PAR PUBLIC ADMINISTRATION REVIEW

Étienne Charbonneau
École nationale d'administration publique
Carey Doberstein
University of British Columbia

COVID-19 Viewpoint

An Empirical Assessment of the Intrusiveness and Reasonableness of Emerging Work Surveillance Technologies in the Public Sector

Étienne Charbonneau is Canada Research Chair in Comparative Public Management at École nationale d'administration publique in Montreal. His recent research focuses on accountability and electronic surveillance.
Email: etienne.charbonneau@enap.ca

Carey Doberstein is assistant professor at the department of Political Science at the University of British Columbia in Vancouver. He is an associate editor of *Canadian Public Administration*. His latest book is *Distributed Democracy: Health Care Governance in Ontario* (University of Toronto Press).
Email: carey.doberstein@ubc.ca

Abstract: *As public sector work environments continue to embrace the digital governance revolution, questions of work surveillance practices and its relationship to performance management continue to evolve, but even more dramatically in the contemporary period of many public servants being forced to shift to remote work from home in response to the COVID-19 pandemic. This article presents the results of three surveys, two of them population-based survey experiments, all conducted during the onset of the COVID-19 pandemic in Canada that compare public servant (n = 346) and citizen (n = 1,008 phone; n = 2,001 web) attitudes to various cutting-edge—though no doubt controversial among some—digital surveillance tools that can be used in the public sector to monitor employee work patterns, often targeted toward remote working conditions. The findings represent data that can help governments and public service associations navigate difficult questions of reasonable privacy intrusions in an increasing digitally connected workforce.*

Evidence for Practice

- New work surveillance technologies are available to use within the public sector and will present acceptability challenges to public managers as they contemplate the introduction of these technologies.
- Multimodal survey data from Canada reveals that public servants and citizens find these emerging work surveillance technologies to be quite intrusive and unreasonable but show relatively more tolerance for digital surveillance over physical surveillance practices.
- Understanding surveillance anxieties among targeted employees will be key to finding a balance between employee privacy rights and employer desires to manage employees in a remote or digital environment.

In the midst of the COVID-19 pandemic, social workers in the Canadian province of Quebec were initially forced by their public sector managers to continue their on-site visits of needy families and in-person team meetings, violating the physical distancing protocols from the Government of Quebec. Managers were apparently concerned with maintaining productivity and chipping away at the wait lists even in a crisis context, afraid that remote working would compromise these efforts (Allard 2020). The minister later denounced the managers and demanded remote working during this period, consistent with the advice of public health experts on the necessary steps to stem the spread of the virus. The COVID-19 pandemic dramatically accelerated an existing trend toward remote work in the public sector, introducing uncertainty with respect to the security of data, the management of the work of teams, and the productivity of individuals, in an environment when nearly entire organizations are working virtually from home. The COVID-19 pandemic has ushered in a period, the length of which is unknown, in which remote working is the norm, and public sector work environments are forced to change quite dramatically while under incredible pressure to serve the government and citizens. With so many public sector employees working from home, this raises unique supervisory demands on human resources managers (Schuster et al. 2020, 3), in particular manager–employee relationships, work assignments, and accountability. One critical piece of this equation relates to work surveillance and the technological advancements that have made digital work surveillance in the context of remote working not only more possible but also potentially more fraught with privacy concerns.

Work surveillance can take various forms from light observation to extremely intrusive observation, from digital surveillance to more complex artificial intelligence analysis. As of June 2020, an uptick in the use of surveillance software was documented for some private firms (Thompson 2020) but not for public organizations in Canada and abroad. A piece of software gaining in popularity with private sector employers since the COVID-19 pandemic is

Public Administration Review, Vol. 80, Iss. 5, pp. 780–791. © 2020 by The American Society for Public Administration.
DOI: 10.1111/puar.13278.

a videoconference-call software that is always on; it takes pictures every few minutes via a front-facing laptop webcam and posts them on a wall so managers can see employees working at their desks (Holmes 2020). There are also software and hardware for monitoring devices (e.g., telephone, email, texts, keystrokes, clicks on computer/internet), one's environment (e.g., geospatial movements, desk sensors at workspace), and biometrics (e.g., heart rate, facial recognition) that are now easily integrated into most workplaces. Even more complex and potentially intrusive surveillance is apparent in police departments pre-COVID-19. To fulfill a mandate from a federal judge, the police department in Oakland, California, uses an artificial intelligence software to flag possible cases of officer corruption by compiling and analyzing "all aspects of an officer's career, including time in the academy, data on police stops, citizen complaints, body camera footage and use of force" (Cassidy 2019). Likewise, in 2020, the Massachusetts State Police plans to introduce geolocalization technology in its 2,900 vehicles to track and validate officer movements throughout shifts (Miller 2020).

Other examples of workplace surveillance can similarly bring clearly into view the privacy implications of the increasingly easy, but also invasive, monitoring potential of employers. In 2019, a class action lawsuit was filed in Illinois on the use of biometrics—in this case fingerprint scanner technology—against employers of Thyssenkrupp Crankshaft, United Airlines, and Hilton Hotels and Resorts to prevent "buddy punching" (coworkers punching in for a friend who is late or absent from work). The plaintiffs argued in part that this is an unreasonable infringement on their privacy to be forced to submit biometric data to the employer. What is considered a reasonable expectation of privacy in any given society or context is not fixed in time (Kugler 2014, 1,206–1,207) and is especially subject to evolution as new technologies become embedded in our personal and professional lives. For some observers, as new technologies enter the market and workplaces, "our expectations of privacy diminish from what is reasonable to what is merely foreseeable" (Johnson 2012, 415). Something analogous to "behavioral fatigue," as is speculated with social distancing during the current pandemic (Pedersen and Favero 2020, 12), might be at play as emotionally and cognitively depleted employees do not resist to new demands put on them.

As consumers, individuals are perhaps growing accustomed to being surveilled by free services offered by Google and Facebook; paid Microsoft software, such as Cortana; or premium devices such as the Apple Watch. It is unclear whether individuals, as workers, have higher expectations of privacy. The digital revolution was already transforming traditional forms of surveillance—swinging by office desk, employing secret shoppers, using sign-out boards—into potentially much more continuous, passive, and all-encompassing surveillance in a context whereby so much of work exists in cyberspace (Ajunwa, Crawford, and Schultz 2017). This type of digital surveillance falls under the umbrella of electronic performance monitoring (EPM)—even if the purpose is not strictly for performance evaluation or enhancements—for which there is enormous diversity in terms of its frequency, purpose, scope, and transparency to the employee (Ravid et al. 2020). The COVID-19 pandemic has accelerated this trend and thus foists upon public sector work environments important questions about what digital work surveillance practices are reasonable intrusions on the privacy of employees.

There is complex legal terrain to navigate in Anglo-American contexts with respect to privacy informed by broad constitutional provisions, employment law, and even collective agreements, all of which are interpreted by human resource managers, professional associations, arbitrators, and judges to reach decisions about what constitutes invasions of privacy by public organizations. For example, in Canada, case law recognizes elements of privacy (Khullar 2012, 392) even if arbitrators or other legal actors consider this a "legal fiction or a misunderstanding" (Khullar 2012, 385). The United States and Canada fall into the same group of common law and statutory rights of action involving privacy torts as opposed to the United Kingdom and Australia where breaches of confidence are the main issue (Paterson 2018, 209). Among various Anglo-American legal regimes, there is enough commonality that courts occasionally draw on case law from other countries, as in Canada, where the U.S. Supreme Court recognized arguments from the early privacy case of *Katz v. United States* (1967) to provide clarity on the privacy dimensions of Canada's Charter of Rights and Freedoms (Johnson 2012, 472).

