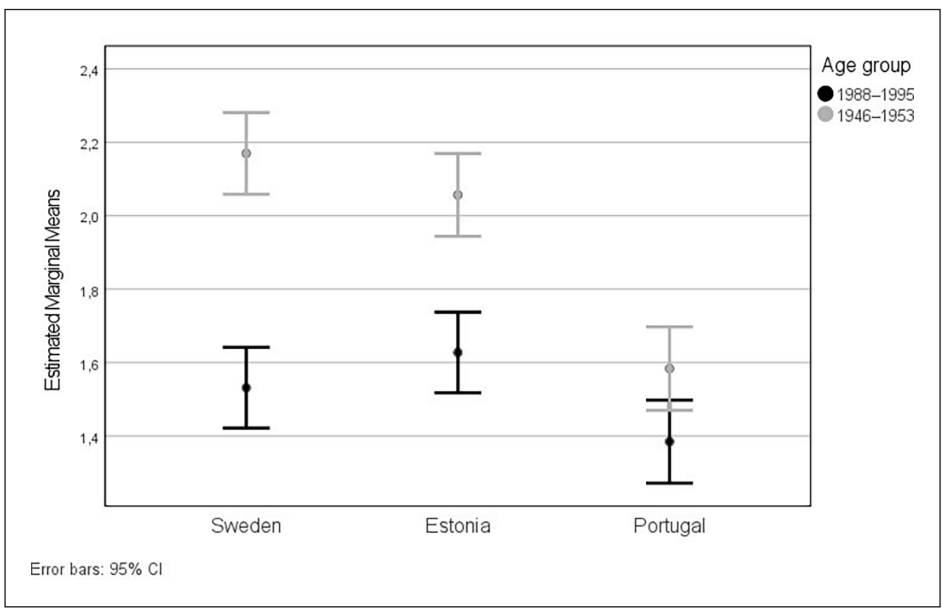


Figure 5. Tolerance toward online state surveillance by countries and generation groups (estimated index means; 0—*lacking* . . . 4—*very high*).

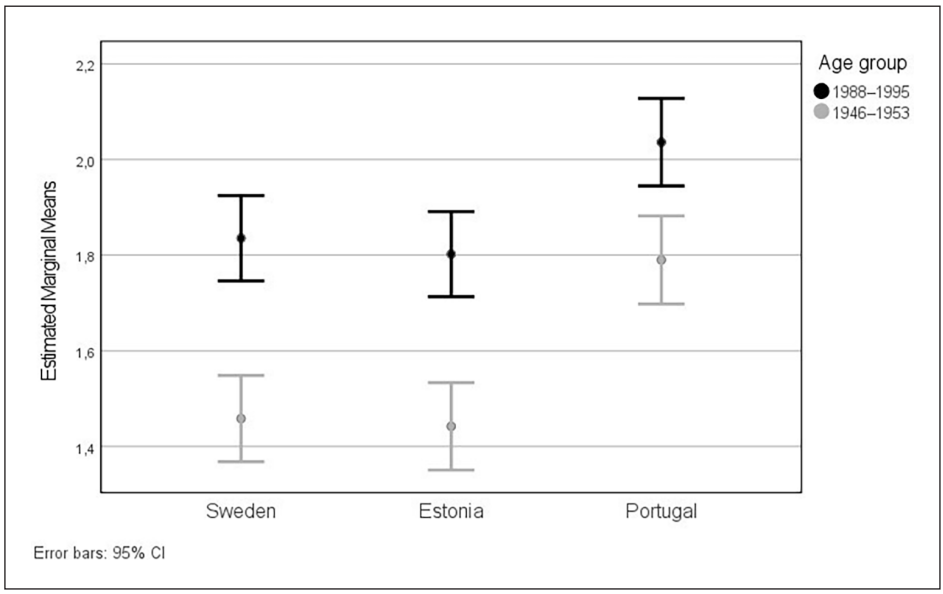


Figure 6. Tolerance toward corporate dataveillance by countries and generation groups (estimated index means; 0—*lacking* . . . 4—*very high*).

countries ($F=26.55$) and country–age interaction ($F=7.39$) were both significant at $p<.001$, with Swedes and Estonians being more tolerant than Portuguese. The intergenerational gap regarding *tolerance toward corporate dataveillance* was reversed in all countries (Figure 6), with younger people reporting significantly higher acceptance for companies to collect and use their personal information as a trade-off for services and benefits ($F=75.58$, $p<.001$). Interestingly, the pattern of country differences was reversed, too: Portuguese respondents were significantly more tolerant toward corporate dataveillance compared to Swedes and Estonians ($F=24.07$, $p<.001$).

