The Acceptance of Digital Surveillance in an Age of Big Data

Mika Westerlund, Diane A. Isabelle, Seppo Leminen

> “*Those who control the present, control the past and those who control the past control the future.*”
>
> George Orwell
> 1984

News media companies and human rights organizations have been increasingly warning about the rise of the surveillance state that builds on distrust and mass surveillance of its citizens. The COVID-19 pandemic is fostering digitalization and state-corporate collaboration, leading to the introduction of contact tracing apps and other digital surveillance technologies that bring about societal benefits, but also increase privacy invasion. This study examines citizens’ concerns about their digital identity, the nation-state’s intelligence activities, and the security of biodata, addressing their impacts on the trust in and acceptance of governmental use of personal data. Our analysis of survey data from 1,486 Canadians suggest that those concerns have negative impacts on citizens’ acceptance of governmental use of personal data, but not necessarily on their trust in the nation-state being respectful of privacy. Government and corporations, it is concluded, should be more transparent about the collection and uses of data, and citizens should be more active in “watching the watchers” in the age of Big Data.

Introduction

Prolific news media such as Bloomberg, Forbes and the Financial Times have increasingly warned about the rise of the “surveillance state” that “aims at preventive mass surveillance on [an] everyday basis” and is connected with potentially coercive use of control against specific people or groups on a political or other basis (Lemieux, 2020). Although Clark (2016) and Sekalala et al. (2020) point out that digitalization could broaden democratic engagement, many states and large corporations are increasingly using digital environments to monitor and direct citizens. The “Snowden leaks” in 2013 revealed the unprecedented scope and magnitude of state-corporate surveillance of our everyday digital activities in pursuit of “datafication” of social life (Milanovic, 2015; Dencik et al., 2016; Hintz et al., 2017). Indeed, Clarke (2019) argues that humanity has entered a period of living in a “digital surveillance economy”, where the acquisition and exploitation of large volumes of personal data through digital devices are used not only by governments for security purposes, but also by corporations to target advertisements, manipulate consumer behaviour, and maximize revenues from goods and services.

Evidently, various stakeholders consider data as a booster to innovation (Isabelle et al., 2020; Leminen et al., 2020a). However, advances in technology and the pervasive adoption of social media have dramatically increased the power of states and multinationals to carry out digital surveillance and even abuse personal online data (Taylor, 2002; Odoemelam, 2015; Sekalala et al., 2020). At the same time, public trust in government has declined in most developed countries (Chanley et al., 2000; Job, 2005; Zhao et al., 2017). Digital surveillance by the nation-state has been justified by the argument that such surveillance can protect people by preventing illegal and dangerous activities, thereby contributing to safety, security, and autonomy in society (Clark, 2016; Zhang et al., 2017). However, governments across the world have come under sharp criticism for their use of digital surveillance technologies to gather massive amounts of personal information, yet with little evidence of this mass surveillance being effective in improving security for users of digital tools (Zhang et al., 2017; Cayford & Pieters, 2018).

Clarke (2019) argued that the growing levels of digital surveillance may even wash away achievements over previous centuries for individual rights that protect humanity as a whole. Unsurprisingly, a notable resistance to surveillance can be seen regularly in media, political circles, and academia (Martin et al., 2009). Most recently, the debate involving digital surveillance has been intensified by the proliferation of contact tracing apps due to the COVID-19 pandemic, as well as the widespread protests that followed the death of George Floyd (Amit et al., 2020; Keshet, 2020; Maier, 2020; McGee et al., 2020; Ram & Gray, 2020; Sekalala et al., 2020). Also, the increasing remote surveillance of teleworkers by their employers (Rosengren & Ottosson, 2016) and the adoption of proctoring software in the educational sector to monitor online exams during the pandemic lockdowns have sparked fierce reactions and discussions across the world (Asher-Schapiro, 2020; Manokha, 2020a; Manokha, 2020b; Stott & Wiggins, 2020). These advancements bringing surveillance to our private homes beg a question: are there any areas left that are not under surveillance?

State-corporate surveillance certainly raises severe concerns about the invasion of privacy (Cayford & Pieters, 2018). Surveillance may have become a normalized key condition of living in a modern “techno-securitized society”, as a way to ensure collective security (Bennett, 2011; Bernal, 2016; Clark, 2016; Petit, 2020). Yet at the same time, individuals’ privacy concerns due to the introduction of ever more privacy-intrusive technologies are not unwarranted. The Snowden revelations on WikiLeaks showed that surveillance by the intelligence services of nation-states has not been limited to marginalized and deserving groups of “wrong-doers”, but rather digital surveillance can target anyone and everyone in a nation, society or community (Dencik et al., 2016). Organizations are attempting to benefit from data beyond the context it has been collected for to create new businesses (Leminen et al., 2018, 2020b). Further, the risk of inappropriate flows of sensitive data collected in one context and spread to another context has increased along with digitalization (Winter & Davidson, 2019). While public polls show that people are willing to share, for example, their medical data to serve the greater good during the COVID-19 pandemic, people also have reservations concerning governmental use of their personal data (Osborne, 2020). Subsequently, many human rights groups, such as Amnesty International, have warned against the expanding use of government surveillance and data collection during the pandemic. The use of digital technologies such as automated facial recognition to identify protesters on video or tracking of smartphones to collect user and location data for undisclosed purposes has also been flagged as potentially or already problematic (Maier, 2020).

This study addresses the calls in previous literature to better understand concerns that citizens have about the rise of digital surveillance amidst socio-technical changes (see for example, Bernal, 2016; Cayford & Pieters, 2018; Beduschi, 2019; Ram & Gray, 2020). Specifically, the study focuses on investigating whether citizens’ concerns about their digital identity, the state’s intelligence activities, and the security of biodata have impacts on their trust in and acceptance of governmental use of personal data. In so doing, the study establishes a set of hypotheses and tests the research model on open survey data from 1,486 Canadians. The results contribute to the growing literature on privacy and digital surveillance by showing both what hampers citizens’ trust in their government and what impacts their acceptance of the gathering and use of personal data for undisclosed purposes by agencies of the state. Further, the results can help citizens, public servants of nation-states, and corporations to find ways to establish common ground where state-corporate actors’ data needs meet citizens’ privacy rights.

The paper is structured as follows: Next, we review the literature on privacy and data security, and establish a set of hypotheses on the impacts of citizens’ concerns about digital identify, the state’s intelligence activities, and security of biodata. We discover it has an impact on their trust in the state respecting their privacy and on their acceptance of government gathering and using their personal data. Then, we describe the data set from the research and the methods of analysis. Thereafter, we report findings from the analysis. Finally, the study concludes by summarizing the key findings, discussing their implications for theory and practice, and suggesting the limitations of the study and avenues for future research.