Yet such court decisions of what is a reasonable expectation of privacy are not solely normative or deduced from first principles. Chao et al. (2018, 265) argue that "all too often those assertions are based not on reliable empirical data, but rather on judges' intuitions and sheer speculations." This conclusion is buttressed by experimental survey research nearly 30 years ago by Slobogin and Schumacher (1993), who compared the expectations of privacy of the public with judges' views (regarding police behaviors) expressed in key court decisions, and found that judges misjudged what the public found intrusive or reasonable in terms of police searches, seizures, and surveillance (Slobogin and Schumacher 1993, 774). Since then, a number of similar studies have emerged (including Blumenthal, Adya, and Mogle 2009; Chao et al. 2018; Fradella, and Fischer 2015; Fradella et al. 2011; Kugler 2014; McAllister 2014; Scott-Hayward et al. 2015) as part of the Empirical Legal Studies movement (Ho and Rubin 2011). This type of empirical research has not been done in a Canadian context and, to our knowledge, has not focused on professional public servants elsewhere. There is thus not only an opportunity to settle to what degree public sector work privacy is a contested public value (Bozeman 2019) but also to broaden this kind of inquiry beyond criminal and police enforcement contexts, as Hoetger (2013, 581) contends that the findings from police searches vis-à-vis privacy "would likely extend to employer searches."

This research provides an empirical assessment of what public servants and citizens in Canada find reasonable and intrusive in terms of electronic workplace surveillance in the public sector because this data can inform, in part, the foundation of the "reasonableness" standard in human resource management policy and legal tests. As we will describe in our methods section, our two citizen-surveys (web and phone) are population-based survey experiments that aim to maximize internal and external validity. While our methodology mimics those of Slobogin and Schumacher (1993) and others who followed, our two large representative samples of citizens permit us to offer a reliable

snapshot to practitioners, compared to previous studies with a small number of participants. A 2014 study of senior government officials involved in national security decision-making revealed that representative polls are the most desirable quantitative studies by practitioners (Avey and Desch 2014, 231–232).

This study thus provides guidance to human resource managers calibrating their work surveillance policies and practices as well as produces empirical data for the inevitable future legal proceedings that grapple with tests of reasonableness, which heretofore emerged primarily from legal reasoning and a weak empirical grounding in Canada (Geist 2003, 178) and the United States (Ciochetti 2011, 356). Geist (2003, 178) explains that Canadian and U.S. jurisprudence has been shifting slowly from only considering whether there is a reasonable expectation of privacy in workplace contexts to an "emerging analysis [that] focuses instead on whether the surveillance itself is reasonable," an area to which social scientists can contribute.

The article proceeds as follows. First, we review the literature that speaks to workplace surveillance, electronic performance management, and emerging technologies in the public sector and following that review, review the comparative legal terrain for privacy in the workplace in Anglo-American contexts. Second, we describe the methodology of this study, which gathers survey data from a panel of Canadian public servants, as well as the broader public, to provide an empirical foundation for tests of the reasonableness of 12 existing and cutting-edge work surveillance technologies that are emerging (or are likely be proposed soon) in the public sector. Following that we present the data and analysis of the survey results, revealing that public servants and citizens similarly find these emerging work surveillance technologies to be quite intrusive and unreasonable, but both groups show greater tolerance for digital surveillance over physical surveillance practices. The final section explores the implications of these findings for public sector environments as governments and public service associations navigate difficult questions of reasonable privacy intrusions in an increasing digitally connected workforce.

Literature Review

Electronic Performance Monitoring (EPM) in Workplaces

A starting point for the study of work surveillance can be traced to Taylor (1912) as part of scientific management approaches focused on efficiency and performance of workers and workflows, objectives that can be tracked much more easily in modern digital work environments than in Taylor's time (Ciochetti 2011, 285–286). Electronic performance monitoring (EPM), broadly speaking, is enabled by the omnipresence of digital devices in modern organizations as well as work patterns such as an increasing number of professional public sector employees who work remotely (Fusi and Feeney 2018). Whereas Taylor was limited to the performance that managers could surveil in person and with considerable human hours devoted to do so, EPM approaches can be continuous, discreet, intrusive, and conducted without warning or consent, and in many cases can be analyzed automatically (Ravid et al. 2020). Ajunwa et al. (2017) note a shift from what they call the more traditional "authoritarian surveillance" that was imposed from above to the more recent phenomenon of "participatory surveillance" whereby employees are asked or expected to use applications (apps) or digital workspaces that purport to be beneficial to them (e.g., wellness apps, productivity apps).

Types of EPM used in modern organizations both in the private and public sectors include device monitoring (e.g., telephone, email, texts, keystrokes, clicks on computer/internet), environmental monitoring (e.g., cameras, geospatial movements, desk sensors at workspace, handwashing badges), and biometric monitoring (e.g., wellness apps, heart rate checks, facial recognition). Each of these types can be implemented such that the scope of data collection is broad or alternatively narrow in scope, as well as continuously or intermittently collected, and for basic accounting (e.g., minutes at desk) or more interpretive analysis (e.g., tone of keywords in emails to estimate office mood). Depending on the context, work surveillance can be aimed toward data-driven performance measurement, reducing or eliminating personal tasks during work hours (e.g., coordinating day care pick up, online banking), or regulating remote working conditions (Ankabi 2017).

EPM has been studied since the 1980s, and whereas early studies were inconclusive on the relationship between the presence of EPM and performance or employee attitudes, contemporary research has discovered that there are many contingencies involved in this equation, in particular that employee effects from EPM depend on an interaction between the purpose, target, intensity, scope, and feedback mechanisms involved in the surveillance as well as individual-level attributes of the employee, such as the person's trust in management (Ravid et al. 2020). Furthermore, the same technology can be seen at times as caring or coercive, depending on the motivations perceived by workers (Anteby and Chan 2018, 248). Why this all matters is that when employees perceive unfair monitoring, they are more likely to report lower job satisfaction and greater stress (Young 2010) and even engage in resistance and creative avoidance (Kayas et al. 2019).

Workplace Privacy Rights in Anglo-American Contexts

The pervasiveness of EPM in modern workplaces—in public and private sectors—presents critical perennial and new questions of privacy rights for employees. Balancing privacy rights of employees with employer desires to surveil their environments has long been a struggle in public law and human resources management, but the surveillance possibilities with new technologies present unique challenges to this equilibrium. The core foundational principle in Anglo-American law regarding privacy at the workplace revolves around the concept of "reasonableness" (Fric 2016, 63–65) for which there are several dimensions: Is there a *reasonable* expectation of privacy in this setting? Was the purpose of the search by the employer *reasonable*? Was the search conducted in a *reasonable* manner? While not all tests established by courts in Anglo-American contexts are the same, they are similarly grounded in the discourse of "reasonableness" (Fric 2016; Hoetger 2013; Hunt and Bell 2015).

American jurisprudence has loomed large in legal framing and thinking on work surveillance in Canada (Eltis 2005, 479; Geist 2003, 163), although Canada has preserved the expectation of privacy at work to a larger degree (Phillips 2015, 479). Yet courts and arbitrators in the United States and Canada have "no bright-line rule for evaluating government employee's expectations for privacy" (Hoetger 2013, 568). For example, for camera-based work

surveillance in Canada, one of the few technologies for which a rich jurisprudence exists, Khullar (2012, 383–389) tracked down five tests with 17 questions, 10 mentions of reasonableness, and 2 explicit mentions of intrusiveness. Most of those tests involve answering questions about whether the surveillance is demonstrably necessary to meet a specific need, the likelihood of its effectiveness in meeting that need, a proportionality test of loss of privacy vis-à-vis benefit gained, and confirmation that there are no less invasive ways to achieve the same end (Levin 2007). Yet answering the questions in these tests ultimately come down to the subjective opinions of judges and arbitrators.

One case exemplifies the apparent subjectivity of legal tests in a Canadian context: *Erwin Eastmond v. Canadian Pacific Railway and Privacy Commissioner of Canada* (2004). Different courts using different tests of what is intrusive and reasonable arrived at different verdicts of what a reasonable person may conclude as the same case snaked up to higher courts. Blasina (2007, 468) concludes from the long *Eastmond* legal saga that "the circumstances may allow different adjudicators to come to different conclusions of fact, although they have given reasonable consideration to the same body of evidence." With so much of the analysis of the balance between the privacy of employees and the rights of employers to observe their work environment hinging on questions of "reasonableness," it is important to explore how that standard is determined. Smith, Madden, and Barton (2016) argue that U.S. courts have tended not to attempt to assess views of reasonableness from the public itself but rather from their own sense of reasonableness; this is echoed by Eltis (2015) with respect to Canadian courts.