To sum up, we can highlight two cross-culturally shared patterns of intergenerational differences. In all countries, the older generation groups scored significantly higher on *trust in state institutions* and *tolerance toward online state surveillance*. By collating this pattern with the observation of the older groups showing significantly higher *support for a strong state* compared to their younger compatriots ($p<.001$; Appendix 1), we may summarize that older generations in all countries are more trustful, conformist, and tolerant regarding state-run matters. Another cross-culturally shared pattern of intergenerational differences was reversed, with younger groups in all countries reporting significantly higher *tolerance toward corporate dataveillance*.

The country context played a significant role regarding all variables used in our comparative analysis. Sweden stuck out by least *experiences*—both actual and mediated—of state surveillance. Estonia was distinguished by the highest levels of reported *experiences of state surveillance* and *trust in the media*. Portugal stood out by the lowest levels of trust—both in *state institutions* and *the media*—and the lowest *tolerance toward*

online state surveillance, contrasted with the highest *tolerance toward corporate dataveillance*. Sweden and Estonia were quite like each other, and different from Portugal, regarding attitudes toward both types of contemporary surveillance and trust in state institutions.

Country–age interaction was significant in the case of four observed variables (actual and mediated *experiences of state surveillance, trust in the media*, and *tolerance toward online state surveillance*).

What predicts tolerance of state and corporate surveillance?

Tolerance toward online state surveillance and tolerance toward corporate dataveillance were strongly correlated (Pearson $r = .236$; $p < .001$): in general, those who tended to grant state authorities every right to monitor their citizens' online communication were also happier for companies to collect and use their personal information under certain conditions. Regression analyses, however, showed that these two attitudinal components had different predictors (Table 1). *Tolerance toward online state surveillance* was, in all countries, strongly predicted by higher tolerance toward corporate dataveillance, trust in state institutions, and lower importance of privacy.

Some noteworthy country-specific nuances were revealed: in Sweden, the second strongest predictor of tolerance toward online state surveillance was support for a strong state, followed by older age, lower importance of privacy, and trust in state institutions. Interestingly, Sweden was the only country where a media-related indicator played a significant role in the model predicting tolerance toward online state surveillance: Swedes with lower mobile device usage skills (who tend to be older people) were more tolerant toward state surveillance. Furthermore, in Sweden, older age was a stronger predictor of tolerance toward online state surveillance ($\beta = .217$; $p < .001$) compared to Estonia ($\beta = .121$; $p < .001$) and Portugal ($\beta = .073$; $p = .021$). This suggests that age and generation-specific features play a more significant role in Sweden where the generation gap regarding trust in state institutions and tolerance toward online state surveillance was steeper compared to Estonia and Portugal (see Figures 3 and 5).

Tolerance toward corporate dataveillance was clearly correlated to media-related practices, skills, and attitudes. In all countries, tolerance toward corporate dataveillance was best predicted by tolerance toward online state surveillance, and strongly correlated with functional diversity of Internet use, trust in the media, and digital skills. In other words, more active, skilled, and trustful users of digital media tended to be more at ease with companies collecting and using their personal information. Younger age was a significant predictor of tolerance toward corporate dataveillance only in Sweden, suggesting, again, that generation-specific features play a more significant role in Sweden compared to other countries. Importance of privacy was positively correlated with tolerance toward corporate dataveillance in Portugal (and less strongly in Sweden), while the direction of this relationship was reversed in all countries in the case of tolerance toward online state surveillance. A likely explanation is that corporate dataveillance is not perceived as a serious threat to personal privacy, while state surveillance practices are seen as potentially corrupting this value.

Table 1. Predictors of tolerance toward online state surveillance and corporate dataveillance (linear regression models; standardized regression coefficients).