Literature Review

Digital surveillance and privacy invasion

While "digital citizenship" refers to increased citizen empowerment in modern societies using digital technologies, digital surveillance has surfaced as a major challenge to this feeling of liberation (Hintz et al., 2017). Surveillance has gradually become so "pervasive and inextricably connected to our everyday activities" (Clement & Obar, 2015) that we unquestionably live in a "surveillance society" (Ibid). This leads us to ponder if there is any room for privacy anymore. Bernal (2016) portrays privacy as an individual right, in opposition to the collective need for security. Indeed, Bennett (2011) interprets privacy as an ego-centric concept that revolves around "the protection of the self, from the state, from organizations and from other individuals". State-corporate actors collecting data from citizens, according to these views and others, should take every effort to protect individual privacy (Amit et al., 2020).

However, the issue of privacy invasion is not necessarily due to the collection of personal data. Instead, the classification and assessment of that data may lead to discrimination based on profiling (Bennett, 2011). Although viewed as being essential for building a data-driven "digital welfare state" (van Zoonen, 2020), the introduction of various "citizen scoring" (Dencik et al., 2019) or "social sorting" systems (Lyon, 2014; Wang & Tucker, 2017) can discriminate citizens in terms of their access to health care, and oppress basic human rights. This can happen, for example, by blocking their ability to travel due to having a lower reputation rating and trustworthiness score on state-wide "social credit systems". Thus, consideration of harms that may arise due to mass surveillance by states and corporations should extend beyond mere privacy issues and incorporate a large variety of society-wide effects (Murray & Fussay, 2019).

Concerns about digital identity

Piecing together an individual's identity, for example, their religious beliefs, based on their social contacts and online behaviour, has become common in monitoring security threats after the 9/11 attacks and other acts of terrorism around the world (Marx, 2015; Odoemelam, 2015; Clark, 2016; Menichelli, 2017). Van den Broek et al. (2017) focus on the increased use of digital "crowd surveillance" technologies to identify individuals involved in public disorder events, such as violent demonstrations and sports hooliganism. Indeed, identifying "individuals in the context" is a key attribute in digital surveillance (Wang & Tucker, 2017), and intelligence authorities commonly use IP address data to obtain user identity information (Forcese, 2015). Digital identity and online behaviour are not just interesting for intelligence authorities, but are also crucial for various online platforms (Budak et al., 2017). According to Clarke (2019), contemporary business models rely on collecting and exploiting massive volumes of personal data to provide markets with improved customer experiences, increased convenience, and time-savings through targeted value propositions. However, the ability of large corporations and governments to monitor and store online behaviour data on a massive scale, actually serves to limit the possibilities of individuals from dissenting and protesting, and supports a form of governance that prioritizes certain social, economic, and political agendas at the expense of others (Dencik et al., 2016).

A recent study by Keshet (2020) suggested that issues of trust surfaced as a major challenge for people involving their government's increased digital surveillance of its citizens in order to monitor the spread of coronavirus and thus in a way control peoples' behaviour in the midst of COVID-19 pandemic. Veliz (2021) notes that the pandemic has accelerated digitalization in society and contributed to widening power asymmetries between consumers and "big tech" companies. Undeniably, privacy has become a critical issue as state-corporate actors seeking to obtain peoples' digital identity information have implemented new technologies and methods to gather that information. Accordingly, as those stakeholders "build on personal data for identification and identity verification, data protection and privacy rights are most clearly affected" (Beduschi, 2019). Taylor (2002) argues that "paradoxically, it is a demand for privacy that drives the need for surveillance and therefore greater privacy and so on," creating a self-perpetuating cycle.

Our starting hypotheses for the research, which we tested with survey data, begin as follows:

H1: Citizens' concerns about digital identity have a negative impact on their trust in the government respecting citizen privacy.

H2: Citizens' concerns about digital identity have a negative impact on their acceptance of governmental use of personal data.

Concerns about the nation-state's intelligence activities
According to Cayford and Pieters (2018), the purpose of a nation-state's intelligence activities is to provide information to help government officials in their decision-making, while not dictating what actions decision-makers should take. That said, Bernal (2016) pointed out that the information provided by Edward Snowden in 2013 revealed that the nature and depth of Internet and communications surveillance for intelligence and national security purposes differed remarkably from what had up to that point been acknowledged publicly. Traditionally, a nation-state's intelligence activities include "strategic intelligence" aimed at foreign governments to comprehend possible threats, as well as "tactical operations" targeted at specific individuals or groups of interest (Cayford & Pieters, 2018). However, recent state-led efforts to secure its citizens against global threats such as terrorism and espionage have turned almost anyone into a potential threat, and therefore likewise into a possible target of surveillance technologies (Petit, 2020). This has affected civil rights and basic freedoms (Milanovic, 2015), as exemplified by U.S. border agents "rightfully" searching travelers' smart phones, and requests by intelligence agencies for technology firms to install backdoors to encrypted services for the sake of national security.

While foreign surveillance for national security purposes may be legitimized in many countries, the surveillance of a nation's own citizens or, as revealed by Snowden leaks, the surveillance of leaders of allied governments is another matter both legally and morally (Milanovic, 2015). One problem is that, for example in Canada, the government's intelligence activities are somewhat free from parliamentary control. This means that Canadian citizens are left merely to trust the authorities without a possibility of verifying the legality of the government's intelligence activities (Israel, 2015). Cayford and Pieters (2018) thus argue that the government and its surveillance officials need to be more transparent and "lead in education for the public", because democracy and surveillance programs can only work as long as the public trust their leaders and authorities, including intelligence agencies. Such education should address what data are being collected and for what purposes. Public trust in authorities depends heavily on the belief that authorities will not and do not misuse personal data, and act fairly when dealing with the public (Cayford & Pieters, 2018; Veliz, 2021). For example, according to Bernal (2016), people perceive "content" gathering for intelligence purposes as more intrusive compared to gathering contextual "metadata". Consequently, content gathering may be excessive data collection, which can lower public trust in the government. That said, effective algorithmic and artificial intelligence-driven "bulk data" monitoring and analysis nowadays have narrowed down the differences between content and metadata into the information value of data (Murray & Fussey, 2019). Thus:

H3: Citizens' concerns about the nation-state's intelligence activities have a negative impact on their trust in the government respecting citizen privacy.