While most case law in Anglo-American contexts has moved beyond a simple assessment of an employee's reasonable expectation of privacy in particular work environments—and instead moving toward assessment as well whether the surveillance itself is reasonable on a host of criteria—this does not address the problem of courts and arbitrators relying primarily on their subjective sense of reasonableness. Reasonableness as a concept ought not to be deduced solely from logic but also from the views of citizens, given that we know expectations and demands for privacy are continually evolving. Yet there are risks in viewing reasonableness by a societal standard informed from aggregated public opinion, as that may be shaped by the very technological advancements that are threatening privacy at work. In particular, Eltis (2015, 496) argues

> if privacy continues to be defined by reference to reasonable expectations, technological imperatives necessarily dictate that the sphere in which one can reasonably claim solitude will decrease. In other words, assessing an individual's right to privacy by reference to society's conception of the measure of privacy that one is entitled to reasonably expect is particularly awkward when such expectations are rapidly eroding, precisely by reason of eventual social habituation to recurring intrusions.

Having a baseline of employee and citizen approval before a technology is widespread is thus useful. Likewise, having an empirical basis for statements about reasonableness in the context of work surveillance technologies can complement logic-based and contextualized tests established by courts and arbitrators in the pursuit of less arbitrary findings.

Empirically Measuring Reasonableness and Intrusiveness

Remarking on American judges' perception of what citizens find reasonable when interacting with the police, Wilson (2008, 40) argues that jury members would be better suited than judges to have a sense of what the public thinks. Ascertaining what society finds reasonable in terms of work surveillance is an empirical question with an empirical (though not fixed in time) answer. Slobogin and Schumacher (1993) discovered in surveys about law enforcement that members of the American public found many practices deemed "reasonable" by American judges to be invasive and in violation of their expectations of privacy. The authors used online experimental vignettes to test the effect of a first/third person view and the absence/presence of evidence on the respondents' view on intrusiveness of police searches. The authors surveyed a small sample of students—some in law schools, some not—on their views of surveillance activities with the aim to establish relative intrusiveness among different practices.

Blumenthal, Adya, and Mogle (2009) essentially replicated Slobogin and Schumacher's (1993) study with 158 undergraduate psychology students but also noted that those students who were exposed to more contextual information about the surveillance were less likely to find it intrusive than those asked about a particular surveillance practice in the abstract. Fradella et al. (2011) surveyed students and faculty at 11 universities, as well as the public via invitations from Facebook, on privacy as it relates to the body, territory, information, and communications, and their agreement with 35 judicial decisions in this realm. The authors concluded that "collectively, the results indicate that courts often misjudge what 'society' is prepared to embrace as a reasonable expectation of privacy" (372).

Scott-Hayward, Fradella, and Fischer (2015, 54) likewise find that the courts are often widely out of step with what the public expects in terms of privacy on five common practices of the third-party doctrine (which enables police to acquire information about online activities and localizations without probable cause from social media companies as well as internet and phone providers,). The most spectacular gap between the courts' views of what the public expects and what respondents expect is that:

> Almost 90 percent of participants felt that law enforcement should never have access, or at least require a level commensurate with probable cause to obtain information about email addresses with which an individual has been in contact. This is in stark contrast to the leading circuit court decision, holding that users have no expectation of privacy in this information.

Chao et al. (2018) also surveyed 1,200 U.S. respondents to compare their expectations of privacy to the ones depicted in court decisions and similarly found that judges overestimate the public's tolerance for police surveillance. The discrepancies for digital surveillance are especially important:

> survey participants consider five of the technology searches to be the most intrusive of all the study's scenarios. All five of these—Stingray devices, drones, obtaining emails, accessing the Cloud, and GPS tracking—were considered more intrusive than a police search of one's bedroom, the

> quintessential violation of privacy that requires justification by probable cause and a warrant. (Chao et al. 2018, 309–310)

In light of empirical legal studies such as these, Scott-Hayward, Fradella, and Fischer (2015, 58) suggest that judges should consult robust public opinion data and not lean exclusively on their own sensitivities about what appears reasonable to citizens. While all of the studies cited above are focused on police surveillance, the questions of reasonableness and intrusiveness of surveillance are parallel to those in the context of work surveillance in the public sector. From these kinds of studies, we are able to identify where the majority of respondents land on the technologies and thus derive where the "reasonable person" stands. Furthermore, the findings related to the enhanced feelings of intrusiveness of digital surveillance are particularly important to explore in the context of work surveillance in the digital era, and especially so in context of the COVID-19 pandemic when much of the public sector is working remotely and will be for some time.

Surveillance Technologies in the Workplace

While there are conceptual parallels in police surveillance cases in Anglo-American contexts with workplace surveillance in the public sector, the technologies used and their contexts are quite different. Thus, while serving as the inspiration for this study, the relationship between a citizen and the state (i.e., police surveillance) is different from that of an employee and an employer (i.e., work surveillance), and as a result, we must compile an empirical evidence base specific to public sector work surveillance and questions of reasonableness and intrusiveness.

Writing from a Canadian context, Levin (2007, 216–217) provided a list of electronic surveillance methods used or piloted by employers ranging from (CCTVs), biometric identifiers, radio frequency identifiers (RFIDs), internet and email monitoring, and keystroke tracking. Since that publication, we know of additional surveillance practices used in the public and private sectors around the world. For example, a device called OccupEye was used at *The Telegraph* (U.K.) newspaper; it is a box placed under one's desk that can track attendance and take body heat measures as part of a productivity assessment of employees (Ajunwa et al. 2017). At Deloitte and the Bank of America, employees have worn "Humanyze badges" that can see and hear everything they do and analyze their speech volume and pitch and can track whom they spend time with and the physical path of their day (Steele 2020). While keyloggers have been a surveillance option for employers for two decades (Geist 2003), newer software such as Clickstream can collect very specific data and produce reports on how people use their computer and the internet throughout the day (Ajunwa et al. 2017). Remote workers may also be digitally surveilled with increased ease, with examples from ODesk.com (now called UpWork) whereby a photo is taken randomly by a front-facing camera six times every hour to estimate time at one's desk (Ajunwa et al. 2017) and from Crossover Worksmart whereby software takes screenshots at random to produce a "digital timecard" every 10 minutes to determine the amount of paid time the employee is working (Captain 2020). While the private sector is where many of these technologies have been piloted, they are increasingly present in the public sector as well, as described explicitly in the new "Policy on Service and Digital" by the Government of Canada (Government of Canada 2020). Some surveillance tools have clearer performance purposes compared to some other surveillance without clear purposes. There are many more examples of cutting-edge surveillance technologies in workplaces in Anglo-American contexts in addition to those identified above that we test explicitly in our survey of Canadians, the design of which is detailed in the next section.

Study Design

"Bureaucrat" is an amorphous term. The dimension we focus on is surveillance for two vivid examples of public servants with (typically) higher and lower appreciation among the public, a social worker ((Fukuyama 2013 and a government tax agent (Tummers et al. 2015). The empirical strategy for this study is to survey Canadians on questions of the reasonableness and intrusiveness of a dozen digital surveillance measures for two types of public sector workers (randomly assigned to respondents): (1) a public servant in the national capital working for the tax collection agency and (2) a social worker in an organization funded by government. These two areas of public service provide us with a maximal range of likability, which might impact one's assessment. One survey is administered to different subpopulations and completed both online and by phone. The first subpopulation is a sample of Canadian public servants from the Canadian Public Sector Research (CPSR) Panel created by the authors, which is a voluntary panel of public servants willing to answer online academic surveys related to the work they do for Canadians. At the time the survey was conducted (March 11–26, 2020), there were 1,206 members, 346 out of 402 who completed the surveys with few missing data, for a response rate of 27 percent. The second subpopulation of Canadians surveyed online was a sample of 2,001 Canadian citizens with the help of Léger Marketing, a national polling company, were surveyed from March 17–26, 2020. In this sample, we intentionally oversampled (n = 1,001) young adults (aged 18–30) in order evaluate hypotheses that younger citizens have lower expectations of privacy and higher degrees of comfort with technologies (Chao et al. 2018) as part of an analytical blocking strategy (Mutz 2011). As such, the sample of Canadians (n = 1,000) collected by Léger in the online survey was a nationally representative sample aside from age.