Predictors	Dependent variable: Tolerance toward online state surveillance			Dependent variable: Tolerance toward corporate dataveillance		
	Sweden	Estonia	Portugal	Sweden	Estonia	Portugal
Age group (0–1)	**.217**	**.121**	.073	**−.105**	−.008	−.036
Tolerance toward corporate dataveillance	**.253**	**.265**	**.323**	–	–	–
Tolerance toward online state surveillance	–	–	–	**.278**	**.270**	**.301**
Importance of privacy	**−.205**	**−.142**	**−.162**	.052	−.023	**.121**
Support for freedom of expression	**−.168**	−.052	−.061	–	–	–
Support for a strong state	**.237**	**.082**	.078	–	–	–
Trust in state institutions	**.201**	**.267**	**.156**	–	–	–
Trust in the media	–	–	–	**.113**	**.113**	**.103**
Functional diversity of internet use	–	–	–	**.094**	**.156**	**.166**
Digital skills	–	–	–	**.167**	**.124**	**.085**
Mobile device usage skills	**−.116**	−.042	−.038	**.132**	.102	.031
N	1094	1083	1044	1094	1083	1044
R	.499	.462	.402	.443	.437	.442
Adjusted R^2	.244	.208	.156	.191	.185	.190

Statistically significant regression coefficients (at $p < .007$, after Bonferroni correction) are in bold.

Interestingly, in our initial models, actual or mediated experiences of state surveillance did not predict tolerance toward either type of contemporary surveillance in any country. Thus, attitudes, values, and mindsets, rather than past or mediated experiences of authoritarianism and surveillance, play a role in accepting state or corporate surveillance under certain conditions.

Concluding discussion

This study contributed to understanding the complexity of factors influencing attitudes toward contemporary surveillance, including the socio-historical context, the generational belonging, and a set of other variables.

First, our analysis revealed cross-cultural differences in the experiences of surveillance: the older generations in Estonia and Portugal reported more experiences of state surveillance in their social networks, compared to their younger counterparts and both generation groups in Sweden. This finding was expected, considering the distinct historical contexts of the three countries. A bit surprisingly, younger Swedes reported higher levels of actual experiences of state surveillance, compared to their older compatriots. As the younger generation in Sweden also demonstrated a higher level of mediated experiences of state surveillance than their older compatriots did, they may have become more aware, observant, and critical about various instances of state surveillance also in real life. Another explanation is that state surveillance has increased in Sweden, both in terms of the volume of surveillance technologies and the media reporting of state surveillance.[1] The increasing surveillance probably affects younger cohorts more than older people, since the young spend more time on the Internet and are, thus, more subject to and aware of online surveillance.

The three countries, furthermore, differed in all surveillance-related attitudes. Sweden and Estonia displayed similarly higher levels of trust in state institutions and tolerance toward online state surveillance, and lower tolerance toward corporate dataveillance, compared to Portugal. The latter stood out also by the lowest trust in the media.

Country–age interaction was significant in the case of four (out of six) observed variables. This suggests that the socio-historical context plays a role in molding the direction and/or magnitude of intergenerational gaps in some surveillance-related mental phenomena. The pattern of intergenerational differences regarding trust in state institutions, support for a strong state, and tolerance toward the two types of surveillance was, however, surprisingly similar in all three countries. The older generations demonstrated, despite their varying socialization contexts and experiences of state surveillance, higher levels of trust in state institutions, support for a strong state, and tolerance toward state surveillance compared to their younger compatriots.

Distinct factors, depending on the country-specific background, may help to explain these complex patterns. In Sweden, the older generation came of age during the "golden age" of the welfare state in the 1950s and 1960s and spent most of their lives at the height of it. As they now see the welfare regime being dismantled, they may want to return to the perceived social order of bygone days. In Estonia, the older generation grew up under the Soviet occupation, but many perceived the totalitarian regime as alien, and, despite severe acts of repression, never lost hope in the restoration of their own state (Lauristin

and Vihalemm, 2020). Their more conformist and tolerant mindset toward state-run matters may result from the combined influence of authoritarian socialization experiences and a genuine trust in regained independent statehood, perceived as radically different from the oppressive Soviet state. The overall similarity to Sweden in terms of trust and tolerance toward state matters is in line with Kalmus et al. (2018), who have shown an increasing trust in state institutions in Estonia in the re-independence period, making it comparable with several "old" European Union (EU) countries. The high level of trust in Estonian e-governance and digital services (Ehin et al., 2022) probably contributes to this pattern.

In Portugal, democracy grew out of a rare mix of a social revolution, an active cultural change, and a conventional democratization process (Fishman, 2019), and the role played by the state in the vast transformation was paramount (Pires and Nunes, 2005). All this combined may have shaped a new set of meanings given to the Portuguese state that may explain higher levels of trust in state endeavors among the older generation. Lower levels of trust in state institutions and the media, compared to Estonia and Sweden, can be explained by the low levels of civic capital (Ramos and Magalhães, 2021), perceived vulnerability to government and economic interests, and the structural deficit of information in Portuguese society (the lower the level of knowledge about an institution, the lower the level of trust attributed to it).