H4: Citizens' concerns about the nation-state's intelligence activities have a negative impact on their acceptance of governmental use of personal data.

Concerns about biodata security
Biometric technologies are further redefining privacy boundaries, as they "do not just involve collection of information about the person, but rather information of the person, intrinsic to them" (Bennett, 2011). Indeed, biometric data such as facial topographies and fingerprints stored in digital databases for recognition purposes bring about new levels of aggregation involving privacy issues (Martin et al., 2009; Bernal, 2016). For example, biometric security technology used at airports allows for passengers to "clear security based on their unique biometric features" (Kim et al., 2020). Border control services across the world are increasingly adopting biometric security technologies such as fingerprints, iris scanning and facial recognition, to replace or complement passport-based entry management at national borders (Lyon, 2007; Marin, 2017).

However, previous research has shown that perceived risks related to biodata have an impact on passengers' intentions to use biometric security (Kim et al., 2020). Ebelogu et al. (2019) add that such risks are linked to privacy due to security concerns. Public polls have frequently indicated that people may perceive the current legal privacy protection frameworks as insufficient because of deficient implementation of laws and weak control mechanisms (Budak et al., 2017).

Commercial and governmental gathering of personal data are often considered as separate and different, without explicit links between the two. For example, Martinez-Marin and Char (2018) argued that monetization exceeds the altruistic interest in improving patient health as a motivator behind private industry development and investment in data-based digital health solutions. However, several scholars (for example, Richards, 2013; Bernal, 2016; Van den Broek et al., 2017) have suggested that public and private surveillance are simply related parts of the same problem, noting that authorities are increasingly being provided with access to biodata records owned by commercial firms. The benefits of such public-private collaboration are evident in solving "cold crime cases", most notoriously the Golden State Killer who was tracked and sentenced to life imprisonment decades after the crimes took place by comparing DNA data from crime scenes with data files on a genealogy website that has over one million DNA profiles from commercial DNA companies (Guerrini et al., 2018). Dedrickson (2018) argues that such DNA databases can be effective in solving crimes, exonerating the innocent, and decreasing racial disparities in law enforcement, thus contributing to social justice and the common good, rather than being a type of "Big Brother" invasion of privacy. On the other hand, access to large facial topography and genetic profile databases could be misused by authoritarian governments to control their own people, potentially focusing on certain ethnic minorities, political movements, or other targeted populations (Wee, 2020; Fox Cahn, 2021).

Without a doubt, the COVID-19 pandemic has accelerated beneficial public-private collaboration regarding data collection and use. Examples include the use of mobile location data to monitor social distancing and quarantine enforcement as well as contact tracing, warning about exposure to COVID-19, modelling patterns, and the flow of coronavirus spread. As well, the creation of new medical databases related to the pandemic, and the use of thermal cameras and wearables to collect relevant biometric data such as skin temperature, heart rate, and breathing (Amit et al., 2020; Kitchin, 2020; Guinchard, 2020). On the other hand, Ram and Gray (2020) argue that policy makers need to consider in a more profound way the efficacy and comparative advantages of tracking apps vis-à-vis more traditional means of controlling and containing epidemic contagion in order to avoid substantial risks to privacy. State-corporate collaboration has likewise served to increase the risks of uncontrolled and illegal sharing of biodata (Guinchard, 2020), privacy violations and abuse of data, either by the government (Sekalala et al., 2020) or for-profit companies due to commercial interests (Klingner et al., 2017). Examples of governmental misuse of biodata include the large number of unauthorized searches by NYPD officers on private facial recognition platforms (Fox Cahn, 2021). Hence:

H5: Citizens' concerns about biodata security have a negative impact on their trust in the government respecting citizen privacy.

H6: Citizens' concerns about biodata security have a negative impact on their acceptance of government using personal data.

Trust in and acceptance of governmental use of data

Surveillance authorities can no longer simply ask people to trust them, while at the same time providing worrisome indications that they may not be trusted themselves (Bernal, 2016). The evermore obvious rise of the surveillance state builds on suspicion and distrust, while society's legal, technical, and bureaucratic systems are designed for extensive surveillance because people are assumed to be inherently untrustworthy (Bernal, 2016). Thus, it is not surprising that citizens may feel distrustful of the government and authorities, since they are being treated with distrust themselves (van Zoonen, 2020). Indeed, Clement and Obar (2015) argued that the growing implementation of digital mass surveillance technologies has hindered "the government's ability to protect the integrity of its communications with citizens", thus undermining citizens' trust in governmental institutions. Bernal (2016) noted that lower levels of citizen trust in the nation-state's intentions to gather and use personal data correlate with a lower level of citizen cooperation with authorities. Further, Cayford and Pieters (2018) suggested that public trust in authorities is linked with the government's ability to run sustainable long-term surveillance programs. Overall, public trust in government has declined in developed countries dramatically over recent decades, while surveillance has not decreased, but rather increased (Chanley et al., 2000; Job, 2005; Zhao et al., 2017).

Technological advances have played a key role in the emergence of the "surveillance state", with rising levels of state surveillance. Surveillance technology has rapidly expanded from cold war era spy technology, such as wiretaps and hidden, or CCTV cameras, to modern spy drones and satellites, as well as various technological and often autonomous systems for targeted and untargeted cyber surveillance. These systems include artificial intelligence technologies to monitor and analyze phone calls, emails, keystrokes, private messaging, social media, videos and photographs, digital device use, geospatial data such as mobile phone location, sensor data including audio and other information collected by Internet of Things (IoT) devices such as virtual assistants, as well as internet traffic and online activity such as clicks, browsing history, online searches, downloads and uploads (Hogan & Shepherd, 2015; Odoemelam, 2015; Watt, 2017; Cayford & Pieters, 2018). Marx (2015) notes that state-corporate surveillance has historically involved power imbalance that favours more powerful actors. Given that the contemporary times may be described as "the age of big data surveillance", Hogan and Shepherd (2015) and Odoemelam (2015) argue that there are few options available for citizens to subvert the transcendent power of current governmental surveillance organizations, thus emphasizing the role of trust in adapting to mass surveillance in society. Hence:

H7: Citizens' trust in the government respecting citizen privacy has a positive impact of their acceptance of governmental use of personal data.

Next, the paper discusses the data and methods of analysis used for testing our hypotheses.