The final subpopulation is also a representative sample of another 1,008 Canadians, but it was administered by phone by Mainstreet Research, a national polling company. The motivation behind using a bimodal data collection strategy for the population-based citizen samples is to mitigate bias of the survey method, which was observed by Boivin and Cordeau (2017) in their study of citizen satisfaction with the Montreal Police Department; they found that telephone respondents were more likely to express satisfaction than online respondents even after controlling for demographics, victimization, and lifestyle. This was also discovered by Herian and Tomkins (2012) in a similar study in Nebraska. Furthermore, other researchers have speculated that members of the public who are registered with an online market research panel may have particular sensibilities toward digital surveillance than the wider public (Abraham et al. 2019; Chao et al. 2018) that we are able to test (and control for in our analysis).

The central task for all survey respondents was to identify, in their opinion, the "reasonableness" and "intrusiveness" of 12 emerging workplace surveillance measures for public sector employees. Similar to Slobogin and Schumacher (1993) who use experimental vignettes

to examine the impact of contextual elements on perceptions of their respondents, we have included technologies with clear performance purposes as well as those without clear purposes and randomly vary the type of public sector worker for whom these surveillance measures are targeting: a public servant in Ottawa working for the Canada Revenue Agency or a social worker in an organization funded by government.

Just as Slobogin and Schumacher (1993) used experimental vignettes to study the impact of contextual elements on the perceptions of their respondents, we borrow the same strategy in this study. Table 1 summarizes the items tested for reasonableness and intrusiveness. In terms of measures of reasonableness and intrusiveness, we followed methods used by Kugler (2014, 1,194), Chao et al. (2018, 295), and Slobogin and Schumacher (1993, 736), each of whom uses a 0–100 intrusiveness scale and a six-point reasonableness scale.

This survey is limited to Canadian public servants and citizens, but we believe the empirical story has the potential to inform debates in a cross-national context. To provide evidence of the extent of comparability of our Canadian sample to an American context, we replicate a survey question advanced by Rainie and Duggan (2016) at the Pew Research Center for Americans (n = 461) in relating to work surveillance. The question is as follows and was replicated in our survey:

Several co-workers of yours have recently had personal belongings stolen from your workplace, and the company is planning to install high-resolution security cameras that use facial recognition technology to help identify the thieves and make the workplace more secure. The footage would stay on file as long as the company wishes to retain it, and could be used to track various measures of employee attendance and performance.

Table 1 Workplace Surveillance Technologies and Their Descriptions as Presented to Respondents in the Surveys (Presented in Random Order)

Key logger: Records how many keys on your computer keyboard were touched per hour
AI email software: Algorithm uses keywords drawn from employee emails to report to bosses about the office's mood
Keycard with radio frequency identification (RFID): Tracking the location of employees and times in which workers are in the building
Internet usage: Reports on the websites workers spend time on and for how long
OccupyEye: Box under desk that senses a body in an office to track attendance and body heat measures
Handwashing badge: Sticker worn by employees to track handwashing practices at work
Random photo capture: Computer camera takes photo randomly six times every hour to ensure those working remotely are at their computer
Clickstream software: Tracks how computer users click and navigate the computer and internet during work hours
Wellness apps: Incentivized wellness programs at work using FitBit or similar technology to monitor physical activity.
Nonvisible camera: Hidden cameras in the workplace to measure the timing of breaks and movements around the office
Humanyze badges: Analyzes employees' speech through volume and pitch, notes who they spend time with, and maps the paths of their days
Facial recognition: Monitoring employee activity and enhancing security of the workplace

Would the scenario be acceptable to you, or not? **(Yes, No, It depends [please explain]).**

To the extent that Canadian respondents mirror the results from this question, we will be able to speak with greater confidence of the cross-national implications of our findings. We also asked all respondents questions about their views of their own colleagues (Yin et al. 2013) at work (or previous job if currently unemployed) and their general trust in others, as potential intervening variables on their reported perceptions of reasonableness and intrusiveness of various workplace surveillance technologies. The full survey can viewed in appendix A1 as can a demographic summary of all respondents, the public servants and the representative samples of Canadian citizens.

Results

On the measure of intrusiveness of the 12 work surveillance technologies, we observe a distinct pattern vis-à-vis public servant respondents and citizen respondents, as shown in table 2: generally a similar order with respect to the technology's intrusiveness but shifted approximately 10–17 points toward more intrusiveness according to public servant respondents compared to citizen respondents. This is expected given that the question is focused on the surveillance of a public sector worker, and thus public servants are likely thinking of the intrusiveness of these technologies in a very personal manner, whereas citizens are thinking about surveilling others—a key distinction observed in the literature (Slobogin and Schumacher 1993). Note that we inspected the results for any patterns in intrusiveness and reasonableness scores with respect to gender and ethnicity and found no large independent effects of these dimensions (age is explored further).

One finding of particular note, however, is that computer software surveillance (e.g., internet usage, Clickstream software, key logger, AI email analysis) is viewed as slightly less intrusive than cameras, photo capture, and Humanyze badges (which are basically a personal audio recorder' of one's work day), despite actually gathering more information on an individual. This may be due to camera and cameralike surveillance being perceived as surveillance without purpose or related meaningfully to performance but rather as a blunt surveillance instrument for general observance. Other arguably more invasive technologies are more tolerated likely because respondents can see their relationship to work productivity or performance, in particular that the surveillance produces a desirable effect on worker and team behavior.

There is a very strong correlation between one's sense of the intrusiveness of a technology and their views of its reasonableness for use in a public sector work environment. There are surveillance technologies outside of the realm of work, however, that are generally viewed as quite intrusive but nonetheless may be viewed as reasonable to use in certain contexts (e.g., ankle monitors as the condition for parole). For the work surveillance technologies examined here, keycards with RFID, which can capture movements around the office environment, was in the low range of intrusiveness according to our respondents (including public servants) but was viewed as unreasonable by public servants. This is likely due to an absence of an obvious surveillance–performance association, which can contribute to the rejection of some types of intrusive technologies.

Table 2 Workplace Surveillance Technologies and Perceived Intrusiveness and Reasonableness, Ranked