Second, we can state that tolerance toward online state surveillance and tolerance toward corporate dataveillance are related: in all three countries, those respondents who tended to grant state authorities the right to monitor the citizens' online communication were also more permissive toward companies collecting and using their personal information under certain conditions. This suggests that attitudes toward diverse types of contemporary surveillance may stem from common values or personality characteristics (such as insecurity; cf. Furnham and Swami, 2019; Svenonius and Björklund, 2018).

Beyond shared underlying factors, tolerance toward online state surveillance and tolerance toward corporate dataveillance were generation-specific and had different predictors. Tolerance toward online state surveillance was, in all countries, more characteristic of the older age group, and it was predicted by trustful, obedient, and less individualistic attitudes toward state authorities and other institutions (tolerance toward corporate dataveillance, trust in state institutions, lower importance of privacy, and support for a strong state). This relationship pattern can be interpreted as a pragmatic trade-off for safety and security—conservative and collectivist values according to the Schwartzian system (Schwartz, 1990)—which are more common to older generations in post-industrial and ex-communist societies and are gradually changing through individualization and intergenerational replacement (Inglehart and Welzel, 2005). We should reckon, however, that besides value-based pragmatism, tolerance may stem from lack of agency and/or awareness of contemporary surveillance mechanisms. If this is the case, the role informational deficiencies (Furini and Tamanini, 2015) play in amplifying vulnerabilities of older groups may further the "grey digital divide" (Morris, 2007) and accentuate the negative impacts of surveillance, worth exploring in further research.

Tolerance toward corporate dataveillance was, in all countries, more characteristic of the younger age group, and it was predicted (besides tolerance toward online state surveillance) by active and self-confident (online) media use (functional diversity of

Internet use, trust in the media, and digital skills). Evidently, such tolerance functions as an interchange for numerous benefits and services offered by social media and online companies, especially for the younger people. Such trade-offs may be read as a way of balancing uneven power relations between users and corporations, while nevertheless, contributing to both the reinforcement of a business model based on the extraction of data from online media users (van Dijck et al., 2018) and the normalization or naturalization of dataveillance as users consider such a practice unavoidable (Mathieu and Hartley-Møller, 2021). Complementary ways of explaining the younger generation's higher tolerance of corporate dataveillance could be seeing this as lack of full awareness of the risks involved, or avoidance of questioning one's routinized practices as a mode of coping with the cognitive dissonance arising from "a privacy paradox" (Barnes, 2006).

Tolerance toward either type of contemporary surveillance was not predicted by individual-level experiences of state surveillance in any country. This, together with other findings, suggests that global cultural and technological developments, forming generational values, mindsets and practices, and individual-level trade-offs are probably more powerful factors behind generation-specific attitudes than past experiences of authoritarianism and surveillance regimes. The survey data do not permit any solid conclusions about the formation of surveillance-related thought patterns, and our hypothetical explanations might be followed up in future research.

Methodological considerations and limitations

The indicators we elaborated or adapted for our comparative survey revealed significant and meaningful relationship patterns in the analyses, thus demonstrating sound construct validity, and the aggregate variables (indices) had good or acceptable internal consistency. The main methodological contribution of this article, thus, consists in developing some new measures for studying surveillance-related experiences, attitudes, and mindsets in quantitative surveys. A limitation lies in the sample consisting exclusively of Internet users, not being representative of the whole generation groups (especially the older). The results call for further explorations, also through qualitative methods that can reveal diverse experiences, narratives, and meanings as well as more nuanced motivations and arguments for trust or distrust in state institutions and the media, and tolerance toward online surveillance.

Statement of confirmation

We, as authors, hereby confirm that we have agreed to the submission. We also confirm that the manuscript is not currently being considered for publication by any other print or electronic journal.

Funding

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: The preparation of this article was supported by a grant from The Bank of Sweden Tercentenary Foundation (P19-0822:1).

ORCID iD

Veronika Kalmus https://orcid.org/0000-0002-1939-5706

Note

1. There were intense debates in Sweden following the hastily established legislation for increased signal traffic surveillance in 2008, and Swedish news media have reported about online surveillance. Bjereld and Oscarsson (2009) reveal that 90% of the Swedish population was aware of the controversial law, and the majority of those who had an opinion were against the law. Interestingly, the age pattern was like our findings: younger cohorts were far more negative and far more engaged, compared to older cohorts, who were more positive regarding the extended surveillance possibilities. The debates, furthermore, might have sensitized the Swedish population to the problematic.