Methods

The study makes use of survey data on Canadians' perceptions about privacy in the digital era. A random-digital dialing telephone survey was conducted in 2018-2019 among Canadian residents, 16 years of age or older, by Phoenix Strategic Perspectives Inc. (Phoenix SPI), a research firm commissioned by the Office of the Privacy Commissioner of Canada (OPC). The data set is publicly and freely available as open data through OPC Communications Directorate website (OPC, 2020) under the "Open Government Licence —Canada". The data set includes anonymous responses from 1,516 residents, but we filtered out those who reported that they do not use the Internet or do not own a cell phone, thus resulting in a final data set of 1,486 usable responses. Of note, previous literature discusses Canadian perspectives on mass surveillance. For example, Geist (2015) argues that the issues of privacy and surveillance in Canada remain largely in the public eye, and thus Canada provides a specifically fruitful context for this kind of research, though we make no assessment of Canada's specific suitability for the research conducted here.

Our hypotheses about the impacts of citizens' concerns regarding their digital identity, the nation-state's intelligence activities, and security of biodata on their trust in and acceptance of government's use of personal data were tested using SmartPLS 3.3.2 software (Ringle et al., 2015). It enabled us to use partial least squares structural equation modelling (PLS-SEM), a variance-based statistical modelling technique that is widely applied in business and social science research (Henseler et al., 2016). PLS-SEM is particularly useful for studying new topics in information technology (Henseler et al., 2016; Hair et al., 2017), because of its capacity to test behavioural models with minimum demands regarding measurement scales and residual distributions (Monecke & Leisch, 2012).

Each of the five constructs in our model was measured by 2-3 variables. In order to align all constructs to reflect citizens' concerns, we reverse-coded variables related to the nation-state's intelligence concerns. Item loadings of all constructs were above the 0.70 threshold, along with >0.70 Composite Reliability (CR) (Lindell & Whitney, 2001) and >0.50 Average Variance Extracted (AVE) values (Henseler et al., 2016). These values indicate convergent validity and suitability of the constructs for this analysis (Table 1). The Fornell-Larcker Criterion suggested sufficient discriminant validity (Fornell-Larcker, 1981) and the standardized root mean square residual (SRMR) was 0.088, suggesting an acceptable model fit (Henseler et al., 2016). Finally, the model showed R^2=12.1% of trust and R^2=14.8% of acceptance of governmental use of personal data.

Findings

The results from the PLS-SEM analysis confirm most of our hypotheses. First, the results confirm that citizens' concerns about their digital identity (H1: β=-0.061, t=1.988, p<0.05) and their nation-state's intelligence activities (H3: β=-0.338, t=12.880, p<0.001) have negative impacts on their trust in government respecting privacy. Second, the results confirm that citizens' concerns about their digital identity (H2: β=-0.062, t=2.218, p<0.05), their nation-state's intelligence activities (H4: β=-0.186, t=6.707, p<0.001), and the security of biodata (H6: β=-0.162, t=5.865, p<0.001) have negative impacts on their acceptance of collection and use of personal data for government purposes.

Third, the results confirm that citizens' trust in the government respecting privacy (H7: β=0.211, t=7.396, p<0.001) has a positive impact on their acceptance of collection and use of personal data for governmental

Table 1. Constructs correlations, reliability and validity

	CR	*AVE*	*Acceptance*	*Biodata*	*Identity*	*Intelligence*	*Trust*
Acceptance	0.853	0.661	(0.813)				
Biodata	0.784	0.645	-0.194	(0.803)			
Identity	0.893	0.807	-0.140	0.374	(0.898)		
Intelligence	0.881	0.788	-0.254	-0.020	0.003	(0.888)	
Trust	0.770	0.626	0.288	-0.061	-0.079	-0.337	(0.791)

purposes. That said, our analysis did not confirm the anticipated negative impact of biodata security concerns on citizens' trust in their government being respectful of privacy (H5: β=-0.045, t=1.578, n.s.). The results, along with information about data and support or lack of support for the hypotheses, are summarized in Table 2.

Discussion and Conclusion

The objective of this study was to investigate concerns that people have about the rise of state-corporate digital mass surveillance amidst rapid socio-technical changes and examine how those concerns affect citizens' trust in and acceptance of governmental use of personal data. Specifically, we focused on concerns people have about their digital identity, the nation-state's intelligence activities, and security of biodata, including iris scans at airports and DNA information stored in databanks of commercial companies such as ancestry tracing firms, which are increasingly accessible to authorities. In so doing, we tested a research model with seven hypotheses on an open survey data about privacy, collected from 1,486 Canadians in 2018-2019. A PLS-SEM analysis confirmed six of the seven hypotheses.

Contribution to theory

Our results have implications for the existing body of literature on surveillance and privacy, by having focused on the links between privacy perception, the nation-state's intelligence activities, and the rise of a surveillance state using big data. The results point out that recent advances in digital technologies, intensified during the COVID-19 pandemic, are major contributors to the increase of digital surveillance. The tightening of state-corporate collaboration to fight the pandemic has opened doors for growing collection, sharing, and use of personal data in digital form.

Overall, the results confirm that citizens' trust in government respecting their privacy and citizens' acceptance of their government's use of personal data with rising levels of surveillance are affected by a number of concerns and cannot be explained by any single factor (see Bernal, 2016), but rather a number of varied factors. This was obvious through the relatively low, yet acceptable R-squared measures. Nonetheless, the study confirms what previous literature suggested regarding the relationship between identity concerns and citizens' acceptance of governmental use of personal data (Beduschi, 2019), as well as between

Table 2. Correlation coefficients and statistical significances

H#	*Hypothesis*	*β*	*t-value*	*Sig.*	*Support*
H1	Identity concerns → Trust (-)	-0.061	1.988	p<0.05	Yes
H2	Identity concerns → Acceptance (-)	-0.062	2.218	p<0.05	Yes
H3	Intelligence concerns → Trust (-)	-0.338	12.880	p<0.001	Yes
H4	Intelligence concerns → Acceptance (-)	-0.186	6.707	p<0.001	Yes
H5	Biodata concerns → Trust (-)	-0.045	1.578	n.s.	No
H6	Biodata concerns → Acceptance (-)	-0.162	5.865	p<0.001	Yes
H7	Trust → Acceptance (+)	0.211	7.396	p<0.001	Yes

citizen's concerns about biodata security and their acceptance of governmental data use (Ebelogu et al., 2019).