	Intrusiveness (0—not at all intrusive to 100 — extremely intrusive)			Reasonableness (1—very unreasonable to 6—very reasonable)		
	Citizens web survey	Citizens phone survey	Public servants web panel	Citizens web survey	Citizens phone survey	Public servants web panel
Technologies	Average intrusiveness	Average intrusiveness	Average intrusiveness	Median (and mean) reasonableness	Median (and mean) reasonableness	Median (and mean) reasonableness
Nonvisible camera	75.6% —	74.6% (n.s.)	89.9% (+14.3%***)	Unreasonable (m = 2.31, —)	Very unreasonable (m = 2.36*)	Very unreasonable (m = 1.59***)
Humanyze badges	74.7% —	75.4% (n.s.)	89.6% (+14.9%***)	Unreasonable (m = 2.38, —)	Unreasonable (m = 2.35)	Very unreasonable (m = 1.60***)
Random photo capture	73.1% —	72.8% (n.s.)	88.2% (+15.2%***)	Unreasonable (m = 2.39, —)	Unreasonable (m = 2.54, n.s.)	Very unreasonable (m = 1.67***)
OccupyEye	67.3% —	70.3% (+3.0%*)	84.4% (+17.1%***)	Unreasonable (m = 2.57, —)	Unreasonable (m = 2.56**)	Very unreasonable (m = 1.71***)
AI email software	68.1% —	68.7% (n.s.)	82.9% (+14.8%***)	Somewhat unreasonable (m = 2.74, —)	Unreasonable (m = 2.60***)	Very unreasonable (m = 1.93***)
Key logger	59.5% —	65.5% (+5.9%***)	73.8% (+14.3%***)	Somewhat unreasonable (m = 2.96, —)	Unreasonable (m = 2.76***)	Unreasonable (m = 2.21***)
Clickstream software	58.7% —	60.7% (n.s.)	69.4% (+10.7%***)	Somewhat unreasonable (m = 3.16, —)	Somewhat unreasonable (m = 3.05*)	Unreasonable (m = 2.70***)
Facial recognition	57.6% —	61.9% (+4.3%**)	68.9% (+11.3%***)	Somewhat unreasonable (m = 3.30, —)	Somewhat unreasonable (m = 3.08***)	Unreasonable (m = 2.65***)
Keycard with Radio Frequency Identification (RFID)	55.8% —	56.7% (n.s.)	64.9% (+9.1%***)	Somewhat unreasonable (m = 3.28, —)	Somewhat unreasonable (m = 3.25, n.s.)	Unreasonable (m = 2.89***)
Internet usage	55.8% —	56.1% (n.s.)	64.4% (+8.6%***)	Somewhat reasonable (m = 3.41, —)	Somewhat unreasonable (m = 3.28*)	Somewhat unreasonable (m = 3.85***)
Wellness apps	48.9% —	63.4% (+14.5%***)	56.1% (+7.2%***)	Somewhat reasonable (m = 3.55, —)	Somewhat unreasonable (m = 3.02***)	Somewhat unreasonable (m = 3.29*)
Handwashing badge	46.9% —	55.2% (+8.2%***)	63.6% (+16.7%***)	Somewhat reasonable (m = 3.66, —)	Somewhat unreasonable (m = 3.44**)	Unreasonable (m = 2.81***)
	(n = 2,001) representative sampling; young oversampled	(n = 1,008) weighted representative sampling	(n = 346)	(n = 2,001) representative sampling; young oversampled	n = 1,008) weighted representative sampling	(n = 346)

*** $p > 0.001$.
** $p > 0.01$.
* $p > 0.05$.

Previous research suggests that a lack a reciprocal trust between political officials and bureaucrats contributes to more technological surveillance within the bureaucracy (Fusi and Feeney 2018, 1,470), so to what extent does this extend to citizens vis-à-vis public servants? In contrast to Fusi and Feeney (2018), our samples included members of the public who mostly work in the private sector, although some are public servants themselves. We were also interested in examining how trust in one's colleagues and others more broadly may shape one's sense of the intrusiveness and reasonableness of various work surveillance technologies. Individuals who bear low trust for their coworkers might very well be more supportive of technologies surveilling their activities. The effect on individuals with lower trust in most people or distrust in supervisors on support for work surveillance has not been firmly established in the literature (Nakhaie and de Lint 2013; Weckert 2002). Figure 1 reveals how both one's trust in colleagues as well as others more generally moderately contributes to intrusiveness and reasonable scores across all the technologies (aggregated), differentiated by the two types of public sector workers who would be targeted by the work surveillance: a public servant in Ottawa working for the Canada Revenue Agency or a social worker in an organization funded by government.

The essential takeaway from figure 1 is that we find no systematic patterns among our respondents with regard to the intrusiveness or reasonableness of a work surveillance technology that is conditional on the type of public sector worker and that while trust in colleagues and trust in others shape the aggregated scores of intrusiveness and reasonableness, the substantive differences are negligible. The survey mode (online versus phone), however, seemingly produced much larger effects on intrusiveness and reasonable scores with those contacted by phone (n = 1,008) tending to find work surveillance technologies more intrusive and less reasonable than the Canadians contacted via a web panel (n = 2,001). We believe this to be a combination of the purposeful oversampling of younger cohorts in the web panel, as well as the

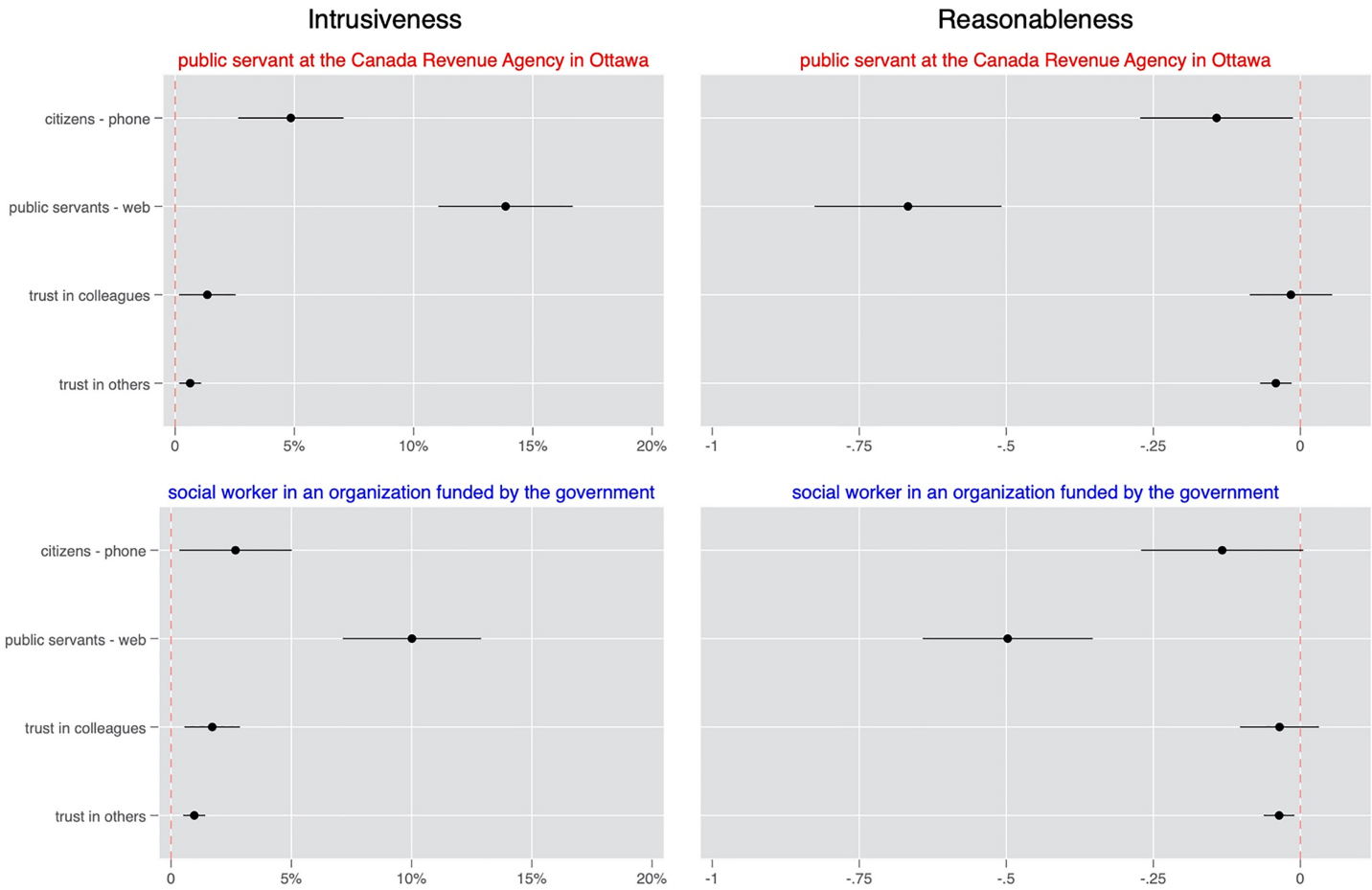

Figure 1 Trust in Colleagues, Trust in Others, and Survey Mode Effects on Aggregated Intrusiveness and Reasonableness Scores (Citizen Web Panel as the Base of Comparison) by Experimental Condition (CI = 95%)

mode (i.e., participants on web panels are likely more comfortable with technology). All that said, when trust in colleagues, trust in others, and the survey mode are held constant, the differences between public sector workers with higher and lower appreciation—social workers and Canada Revenue agents, respectively—are not large enough to be statistically significant.