References

Andrejevic M (2007) *iSpy: Surveillance and Power in the Interactive Era*. Lawrence, KS: The University Press of Kansas.

Andrejevic M and Gates K (2014) Big Data surveillance. *Surveillance & Society* 12(2): 185–196.

Bacelar de Gouveia J (2021) CyberLaw and CyberSecurity. *Revista Jurídica Portucalense* 29: 59–77.

Barnes SB (2006) A privacy paradox: social networking in the United States. *First Monday*. Available at: http://journals.uic.edu/ojs/index.php/fm/article/view/1394/1312

Bergstrom A (2015) Online privacy concerns: a broad approach to understanding the concerns of different groups for different uses. *Computers in Human Behavior* 53: 419–426.

Bermejo F (2009) Audience manufacture in historical perspective: from broadcasting to Google. *New Media & Society* 11(1–2): 133–154.

Bjereld U and Oscarsson H (2009) Folket och FRA. In: Holmberg S and Weibull L (eds) *Svensk Höst*. Göteborg: SOM-institutet, pp. 293–298.

Bodó B (2021) Mediated trust: a theoretical framework to address the trustworthiness of technological trust mediators. *New Media & Society* 23(9): 2668–2690.

Bolin G (2011) *Value and the Media: Cultural Production and Consumption in Digital Markets*. Farnham: Ashgate.

Bolin G (2016) *Media Generations: Experience, Identity and Mediatised Social Change*. London and New York: Routledge.

Bolin G (2018) Media use and the extended commodification of the lifeworld. In: Bilić P, Primorac J and Valtýsson B (eds) *Technologies of Labour and the Politics of Contradiction*. London: Palgrave Macmillan, pp. 235–252.

Bolin G and Jerslev A (2018) Surveillance through media, by media, in media. *Northern Lights* 16(1): 3–21.

Botsnam R (2017) *Who Can You Trust? How Technology Brought Us Together and Why It Might Drive Us Apart*. New York: Public Affairs.

Cadwalladr C (2018) Revealed: how 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. *The Guardian*, 17 March. Available at: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

Clarke RA (1988) Information technology and dataveillance. *Communications of the ACM* 31(5): 498–512.

Comissão Nacional de Proteçãode Dados (CNPD) (2022) Comissão Nacional de Proteçãode Dados. Available at: https://www.cnpd.pt/comunicacao-publica/noticias/cnpd-ordena-elim

inacao-dos-dados-das-comunicacoes-conservados-ao-abrigo-de-norma-declarada-inconstitucional/ (accessed 13 August 2022).
Costa Pinto A and Adinolfi G (2014) Salazar's 'new state': the paradoxes of hybridization in the fascist era. In: Costa Pinto A and Kallis A (eds) *Rethinking Fascism and Dictatorship in Europe*. New York: Palgrave Macmillan, pp. 154–175.
Draper N and Turow J (2019) The corporate cultivation of digital resignation. *New Media & Society* 21(8): 1824–1839.
Ehin P, Solvak M, Willemson J, et al. (2022) Internet voting in Estonia 2005–2019: evidence from eleven elections. *Government Information Quarterly* 39(4): 101718.
Figueiras R (2019) The role of mediatisation in the dynamic stabilisation of surveillance capitalism. In: Jakobsson P and Stiernstedt F (eds) *Fritt från fältet—Om medier, generationer och värden*. Huddinge: Södertörn University, pp. 169–186.
Finkel SE, Sigelman L and Humphries S (1999) Democratic values and political tolerance. In: Robinson JP, Shaver PR and Wrightsman LS (eds) *Measures of Political Attitudes*. San Diego, CA: Academic Press, pp. 203–296.
Fishman R (2019) *Democratic Practice: Origins of the Iberian Divide in Political Inclusion*. Oxford: Oxford University Press.
Flyghed J (2006) *Det hotande övervakningssamhället*. Framtider no. 4/2006. Stockholm: Institutet för framtidsstudier.
Fuchs C, Boersma K, Albrechtslund A, et al. (eds) (2011) *Internet and Surveillance: The Challenges of Web 2.0 and Social Media*. New York: Routledge.
Funke F (2005) The dimensionality of right-wing authoritarianism: lessons from the dilemma between theory and measurement. *Political Psychology* 26(2): 195–218.
Furini M and Tamanini V (2015) Location privacy and public metadata in social media platforms: attitudes, behaviors and opinions. *Multimedia Tools and Applications* 74(21): 9795–9825.
Furnham A and Swami V (2019) Attitudes toward surveillance: personality, belief and value correlates. *Psychology* 10: 609–623.
Gandy O (1993) *The Panoptic Sort: A Political Economy of Personal Information*. Boulder, CO: Westview.
Gates K (2011) *Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance*. New York: New York UP.
Giroux H (2015) Totalitarian paranoia in the post-Orwellian surveillance state. *Cultural Studies* 29(2): 108–140.
Grass ML (2004) The legal regulation of CCTV in Europe. *Surveillance & Society (CCTV Special)* 2(2–3): 216–229.
Gunnartz K (2006) *Välkommen till övervakningssamhället*. Stockholm: Bokförlaget DN.
Haggerty KD and Ericson RV (2000) The surveillant assemblage. *British Journal of Sociology* 51(4): 605–622.
Inglehart R and Welzel C (2005) *Modernization, Cultural Change, and Democracy: The Human Development Sequence*. Cambridge: Cambridge University Press.
Introna LD and Wood D (2004) Picturing algorithmic surveillance: the politics of facial recognition systems. *Surveillance & Society* 2(2–3): 177–198.
Jansson A (2010) Integritetsrisker och nya medier. In: Holmberg S and Weibull L (eds) *Nordiskt ljus*. Göteborg: SOM-institutet, pp. 261–276.
Jansson A (2012) Perceptions of surveillance: reflexivity and trust in a mediatized world (the case of Sweden). *European Journal of Communication* 27(4): 410–427.
Kalmus V, Kõuts-Klemm R, Beilmann M, et al. (2018) Long-lasting shadows of (post)communism? Generational and ethnic divides in political and civic participation in Estonia. In: Wimmer J, Wallner C, Winter R, et al. (eds) *(Mis)understanding Political Participation:*