Additionally, the result of an unconfirmed hypothesis about the impact of citizens' biodata concerns on their trust in government respecting privacy has interesting implications to theory. In principle, it suggests that while citizens may not trust their government being respectful of privacy, yet at the same time they can accept the gathering and use of personal data by the government for undisclosed purposes. For example, people across the world are increasingly using private ancestry tracing services that collect and store DNA information, that is, highly sensitive biodata, even though government authorities may be given access to DNA profiles in these databases for criminal investigation needs, either voluntarily by the database owner or through a court order (see Jee, 2019). Dedrickson (2018) argues that the unfettered access state authorities have to private DNA profile databases may raise citizen resistance. However, Guerrini et al. (2018) note that many people simply choose to ignore or even support the state authority's invasion of DNA databases, if the purpose is to catch violent and dangerous offenders. These findings contribute to discussion on digital surveillance by confirming arguments in previous literature that while the surveillance state is built upon distrust that justifies digital mass surveillance of its citizens, people may also be distrustful of their government (Bernal, 2016; van Zoonen, 2020). This bi-directional distrust feeds the reciprocal growth of tensions between the nation-state and its people, suggesting that state-corporate surveillance actors should be more transparent about their collection and use of citizens' personal data.

Implications for practice

It is evident from our study that the more people trust in their government being respectful of citizens' privacy, the more positive they feel about the government and its actions. The findings on the impacts of citizens' concerns about their nation-state's intelligence activities and their trust in and acceptance of governmental gathering and use of personal data highlight the need for government intelligence agencies to be more transparent about what data are being collected and how they are collected. We believe that democracy and the longevity of surveillance programs, as well as the use of citizen's personal data for creating a digital welfare state, rather than an authoritarian surveillance state, require that citizens can trust their leaders and authorities (Cayford & Pieters, 2018). The more secrecy by public servants and deviation in what is being told from various official sources about the matter, the more substantial public reactions will be when information about the extent of digital surveillance leaks to public through whistle-blowers, as evident through the Snowden leaks (see Clark, 2016). Likewise, when people find out that sensitive personal data is being collected from them without their knowledge or consent, through targeted or untargeted digital surveillance. For example, knowing that employers may use surveillance tools such as computer screenshots, recording phone conversations, tracking mobile phone locations, and keylogging activities to monitor their remote workers' productivity, has been found to result in the loss of a sense of safety, as well as alienation of workers from their private homes due to employers' invasion of those personal "safe spaces" (Zhang et al., 2017; Manokha, 2020).

In addition to increasing the transparency of state-corporate surveillance activities, we believe that citizens should have opportunities to choose and resist technologically automated surveillance, such as algorithmic recognition used in machines (Martin et al., 2009). We also agree with the view of Ram and Gray (2020) and Veliz (2021), that only by adopting a diverse set of procedural and substantive safeguards, including regulation and strict limitations on personal data gathering, aggregation, storage, access, analysis, and use by state organizations and corporations, and by subjecting their digital surveillance programs to constant review performed by independent third-parties, can we hope to protect democracy, citizens' privacy, and well-being in the ever-more digitalized world. Additionally, multinational corporations should voluntarily take actions to better support online user privacy, following the example of Google that recently announced they will end sale of ads using individual web tracking data and refrain from developing new ways to follow individual users across the internet, an action welcomed by the global online audience in a time when consumers are more aware and concerned of their data being used unwittingly (Chan & Anderson, 2021). Further, citizens should be encouraged to actively engage in "sousveillance" or "metaveillance", in other words, counter-conduct activities aiming to "watch the watchers" as a way to ensure the fair, respectful, legitimate, and non-discriminative use of state-corporate surveillance data, and to maintain the balance of power by flattening the "hierarchized system of policing" in society and workplaces (see Odoemelam, 2015; Hintz et al., 2017; Manokha, 2020b; Sekalala et al., 2020).

Limitations and future research avenues
Our study has limitations that could be addressed in future research. First, although the open survey data on Canadians' perceptions about privacy in the digital era were highly useful for the needs of our study, the questionnaire was not designed by us. Thus, there are inevitable limitations regarding what we could perform with the data and what potentially important factors were left out. Future research could build upon our findings from the open data set and conduct a survey with purposefully designed questions related to key points in our study, as well as involve other types of concerns such as communications-related (cf. Friedewald et al., 2013).

Second, the data were anonymous with little information besides the responses to privacy questions. Thus, we were unable to draw conclusions between demographics and privacy perceptions. Future research should examine the links between privacy concerns and trust in and peoples' acceptance of government gathering and use of personal data involving demographics. This would potentially enable identifying links between demographic groups such as by age, gender, or ethnicity.

Third, the data were collected in Canada which gives a specific cultural, political, and geographical research context. Zhang et al. (2017) argues that people in different countries may view surveillance differently due to cultural, political, and social elements. Hence, in parallel with the notions of Zhang et al. (2017) and Clarke (2019), future research should investigate public opinion about digital surveillance not only in one country, but also in other countries, regions, and cultural environments.

Acknowledgments

An earlier version of this paper was presented at the ISPIM Connects Global Conference from December 7-8th, 2020. Also, Professor Seppo Leminen warmly acknowledges the funding from Drammen City Municipality for his chaired professorship of Innovation and Entrepreneurship, which enabled completing his part in the article.

References

Amit, M., Kimhi, H., Bader, T., Chen, J., Glassberg, E., & Benov, A. 2020. Mass-surveillance technologies to fight coronavirus spread: the case of Israel. *Nature Medicine*, 26: 1167-1169.
DOI: https://doi.org/10.1038/s41591-020-0927-z

Asher-Schapiro, A. 2020. Unfair surveillance'? Online exam software sparks global student revolt. *Reuters*, November 10, 2020.
Accessed online: https://www.reuters.com/article/us-global-tech-education-trfn-idUSKBN27Q1Q1

Beduschi, A. 2019. Digital identity: Contemporary challenges for data protection, privacy and non-discrimination rights. *Big Data & Society*, 6(2): 1-6.
DOI: https://doi.org/10.1177/2053951719855091

Bennett, C. J. 2011. In defence of privacy: The concept and the regime. *Surveillance & Society*, 8(4): 485-496.
DOI: https://doi.org/10.24908/ss.v8i4.4184

Bernal, P. 2016. Data gathering, surveillance and human rights: recasting the debate. *Journal of Cyber Policy*, 1(2): 243-264.
DOI: https://doi.org/10.1080/23738871.2016.1228990

Budak, J., Rajh, E., & Recher, V. 2017. Citizens' privacy concerns - Does national culture matter? In: Friedewald, M., Burgess, J.P., Cas, J., Bellanova, R., & Peissl, W. (Eds.), Surveillance, Privacy, and Security - Citizens' Perspectives. *PRIO New Security Studies*, Routledge: 36-51.