To further investigate the potential of an age cohort effect, figure 2 illustrates the differences between younger (18–30, n = 1,169) and older (30+, n = 1,840) citizens in terms of their intrusiveness and reasonableness scores for 12 work surveillance technologies (representative web panel and weighted-representative phone survey data pooled). Younger citizens find wellness apps and handwashing badges on balance not intrusive, and most lean toward the position that they are "somewhat reasonable." Younger citizens mostly agree with other citizens as to the intrusiveness and reasonableness of OccupyEye, AI email software, and key loggers, even if they find them slightly less objectionable. Nevertheless, younger citizens find random photo capture software and internet usage monitoring statistically more intrusive and less reasonable than older cohorts. Age is not a distinguishing factor for the intrusiveness and reasonableness scores for nonvisible cameras, Humanyze badges, Clickstream software, facial recognition, and RFID.

The final area of data analysis speaks to the comparability of the findings from a Canadian context to elsewhere, in particular to the United States. Recall that we replicated a question from Rainie and Duggan's (2016) study (n = 461) with regard to the acceptability of office surveillance cameras with facial recognition capability for the purposes of security and performance analysis. Our large Canadian sample from the web panel mirrors closely the findings from the smaller U.S. online panel respondents on this question, with 52.3 percent finding them acceptable (z = 0.67; n.s.), compared to 54 percent. However, our representative phone respondents differ widely from the U.S. web panel participants; 28.8 percent find it acceptable (z = 9.31; $p < .001$). This may be explained by the fact that while both self-selecting to participate in a study, web panel participants are different than phone respondents because they had to register to a panel prior to a study, hence self-selecting twice. Phone surveys are costly, more than $10 dollars per respondent, rather than 55¢ per respondents on crowdsourcing platforms (Pedersen and Favero 2020, 27), but phone surveys reach citizens who are seldom studied otherwise, in particular those who may exhibit reticence with regard to the internet. Regardless, the close alignment of our web panel sample across the two countries to the same question related to work surveillance lends confidence to drawing inferences from this study to the American context.

Discussion

In designing this study, we set out to find—largely through media stories and tech journalism—the most cutting-edge workplace surveillance technologies being proposed or used in Anglo-American

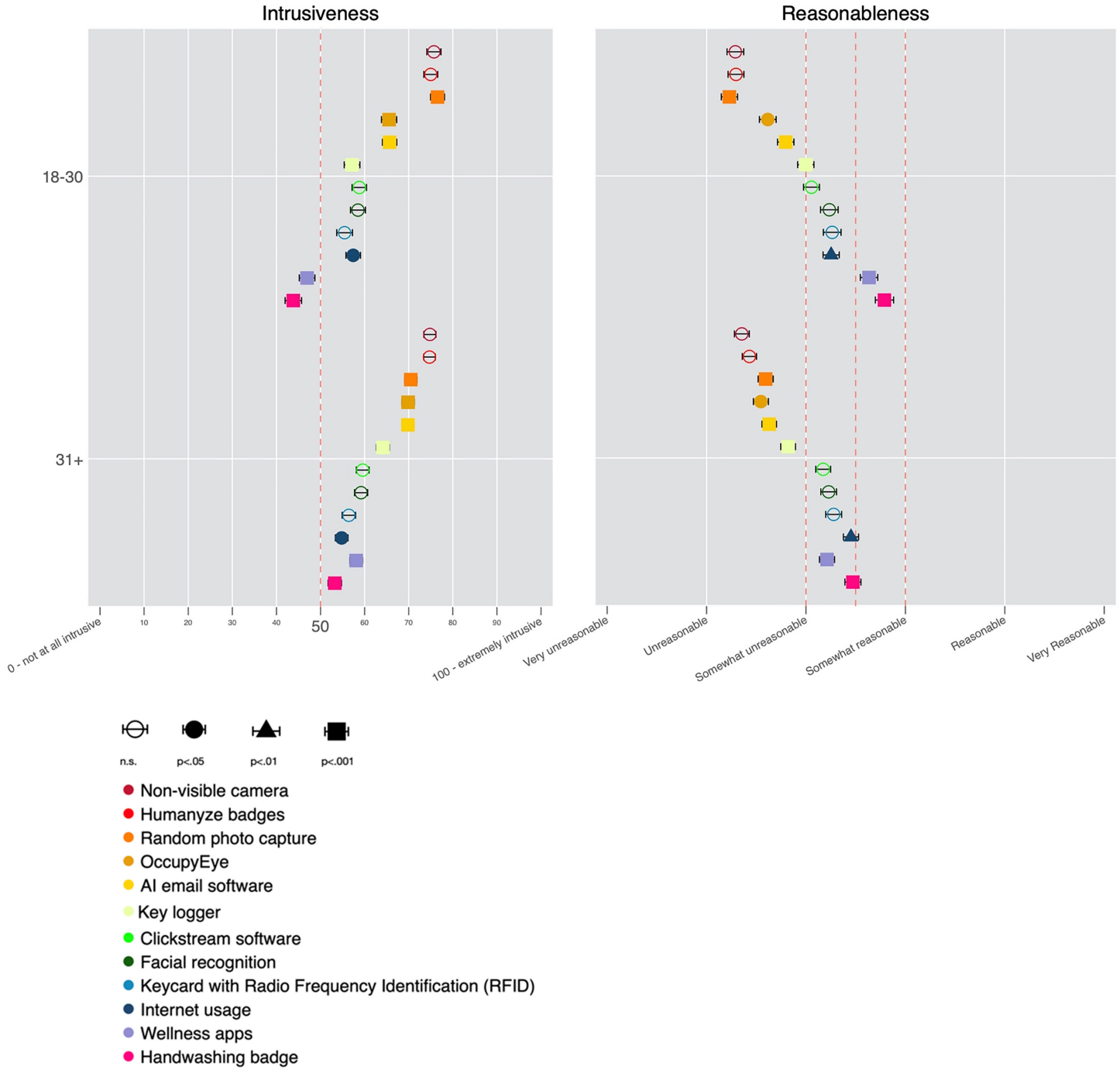

Figure 2 Differences between the Intrusiveness and Reasonableness Scores of 12 Work Surveillance Technologies According to Young (18–30 Year Olds; n = 1,169); and Older (30+Years; n = 1,840) Respondents (Representative Webpanel and Weighted-Representative Phone Survey Data Pooled)

contexts and to take their temperature among the Canadian public and public servants with regard to their sense of the technology's intrusiveness. We discovered that the Canadian public and public servants find most of the emerging surveillance technologies quite intrusive and their use unreasonable in public sector work environments. Yet, as we discovered earlier in the review of court and arbitration cases, judges and arbitrators are, by contrast, much more permissive of camera and phone technologies in the workplace and thus operate on assumptions about reasonableness that are often disconnected from those of the public. Determining the balance of worker privacy rights and employer desire to know the happenings of the workplace, particularly in the context of a sudden (and likely sustained) surge in remote working as a result of COVID-19, is key going forward.

From this study, we are able to deduce a number of dimensions of privacy concerns among those who would be surveilled, as well as the broader expectations of the citizenry with respect to what is reasonable, as depicted in table 3. Technologies that aim to capture the physical activity of employees (cameras, movement trackers, etc.) are viewed as slightly more intrusive than digital footprint technologies (keystroke loggers, Clickstream software, email AI

analysis), despite the fact that the latter actually collect more useful information from a productivity standpoint. All "very unreasonable" work surveillance technologies in table 3 have in common a lack of a clear surveillance–performance link; in other words, the surveillance is not so much associated with their work productivity and task achievements but about monitoring them or their bodies in the environment. It is also worth being mindful of the age cohort effects of work surveillance attitudes in the context of recruitment and retention in the public sector; new recruits are likely to be especially repulsed by work surveillance technologies such as random photo capture software and internet usage monitoring.