Digital Practices, New Forms of Participation and the Renewal of Democracy. New York and Abingdon: Routledge and Taylor & Francis, pp. 35−56.

Kasekamp A (2010) *A History of the Baltic States*. London: Palgrave McMillan.

Kennedy H and Hill RL (2018) The feeling of numbers: emotions in everyday engagements with data and their visualisation. *Sociology* 52(4): 830–848.

Kennedy H, Elgesem D and Miguel C (2015) On fairness: user perspectives on social media data mining. *Convergence* 21(4): 1–19.

Kesan JP, Hayes CM and Bashir MN (2016) A comprehensive empirical study of data privacy, trust, and consumer autonomy. *Indiana Law Journal* 91(2): 267–352.

Kosterich A and Napoli P (2016) Reconfiguring the audience commodity: the institutionalization of social TV analytics as market information regime. *Television & New Media* 17(3): 254–271.

Lauristin M and Vihalemm P (2020) The "Estonian way" of the post-communist transformation through the lens of the morphogenetic model. In: Kalmus V, Lauristin M, Opermann S, et al. (eds) *Researching Estonian Transformation: Morphogenetic Reflections*. Tartu: University of Tartu Press, pp. 33–73.

Leckner S (2018) Sceptics and supporters of corporate use of behavioural data: a study of attitudes towards informational privacy and internet surveillance in Sweden. *Northern Lights* 16(1): 113–132.

Liu C (2022) Who supports expanding surveillance? Exploring public opinion of Chinese social credit systems. *International Sociology* 37: 391–412.

Lutz C, Hoffmann CP and Ranzini G (2020) Data capitalism and the user: an exploration of privacy cynicism in Germany. *New Media & Society* 22(7): 1168–1187.

Lyon D (2015) *Surveillance after Snowden*. Cambridge and Malden, MA: Polity Press.

Mannheim K (1952 [1928]) The problem of generations. In: Mannheim K (ed.) *Essays in the Sociology of Knowledge*. London: Routledge and Kegan Paul, pp. 276–320.

Männiste M (2022) *Big data imaginaries of data pioneers: changed data relations and challenges to agency*. PhD Thesis, University of Tartu, Tartu.

Martin JD, Naqvi SS and Narwahg I (2020) Attitudes about censorship and Internet surveillance among South Asians and nationals in the Arab Gulf: predictors of digital self-expression values. *International Communication Research Journal* 55(1): 21–38.

Martin JD, Naqvi SS and Schoenbach K (2019) Attribute substitution and stereotypes about the online Arab public sphere: predictors of concerns about Internet surveillance in five Arab countries. *New Media & Society* 21(4): 1085–1104.

Masso A and Männiste M (2018) The role of institutional trust in Estonians' privacy concerns. *Studies in Transition States and Societies* 10(2): 22–39.