Cayford, M., & Pieters W. 2018. The effectiveness of surveillance technology: What intelligence officials are saying. *The Information Society*, 34(2): 88-103.
DOI: https://doi.org/10.1080/01972243.2017.1414721

Chan, K., & Anderson, M. 2021. Google ends sale of ads using individual web tracking data. *CTV News*, March 3, 2021. Accessed online: https://www.ctvnews.ca/sci-tech/google-ends-sale-of-ads-using-individual-web-tracking-data-1.5331738

Chanley V.A., Rudolph, T.J., & Rahn, W.M. 2000. The origins and consequences of public trust in government: a time series analysis. *Public Opinion Quarterly*, 64(3): 239-256.
DOI: https://doi.org/10.1086/317987. PMID: 11114267

Clark, I. 2016. The digital divide in the post-Snowden era. *Journal of Radical Librarianship*, 2: 1-32.
DOI: https://repository.uel.ac.uk/item/851y5

Clarke, R. 2019. Risks inherent in the digital surveillance economy: A research agenda. *Journal of Information Technology*, 34(1): 59-80.
DOI: https://doi.org/10.1177/0268396218815559

Clement, A., & Obar, J.A. 2015. Canadian Internet "Boomerang" Traffic and Mass NSA Surveillance: Responding to Privacy and Network Sovereignty Challenges. In: Geist, M. (Ed.) *Law, Privacy and Surveillance in Canada in the Post-Snowden Era*. The University of Ottawa Press: 13-44.

Dedrickson, K. 2018. Universal DNA databases: a way to improve privacy? *Journal of Law and the Biosciences*, 4(3): 637-647.
DOI: https://doi.org/10.1093/jlb/lsx041

Dencik, L., Hintz, A., & Cable, J. 2016. Towards data justice? The ambiguity of anti-surveillance resistance in political activism. *Big Data & Society*, 3(2): 1-12.
DOI: https://doi.org/10.1177/2053951716679678

Dencik, L., Redden, J., Hintz, A., & Warne, H. 2019. The 'golden view': data-driven governance in the scoring society. *Internet Policy Review*, 8(2).
DOI: https://doi.org/10.14763/2019.2.1413

Ebelogu, C.U., Adelaiye, O., & Silas, S. 2019. Privacy Concerns in Biometrics. *IEEE-SEM*, 10(7): 45-52.

Forcese, C. 2015. Law, Logarithms, and Liberties: Legal Issues Arising from CSE's Metadata Collection Initiatives. In: Geist, M. (Ed.) *Law, Privacy and Surveillance in Canada in the Post-Snowden Era*. The University of Ottawa Press: 127-160.

Fornell, C., & Larcker, D.F. 1981. Evaluating Structural Equation Models with Unobservable Variables and Measurement Error. *Journal of Marketing Research*, 18(1): 39-50.
DOI: https://doi.org/10.1177/002224378101800104

Fox Cahn, A. 2021. The U.S. can't rebuke global tyranny when our companies sell tools that enable it. *Fast Company*, February 5, 2021.
Accessed online: https://www.fastcompany.com/90601037/american-surviellance-state-facial-recognition-hypocrisy

Friedewald, M., Finn, R.L., & Wright, D. 2013. Seven Types of Privacy. In: Gutwirth, S., Leenes, R., de Hert, P., & Poullet Y. (Eds.) *European Data Protection: Coming of Age*. Springer: 3-32.
DOI: https://doi.org/10.1007/978-94-007-5170-5

Geist, M. (Ed.). 2015. Law, Privacy and Surveillance in Canada in the Post-Snowden Era. The University of Ottawa Press: Canada.
DOI: https://doi.org/10.26530/oapen_569531

Guerrini, C.J., Robinson, J.O., Petersen, D., & McGuire, A.L. 2018. Should police have access to genetic genealogy databases? Capturing the Golden State Killer and other criminals using a controversial new forensic technique. *PLoS Biology*, 16(10), e2006906.
DOI: https://doi.org/10.1371/journal.pbio.2006906

Guinchard, A. 2020. Our digital footprint under Covid-19: should we fear the UK digital contact tracing app? *International Review of Law, Computers & Technology*, 35(1): 84-97.
DOI: https://doi.org/10.1080/13600869.2020.1794569

Henseler, J., Hubona, G., & Ray, P.A. 2016. Using PLS path modelling in new technology research: updated guidelines. *Industrial Management & Data Systems*. 116(1): 2-20.
DOI: https://doi.org/10.1108/IMDS-09-2015-0382

Hintz, A., Dencik, L., & Wahl-Jorgensen, K. 2017. Digital Citizenship and Surveillance Society - Introduction. *International Journal of Communication*, 11: 731-739.

Hogan, M., & Shepherd, T. 2015. Information Ownership and Materiality in an Age of Big Data Surveillance. *Journal of Information Policy*, 5: 6-31.
DOI: https://doi.org/10.5325/jinfopoli.5.2015.0006

Isabelle, D.A., Westerlund, M., Mane, M., & Leminen, S. 2020. The Role of Analytics in Data-Driven Business Models of Multi-Sided Platforms: An exploration in the food industry. *Technology Innovation Management Review*, 10(7): 5-16.
DOI: http://doi.org/10.22215/timreview/1371

Israel, T. 2015. Foreign Intelligence in an Inter-Networked World: Time for a Re-Evaluation', In: Geist, M. (Ed.) *Law, Privacy and Surveillance in Canada in the Post-Snowden Era*. The University of Ottawa Press: 71-101.

Jee, C. 2019. A detective has been granted access to an entire private DNA database. *MIT Technology Review*, November 6, 2019.
Accessed online: https://www.technologyreview.com/2019/11/06/132047/a-detective-has-been-given-access-to-private-consumer-dna-data-for-the-first-time/

Job, J. 2005. How is trust in government created? It begins at home, but ends in the parliament. *Australian Review of Public Affairs*, 6(1): 1-23.