This speaks to the emotional content of workplace surveillance technologies that can influence morale and anxiety; thus, knowing the nature of the concerns of types of work surveillance on the employee side and of citizens more generally, as well as tolerance for some types of surveillance, is important for public sector employers and human resource managers as well as arbitrators and courts in cases of disputes. An empirical basis for claims of intrusiveness and reasonableness is an essential supplement to deductively derived principles of legal concepts such as "reasonableness" and can aid in achieving a more systematic balance and avoiding the arbitrary and conflicting findings we see in Anglo-American contexts with regard to reasonable and unreasonable workplace surveillance (Fradella et al. 2011, 371).

In their study, Slobogin and Schumacher (1993, 743) proffered that justices of the U.S. Supreme Court could use their results on work surveillance in four different ways: reject or ignore them, change their legal analysis to make the results of the judges–citizen gap null, incorporate the results in the way they reach decisions (including reversing themselves), or finally build a new way to model their decisions in the future to reflect the views of the members of the society they serve. Yet most of the questions about public sector work surveillance will not be sorted out in the courts but in the choices of public managers and human resource teams in conjunction with public service unions and privacy commissioners, which Fusi and Feeney (2018) confirm with their finding of the enormous variation in the use of work surveillance technologies in the United States. This research is aimed at building an empirical base from which to inform managers' and policymakers' ongoing conversation about appropriate public sector work surveillance that truly balances worker privacy rights and concerns with the employer's desire to maintain a productive workplace in a context of growing remote working outside of the traditional office environment. By focusing on the technologies that are certainly soon to be proposed, we are able to provide public sector parties a foundational analysis of these emerging technologies in relation to one another, as well as a framework in which to examine the trade-offs before they are put in place and become the source of controversy.

Table 3 Typology of the Surveillance-Performance Link and Views of Unreasonable Work Surveillance Technologies

	Median Respondent on Reasonableness (public servants)	
Clear Surveillance Performance Link	Somewhat Unreasonable or Unreasonable	Very Unreasonable
Yes	Key logger Clickstream software Internet usage	-
No	Facial recognition Keycard w/RFID Handwashing badge Wellness apps	Nonvisible camera Humanyze badges Random photo capture OccupEye AI email software

While we believe that an empirical basis for discussions is an important complement to negotiations over public sector work surveillance, there are limitations to this research, although much of which can be addressed in future research. First, when arbitrators or judges hear workplace privacy cases, they are considering many more elements and contextual details of a particular dispute; the item-vignette technologies in our survey are stripped of such context and thus represent abstractions, not cases. As others before us have acknowledged (Chao et al. 2018, 316), that is an inherent limitation to this method. At the same time, we could not have surveyed the public expecting them to read the amount of material that judges consider, but perhaps richer (but fewer) vignettes that add more contextual dimensions could be illuminating in a future study. A second limitation is that the Canadian sample may not travel as far as we assume. While we attempt to address this with a replication question from a 2016 Pew study of Americans to establish a measure of alignment of samples, further studies will need to investigate for the presence of country-specific norms of public sector work surveillance.

Conclusion

In their essay on the ethics of work surveillance in the public sector, West and Bowman (2016, 637) stated that "privacy is not just an individual right but also a societal good: The presumption of freedom and independence from being constantly watched and the ability to create one's professional role in an authentic manner. Strong reasons, then, must exist to subject employees to surveillance." We agree with this sentiment and further argue that we must be very careful about work surveillance as the technological capacity advances in such a way that it allows it to be done in a much more continuous, passive, and all-encompassing manner. Described as the third shock to the millennial paradigm, the COVID 19 pandemic has the potential to introduce a measure presented as temporary but that can become the new normal (Roberts 2020, 1). The ability to do it—and the relatively low-cost options from companies that provide such surveillance services—does not mean that public sector employers should do it or that it is the best manner in which to promote high performance among employees. Yet, at the same time, we ought to appreciate that the workplace is changing dramatically as part of a longer-term trend with surges in remote work outside the traditional environment in the context of COVID-19, and certainly thereafter, in which public managers need to responsibly adapt. The private sector is pioneering the use of these surveillance technologies—often with push back from employees—but the public sector in particular needs to get this right because it is working on behalf of citizens to support the governments they elect, and thus we are all invested in a public sector work environment that achieves a mutually acceptable—and reasonable—balance of privacy and surveillance in these settings.

Acknowledgments

We thank the members of the Canadian Public Sector Research Panel for participating in the research. We also thank Pr Nicholas

Jobidon for his initial suggestions about legal jurisprudence and Itizez Slama for her work with the panel's recruitment.

References

Abraham, Martin, Cornelia Niessen, Claus Schnabel, Kerstin Lorek, Veronika Grimm, Kathrin Möslein, and Matthias Wrede. 2019. Electronic Monitoring at Work: The Role of Attitudes, Functions, and Perceived Control for the Acceptance of Tracking Technologies. *Human Resource Management Journal* 29(4): 657–75.

Ajunwa, Ifeoma, Kate Crawford, and Jason Schultz. 2017. Limitless Worker Surveillance. *California Law Review* 105(3): 735–76.

Allard, Marc. 2020. *COVID-19: Les travailleurs sociaux n'ont pas tous besoin d'être sur le terrain, dit le ministre Carmant*. Quebec City, QC: Le Soleil.

Anteby, Michel, and Curtis K. Chan. 2018. A Self-Fulfilling Cycle of Coercive Surveillance: Workers' Invisibility Practices and Managerial Justification. *Organization Science* 29(2): 247–63.

Avey, Paul C., and Michael C. Desch. 2014. What Do Policymakers Want from us: Results of a Survey of Current and Former Senior National Security Decision Makers. *International Studies Quarterly* 58(2): 227–46.

Blumenthal, Jeremy A., Meera Adya, and Jacqueline Mogle. 2009. The Multiple Dimensions of Privacy: Testing Lay "Expectations of Privacy". *Journal of Constitutional Law* 11(2): 331–73.

Boivin, Rémi, and Gilbert Cordeau. 2017. Do Web Surveys Facilitate Reporting Less Favourable Opinions about Law Enforcement? *Security Journal* 30(2): 335–48.

Bozeman, Barry. 2019. Public Values: Citizens' Perspective. *Public Management Review* 21(6): 817–38.

Captain, Sean. 2020. *20 Years, your Boss May Track your every Glance, Keystroke, and Heartbeat*. Boston: *Fast Company*.

Cassidy, Megan. 2019. *Oakland, Calif., to Use Tech to Fight Police Corruption*. San Francisco: San Francisco Chronicle.

Chao, Bernard, Catherine Durso, Ian Farrell, and Christopher Robertson. 2018. Why Courts Fail to Protect Privacy: Race, Age, Bias, and Technology. *California Law Review* 106(2): 263–324.

Eltis, Karen. 2005. La surveillance du courrier électronique en milieu de travail: le Québec succombera t-il à l'influence de l'approche américaine. *McGill Law Journal* 51(3): 475–502.

———. 2015. Piecing Together Jones, A.B. and Cole: Towards a "Proportional" Model of Shared Accountability in Workplace Privacy. *Canadian Labour and Employment Law Journal* 18(2): 493–515.

Fradella, Henry F., Weston J. Morrow, Ryan G. Fischer, and Connie Ireland. 2011. Quantifying Katz: Empirically Measuring Reasonable Expectations of Privacy in the Fourth Amendment Context. *American Journal of Criminal Law* 38(3): 289–374.

Fric, Agathon. 2016. Reasonableness as Proportionality: Towards Better Constructive Interpretation of the Law on Searching Computers in Canada. *Appeal: Review of Current Law and Law Reform* 21: 59–82.

Fukuyama, Francis. 2013. What Is Governance? *Governance* 26(3): 347–68.

Fusi, Frederica, and Mary K. Feeney. 2018. Electronic Monitoring in Public Organizations: Evidence from U.S. Local Governments. *Public Management Review* 20(10): 1465–89.

Geist, Michael A. 2003. Computer and E-Mail Workplace Surveillance in Canada: The Shift from Reasonable Expectation of Privacy to Reasonable Surveillance. *Canadian Bar Review* 82(2): 151–90.

Government of Canada. 2020. *Policy on Service and Digital*. Ottawa, ON: Treasury Board of Canada https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32603. [accessed April 3, 2020].