Masso A, Lauristin M, Opermann S, et al. (2020) Applying the morphogenetic perspective for the analysis of Estonian social transformations. In: Kalmus V, Lauristin M, Opermann S, et al. (eds) *Researching Estonian Transformation: Morphogenetic Reflections*. Tartu: University of Tartu Press, pp. 1–31.

Mathieu D and Hartley-Møller J (2021) Low on trust, high on use datafied media, trust and everyday life. *Big Data & Society* 8(2). DOI: 10.1177/20539517211059480.

Morris A (2007) E-literacy and the grey digital divide: a review with recommendations. *Journal of Information Literacy* 1(3): 13–28.

Nissenbaum H (2004) Privacy as contextual integrity. *Washington Law Review* 79(1): 119158.

Norris C, McCahill M and Wood D (2003) The growth of CCTV: a global perspective on the international diffusion of video surveillance in publicly accessible space. *Surveillance & Society* 1(2): 110135.

Obar JA and Oeldorf-Hirsch A (2020) The biggest lie on the Internet: ignoring the privacy policies and terms of service policies of social networking services. *Information, Communication & Society* 23(1): 128147.

Ofcom (2019) Adults' media use and attitudes report. Available at: https://www.ofcom.org.uk/research-and-data/media-literacy-research/adults/adults-media-use-and-attitudes (accessed 4 January 2022).

Pew Research Center (2014) Public perceptions of privacy and security in the post-Snowden era. Available at: https://www.pewresearch.org/wp-content/uploads/sites/9/2015/07/Privacy PanelTopline (accessed 2 February 2020).

Pimentel IF (2007) *A História da PIDE*. Lisboa: Temas e Debates.

Pires I and Nunes F (2005) Fluxos de Investimento Ibérico: Novas Formas de Invasão Territorial ou a Consolidação de um Espaço Económico Aberto e Gerador de Confiança Recíproca? In: *X Colóquio ibérico de Geografia "A Geografia Ibérica no Contexto Europeu,"* Évora, 22−24 September.

Pîrvu M (2021) The degradation of human rights and free press through the Pegasus software in the area of surveillance, as a threat to international security: a debate of civil liberties and censorship. In: *STRATEGIES XXI international scientific conference*, Bucharest, Romania, 9−10 December.

Priks M (2015) The effects of surveillance cameras on crime: evidence from the Stockholm subway. *The Economic Journal* 125: 289305.

Ramos A and Magalhães P (2021) *Os valores dos portugueses. Resultados do European Values Study*. Lisboa: Fundação Calouste Gulbenkian.

Raynes-Goldie K (2010) Aliases, creeping and wall cleaning: understanding privacy in the age of Facebook. *First Monday*. Available at: http://firstmonday.org/ojs/index.php/fm/article/view/2775/2432

Razaghpanah A, Nithyanand R, Vallina-Rodriguez N, et al. (2018) Apps, trackers, privacy, and regulators: a global study of the mobile tracking ecosystem. In: *Network and distributed systems security (NDSS) symposium*, San Diego, CA, 18−21 February.

Sarakakis K and Winter L (2017) Social media users' legal consciousness about privacy. *Social Media + Society* 3(1): 114.

Schwartz SH (1990) Individualism–collectivism: critique and proposed refinements. *Journal of Cross-Cultural Psychology* 21(2): 139157.

Smahel D, Machackova H, Mascheroni G, et al. (2020) *EU Kids Online 2020: Survey Results from 19 Countries*. London: London School of Economics and Political Science.

Svenonius O and Björklund F (2018) Explaining attitudes to secret surveillance in post-communist societies. *East European Politics* 34(2): 123151.

Trepte S, Reinecke L, Ellison NB, et al. (2017) A cross-cultural perspective on the privacy calculus. *Social Media + Society* 3(1). DOI: 10.1177/2056305116688035.

Trottier D (2012) *Social Media as Surveillance: Rethinking Visibility in a Converging World*. Farnham: Ashgate.

Trottier D and Lyon D (2012) Key features of social media surveillance. In: Fuchs C, Broersma K, Albrechtslund A, et al. (eds) *Internet and Surveillance: The Challenges of Web 2.0 and Social Media*. London: Routledge, pp. 89−105.

Turow J, Hennessy M and Draper N (2015) *The Tradeoff Fallacy: How Marketers Are Misrepresenting American Consumers and Opening Them Up to Exploitation*. Philadelphia, PA: Annenberg School of Communication.