Keshet, Y. 2020. Fear of panoptic surveillance: using digital technology to control the COVID-19 epidemic. *Israel Journal of Health Policy Research*, 9: 67.
DOI: https://doi.org/10.1186/s13584-020-00429-7

Kim, C., Lee, K.C., & Costello, F.J. 2020. The Intention of Passengers towards Repeat Use of Biometric Security for Sustainable Airport Management. *Sustainability*, 12(11): 4528.
DOI: https://doi.org/10.3390/su12114528

Kitchin, R. 2020. Civil liberties or public health, or civil liberties and public health? Using surveillance technologies to tackle the spread of COVID-19. *Space and Polity*.
DOI: https://doi.org/10.1080/13562576.2020.1770587

Klingler, C., Silva, D.S., Schuermann, C., Reis, A.A., Saxena A., & Strech, D. 2017. Ethical issues in public health surveillance: a systematic qualitative review. *BMC Public Health*, 17: 295.
DOI: https://doi.org/10.1186/s12889-017-4200-4

Lemieux, P. 2018. Why the Surveillance State is Dangerous. *The Library of Economics and Liberty*, June 10, 2018
Accessed online: https://www.econlib.org/archives/2018/06/why_the_surveil.html

Leminen, S., Nyström, A.-G., & Westerlund, M. 2020. Change processes in open innovation networks - exploring living labs. *Industrial Marketing Management*. 91: 701-718.
DOI: https://doi.org/10.1016/j.indmarman.2019.01.013

Leminen, S., Rajahonka, M., Wendelin, R., & Westerlund, M. 2020. Industrial Internet of Things Business

Models in the Machine-to-Machine Context. *Industrial Marketing Management*. 84: 298-311. DOI: https://doi.org/10.1016/j.indmarman.2019.08.008

Leminen, S., Rajahonka, M., Westerlund, M., & Wendelin R. 2018. The Future of the Internet of Things: Toward Heterarchical Ecosystems and Service Business Models. *Journal of Business & Industrial Marketing*. 33(6): 749-767.
DOI: https://doi.org/10.1108/JBIM-10-2015-0206

Lindell, M.K., & Whitney D.J. 2001. Accounting for common method variance in cross-sectional research designs. *Journal of Applied Psychology*, 86(1): 114-121. DOI: https://doi.org/10.1037/0021-9010.86.1.114

Lyon, D. 2007. Surveillance, Security and Social Sorting - Emerging Research Priorities. *International Criminal Justice Review*, 17(3): 161-170.
DOI: https://doi.org/10.1177/1057567707306643

Lyon, D. 2014. Surveillance, Snowden, and Big Data: Capacities, consequences, critique. *Big Data & Society*, 1(2): 1-13.
DOI: https://doi.org/10.1177/2053951714541861

Maier, K. 2020. The Surveillance State is a Reality. *Bloomberg*, June 26, 2020.
Accessed online: https://www.bloomberg.com/news/newsletters/2020-06-26/the-surveillance-state-is-a-reality

Manokha, I. 2020a. Covid-19: Teleworking, Surveillance and 24/7 Work. Some Reflexions on the Expected Growth of Remote Work After the Pandemic. *Political Anthropological Research on International Social Sciences*, 1(2): 273-287.
DOI: https://doi.org/10.1163/25903276-BJA10009

Manokha, I. 2020b. The Implications of Digital Employee Monitoring and People Analytics for Power Relations in the Workplace. *Surveillance & Society*, 18(4): 540-554.
DOI: https://doi.org/10.24908/ss.v18i4.13776

Marin, L. 2017. The deployment of drone technology in border surveillance - between techno-securitization and challenges to privacy and data protection. In: Friedewald, M., Burgess, J.P., Cas, J., Bellanova, R., & Peissl, W. (Eds.) *Surveillance, Privacy, and Security - Citizens' Perspectives*. PRIO New Security Studies, Routledge: 107-122.

Martin, A.K., van Brakel, R.E., & Bernhard, D.J. 2009. Understanding resistance to digital surveillance: Towards a multi-disciplinary, multi-actor framework. Surveillance & Society, 6(3): 213-232. DOI: https://doi.org/10.24908/ss.v6i3.3282

Martinez-Martin, N., & Char, D. 2018. Surveillance and Digital Health. *American Journal of Bioethics*, 18(9): 67-68. DOI: https://dx.doi.org/10.1080%2F15265161.2018.1498954

Marx, G.T. 2015. Surveillance Studies. In: Wright, J.D. (Ed.) *International Encyclopedia of the Social & Behavioral Sciences* (Second Edition). 23: 733-741.
DOI: http://dx.doi.org/10.1016/B978-0-08-097086-8.64025-4

McGee, P., Murphy, H., & Bradshaw, T. 2020. Coronavirus apps: the risk of slipping into a surveillance state. Financial Times, April 28, 2020.
DOI: https://www.ft.com/content/d2609e26-8875-11ea-a01c-a28a3e3fbd33

Menichelli, F. 2017. Beyond the trade-off between privacy and security? In: Friedewald, M., Burgess, J.P., Cas, J., Bellanova, R., & Peissl, W. (Eds.). *2017. Surveillance, Privacy, and Security - Citizens' Perspectives*. PRIO New Security Studies, Routledge: 91-104.
DOI: https://doi.org/10.4324/9781315619309

Milanovic, M. 2015. Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age. *Harvard International Law Journal*, 56(1): 81-146.

Monecke, A., Leisch, F. 2012. semPLS: structural equation modeling using partial least squares. *Journal of Statistical Software*, 48(3): 1-32.
DOI: http://dx.doi.org/10.18637/jss.v048.i03

Murray, D., & Fussay, P. 2019. Bulk surveillance in the digital age: rethinking the human rights law approach to bulk monitoring of communications data. *Israel Law Review*, 52(1): 31-60.
DOI: https://doi.org/10.1017/S0021223718000304

Odoemelam, C.E. 2015. Adapting to Surveillance and Privacy Issues in the Era of Technological and Social Networking. *International Journal of Social Science and Humanity*, 5(6): 572-577.
DOI: https://doi.org/10.7763/IJSSH.2015.V5.520

OPC. 2020. *2018-19 Survey of Canadians on Privacy.* Accessed online: https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2019/por_2019_ca/

Osborne, C. 2020. Half of US citizens would share medical data beyond COVID-19 despite surveillance state worries. *ZDNet*, September 23, 2020.
Accessed online: https://www.zdnet.com/article/half-of-us-citizens-are-happy-to-share-medical-data-beyond-covid-19-despite-surveillance-state-worries/

Petit, P. 2020. 'Everywhere Surveillance': Global Surveillance Regimes as Techno-Securitization. *Science as Culture*, 29(1): 30-56.
DOI: https://doi.org/10.1080/09505431.2019.1586866

Ram, N., & Gray, D. 2020. Mass surveillance in the age of COVID-19. *Journal of Law and the Biosciences*, 7(1), lsaa023.
DOI: https://doi.org/10.1093/jlb/lsaa023