Herian, Mitchel N., and Alan J. Tomkins. 2012. Citizen Satisfaction Survey Data: A Mode Comparison of the Derived Importance-Performance Approach. *American Review of Public Administration* 42(1): 66–86.

Ho, Daniel E., and Donald B. Rubin. 2011. Credible Causal Inference for Empirical Legal Studies. *Annual Review of Law and Social Science* 7: 17–40.

Hoetger, Lori. 2013. Did my Boss Just Read that? Applying a Coding Vs. Content Distinction in Determining Government Employees' Reasonable Expectation of Privacy in Employer- Provided Electronic Communication Devices after City of Ontario v. Quon, 130 S. Ct. 2619 (2010). *Nebraska Law Review* 90(2): 559–85.

Holmes, Aaron. 2020. *Employees at Home Are Being Photographed every 5 Minutes by an Always-on Video Service to Ensure they're Actually Working — And the Service Is Seeing a Rapid Expansion since the Coronavirus Outbreak*. New York: Business Insider.

Hunt, Chris, and Corinn Bell. 2015. Employer Monitoring of Employee Online Activities outside the Workplace: Not Taking Privacy Seriously. *Canadian Labour and Employment Law* 18(2): 411–58.

Johnson, Mathew. 2012. Privacy in the Balance - Novel Search Technologies, Reasonable Expectations, and Recalibrating Section 8. *Criminal Law Quarterly* 58(3): 442–509.

Kayas, O.G., T. Hines, R. McLean, and G.H. Wright. 2019. Resisting Government Rendered Surveillance in a Local Authority. *Public Management Review* 21(8): 1170–90.

Khullar, Ritu. 2012. Influence of Oakes Outside the Charter, Specifically Labour Arbitration Jurisprudence. *Ottawa Law Review* 43(3): 377–93.

Kugler, Matthew B. 2014. The Perceived Intrusiveness of Searching Electronic Devices at the Border: An Empirical Study. *University of Chicago Law Review* 81(3): 1165–211.

Levin, Avner. 2007. Big and Little Brother: The Potential Erosion of Workplace Privacy in Canada. *Canadian Journal of Law and Society* 22(2): 197–230.

McAllister, Marc. 2014. GPS and Cell Phone Tracking: A Constitutional and Empirical Analysis. *University of Cincinnati Law Review* 82(1): 207–56.

Miller, Norman. 2020, January 10th). *Massachusetts State Police Adopt New Officer-Tracking Tech*. Framingham, MA: Metrowest Daily News.

Mutz, Diana C. 2011. *Population-Based Survey Experiments*. Princeton, NJ: Princeton University Press.

Nakhaie, Reza, and Willem de Lint. 2013. Trust and Support for Surveillance Policies in Canadian and American Opinion. *International Criminal Justice Review* 23(2): 149–69.

Paterson, Moira. 2018. Regulating Surveillance: Suggestions for a Possible Way Forward. *Canadian Journal of Comparative and Contemporary Law* 4(1): 193–230.

Pedersen, Mogens Jin, and Nathan Favero. 2020. Social Distancing during the COVID-19 Pandemic: Who Are the Present and Future Non-compliers? *Public Administration Review* 80(4): 1–32.

Phillips, Emma. 2015. The Changing Dimensions of Privacy in the Workplace: Legal Rights and Labour Realities. *Canadian Labour and Employment Law Journal* 18(2): 467–91.

Rainie, Lee, and Maeve Duggan. 2016. *Privacy and Information Sharing*. Washington, DC: Pew Research Center.

Ravid, Daniel M., David L. Tomczak, Jerod C. White, and Tara S. Behrend. 2020. EPM 20/20: A Review, Framework, and Research Agenda for Electronic Performance Monitoring. *Journal of Management* 46(1): 467–91.

Roberts, Alasdair. 2020. The Third and Fatal Shock: How Pandemic Killed the Millennial Paradigm. *Public Administration Review* 80(4): 1–7.

Schuster, Christian, Lauren Weitzman, Kim Sass Mikkelsen, Jan Meyer-Sahling, Katherine Bersch, Francis Fukuyama, Patricia Paskov, Daniel Rogger, Dinsha Mistree, and Kerenssa Kay. 2020. Responding to COVID-19 through Surveys of Public Servants. *Public Administration Review* 80(4): 1–20.

Scott-Hayward, Christine S., Henry F. Fradella, and Ryan G. Fischer. 2015. Does Privacy Require Secrecy? Societal Expectations of Privacy in the Digital Age. *American Journal of Criminal Law* 43(1): 19–60.

Slobogin, Christopher, and Joseph E. Schumacher. 1993. Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at "Understandings Recognized and Permitted by Society". *Duke Law Journal* 42(4): 727–75.

Smith, Alisa, Sean Madden, and Robert P. Barton. 2016. An Empirical Examination of Societal Expectations of Privacy in the Digital Age of GPS, Cell Phone Towers, & Drones. *Albany Law Journal of Science and Technology* 26(1): 111–42.

Steele, Chandra. 2020. *The Quantified Employee: How Companies Use Tech to Track Workers*. New York: PC Magazine.

Taylor, Frederick W. 1912, 2012). Scientific Management. In *Classics of Public Administration* (Vol. 7th, pp., edited by Jay M. Shafritz and Albert C. Hyde, 37–43. Boston: Wadsworth.

Thompson, Clive. 2020. June 9th. In *What if Working from Home Goes on … Forever?* New York: New York Times Magazine.

Tummers, Lars L., Victor Bekkers, Evelien Vink, and Michael Musheno. 2015. Coping during Public Service Delivery: A Conceptualization and Systematic Review of the Literature. *Journal of Public Administration Research and Theory* 25(4): 1099–126.

Weckert, John. 2002. Trust, Corruption, and Surveillance in the Electronic Workplace. In *Human Choice and Computers: Issues of Choice and Quality of Life in the Information Society*, edited by Klaus Brunnstein and Jacques Berleur, 109–20. Boston: Springer.

West, Jonathan P., and James S. Bowman. 2016. Electronic Surveillance at Work: An Ethical Analysis. *Administration & Society* 48(5): 628–51.

Appendix

		Citizens Web Survey	Citizens Phone Survey	Public Servants Webpanel
		(n = 2,001)representative sampling; young oversampled	(n = 1,008)weighted representative sampling	(n = 346)
Age	18–30	50.2% (1005)	17.6% (≈177)	13.3% (46)
	31–40	14.3% (284)	22.6% (≈228)	29.2% (101)
	41–54	14.4% (297)	24.0% (≈242)	35.6% (123)
	55+	20.7% (415)	35.7% (≈361)	22.0% (76)
Gender	Female	50.7% (1015)	44.4% (≈447)	53.8% (186)
	Male	48.4% (968)	49.1% (≈495)	44.2% (153)
	Nonbinary, transgender, rather not say	1.4% (18)	6.6% (≈66)	2.0% (7)
Canadians come from all over the world. What is your ethnic origin?	European	59.5% (1191)	62.6% (≈631)	68.5% (235)
	Black	3.8% (75)	4.5% (≈45)	1.5% (5)
	South Asian	6.5% (129)	3.5% (≈35)	4.1% (14)
	East Asian	7.4% (148)	1.6% (≈16)	5.3% (18)
	Latin America	2.0% (40)	1.3% (≈43)	2.0% (7)
	Indigenous	2.0% (40)	3.6% (≈37)	1.2% (4)
	Other	11.9% (239)	7.2% (≈72)	10.8% (37)
	Prefer not to say	7.0% (139)	15.7% (≈158)	6.7% (23)
Education	High school/GED	34.5% (691)	17.3% (≈175)	0.9% (3)
	College diploma or vocational training	28.8% (576)	30.1% (≈304)	7.2% (25)
	Undergraduate degree	25.8% (517)	29.6% (≈299)	29.2% (101)
	Masters or add. Professional training	9.0% (180)	18.6% (≈187)	56.1% (194)
	Medical or doctorate degree	1.9% (37)	4.3% (≈44)	6.7% (23)