Turow J, Hennessy M, Draper N, et al. (2018) Divided we feel: partisan politics drive Americans' emotions regarding surveillance of low-income populations. Annenberg research report, University of Pennsylvania, Philadelphia, PA.

van Dijck J (2014) Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology. *Surveillance & Society* 12(2): 197208.
van Dijck J, Poell T and de Waal M (2018) *The Platform Society: Public Values in a Connective World*. Oxford: Oxford University Press.
Weiner A and Rahi-Tamm A (2012) Getting to know you: the Soviet surveillance system, 1939–57. *Kritika: Explorations in Russian and Eurasian History* 13(1): 545.
Werbach K (2021) Panopticon reborn: social credit as regulation for the algorithmic age. *University of Illinois Law Review*. Available at: https://ssrn.com/abstract=3589804
Zuboff S (2015) Big other: surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology* 30(1): 7589.

Author biographies

Veronika Kalmus is Professor of Sociology at the Institute of Social Studies, University of Tartu, Estonia. She focuses on generations, socialization, mediatization, (new) media use, social changes, values, and discourses. She is a member of the section Film, Media and Visual Studies in Academia Europaea.

Göran Bolin is Professor of Media & Communication Studies at Södertörn University, Sweden. His research is focused on the relations between media production and media use in digital markets, and the implications of digitization and datafication on media use and production.

Rita Figueiras is Professor of Political Communication and Sociology of Communication at Universidade Católica Portuguesa, Portugal. Her research is focused on the relationship between media technology and power, news consumption, mediatization, and datafication.

Appendix 1. Descriptive statistics for dependent and independent variables by countries and age groups.

Variable			Total	Sweden		Estonia		Portugal	
Index	Reliability coefficient	Statistics		Younger	Older	Younger	Older	Younger	Older
Tolerance toward online state surveillance[a]	.887*	*M*	1.73	1.53	2.17	1.63	2.06	1.38	1.58
		SD	1.35	1.32	1.45	1.25	1.23	1.24	1.43
Tolerance toward corporate dataveillance[a]	.722*	*M*	1.73	1.84	1.46	1.80	1.44	2.04	1.79
		SD	1.09	1.10	1.05	1.05	1.10	1.01	1.11
Experiences of state surveillance[a]	.774**	*M*	1.09	1.10	0.48	1.13	1.73	0.79	1.35
		SD	1.36	1.34	0.90	1.35	1.54	1.15	1.42
Mediated experiences of state surveillance[a]	.705**	*M*	1.85	1.89	1.14	2.05	2.07	1.72	2.25
		SD	1.50	1.44	1.35	1.45	1.57	1.42	1.49
Importance of privacy[a]	.854*	*M*	3.88	3.25	3.55	4.07	3.59	4.51	4.34
		SD	1.34	1.49	1.33	1.16	1.42	0.95	1.10
Support for freedom of expression[a]	.633**	*M*	2.69	2.15	3.32	2.53	2.47	2.62	3.05
		SD	1.30	1.56	1.03	1.21	1.13	1.30	1.18
Support for a strong state[a]	.551**	*M*	1.65	1.38	2.30	1.11	1.27	1.80	2.05
		SD	1.30	1.31	1.40	0.98	1.12	1.16	1.32
Trust in state institutions[a]	.860*	*M*	1.97	1.91	2.34	1.94	2.22	1.60	1.80
		SD	1.18	1.25	1.17	1.14	1.07	1.11	1.17
Trust in the media[a]	.757*	*M*	1.24	1.32	1.09	1.29	1.44	1.08	1.19
		SD	1.37	1.41	1.20	1.30	1.34	1.43	1.48
Functional diversity of Internet use[b]	.830*	*M*	3.03	3.66	2.36	3.51	2.26	3.52	2.84
		SD	1.13	0.99	0.10	0.87	0.94	0.93	1.11
Digital skills[b]	.822*	*M*	3.11	3.19	2.68	3.64	2.68	3.61	2.84
		SD	1.04	1.09	0.94	0.82	0.93	0.93	1.05
Mobile device usage skills[a]	.763*	*M*	2.44	2.58	1.85	3.17	1.25	3.41	2.36
		SD	1.46	1.41	1.35	1.13	1.16	0.98	1.44
		N	3221	553	541	556	527	525	519

[a]Scale: 0—*lacking* . . . 4—*very high*.
[b]Scale: 1—*very low* . . . 5—*very high*.
*Cronbach's α; **Spearman–Brown coefficient (for two-item indices).