Richards, N.M. 2013. The dangers of surveillance. *Harvard Law Review*, 126(7): 1934-1965.
Accessed online: http://www.jstor.org/stable/23415062

Ringle, C.M., Wende, S., Becker, J.-M. 2015. *SmartPLS 3. Boenningstedt: SmartPLS GmbH.*
Accessed online: http://www.smartpls.com

Rosengren, C., & Ottosson, M. 2016. Employee monitoring in a digital context. In: Daniels, J., Gregory, K., & McMillan Cottom, T. (Eds.). *Digital Sociologies*. Bristol University Press, Policy Press: 181-194.
https://doi.org/10.2307/j.ctt1t89cfr.18

Sekalala, S., Dagron, S., Forman, L., & Mason Meier, B. 2020. Analyzing the Human Rights Impact of Increased Digital Public Health Surveillance during the COVID-19 Crisis. *Health and Human Rights Journal*, 22(2): 7-20.
Accessed online: http://www.ncbi.nlm.nih.gov/pmc/articles/pmc7762901/

Stott, E., & Wiggins, N. 2020. Being monitored by your boss while working from home – necessary trade-off or 'stupid' surveillance? *ABC Radio National*, October 15, 2020.
Accessed online: https://www.abc.net.au/news/2020-10-16/work-from-home-tracking-software-monitoring/12766020

Taylor, N. 2002. State Surveillance and the Right to Privacy. *Surveillance & Society*, 1(1): 66-85.
DOI: https://doi.org/10.24908/ss.v1i1.3394

van den Broek, T., Ooms, M., Friedewald, M., van Lieshout, M., & Rung, S. 2017. Privacy and security - Citizens' desires for an equal footing. In: Friedewald, M., Burgess, J.P., Cas, J., Bellanova, R., & Peissl, W. (Eds.) *Surveillance, Privacy, and Security - Citizens' Perspectives*. PRIO New Security Studies, Routledge: 15-35.

van Zoonen, L. 2020. Data governance and citizen participation in the digital welfare state. *Data & Policy*, 2, e10.
DOI: https://doi.org/10.1017/dap.2020.10

Veliz, C. 2021. Privacy and digital ethics after the pandemic. *Nature Electronics*, 4: 10-11.
DOI: https://doi.org/10.1038/s41928-020-00536-y

Wang, V., & Tucker, J.V. 2017. Surveillance and identity: conceptual framework and formal models. *Journal of Cybersecurity*, 3(3): 145-158.
DOI: https://doi.org/10.1093/cybsec/tyx010

Watt, E. 2017. The right to privacy and the future of mass surveillance. *The International Journal of Human Rights*, 21(7): 773-799.
DOI: https://doi.org/10.1080/13642987.2017.1298091

Wee, S.L. 2020. China is collecting DNA from tens of millions of men and boys, using U.S. equipment. *The New York Times*, June 17, 2020.
Accessed online: https://www.nytimes.com/2020/06/17/world/asia/China-DNA-surveillance.html

Winter, J.S., & Davidson, E. 2019. Big data governance of personal health information and challenges to contextual integrity. *The Information Society*, 35(1): 36-51.
Accessed online: https://doi.org/10.1080/01972243.2018.1542648

Zhang, B., Peterson Jr., H.M., & Sun, W. 2017. Perception of Digital Surveillance: A Comparative Study of High School Students in the U.S. and China. *Issues in Information Systems*, 18(1): 98-108.
DOI: https://doi.org/10.48009/1_iis_2017_98-108

Zhao, D., & Hu, W. 2017. Determinants of public trust in government: empirical evidence from urban China. *International Review of Administrative Sciences*, 83(2): 358-377. DOI: https://doi.org/10.1177/0020852315582136

The Acceptance of Digital Surveillance in an Age of Big Data

Mika Westerlund, Diane A. Isabelle, Seppo Leminen

About the Author

Mika Westerlund, DSc (Econ), is an Associate Professor at Carleton University in Ottawa, Canada. He previously held positions as a Postdoctoral Scholar in the Haas School of Business at the University of California Berkeley and in the School of Economics at Aalto University in Helsinki, Finland. Mika earned his doctoral degree in Marketing from the Helsinki School of Economics in Finland. His research interests include open and user innovation, the Internet of Things, business strategy, and management models in high-tech and service-intensive industries.

Diane A. Isabelle, PhD, is an Associate Professor of International Business at Carleton University. Her research focuses broadly on the areas of science, innovation, and techno-entrepreneurship within a global context. Specifically, her research is organized around the following three inter-related themes: 1) International entrepreneurship & ecosystems, 2) Internationalization (International New Ventures and SMEs), 3) Global collaborative research and Science, Technology and Innovation policy. In addition to these themes, she is researching and publishing on Technology-integrated and international interdisciplinary experiential learning in higher education. Prior to joining Sprott in 2011, Dr. Isabelle worked in several senior executive roles related to science, technology and industrial research (Industrial Research Assistance Program - IRAP) at the National Research Council of Canada (NRC), the Government of Canada’s premier research and technology organization. She started her career as a project engineer for several multinational firms, including General Electric, Esso and Boeing Aerospace.

Seppo Leminen is Drammen City Municipality chaired (Full) Professor of Innovation and Entrepreneurship in the USN School of Business at the University of South-Eastern Norway in Norway, an Adjunct Professor of Business Development at Aalto University in Finland and an Adjunct Research Professor at Carleton University in Canada. He holds a doctoral degree in Marketing from the Hanken School of Economics and a doctoral degree in Industrial Engineering and Management in the School of Science at Aalto University. He is an Associate Editor in Techovation and an Associate editor in BRQ, Business Research Quarterly. His current research topics includes digital business models and ecosystems (cf. Internet of Things), robotics, block chains, living labs, innovation ecosystems, collaborative and networked models of innovations, collaborative methods of innovations, as well as management and marketing models for different types of companies. Results from his research have been reported in *Industrial Marketing Management, the Journal of Cleaner Production, the Journal of Engineering and Technology Management, the Journal of Business & Industrial Marketing, Management Decision, the International Journal of Innovation Management,* and *the Technology Innovation Management Review,* among many others.

Citation: Westerlund, M., Isabelle, D.A., Leminen, S. 2021. The Acceptance of Digital Surveillance in an Age of Big Data. Technology Innovation Management Review, 11(3): 32-44.
http://doi.org/10.22215/timreview/1427

Keywords: Digital surveillance, mass surveillance, privacy, acceptance, biometric, digital identity, citizen privacy, personal data, intelligence activities