




# Measuring the Acceptability of Facial Recognition-Enabled Work Surveillance Cameras in the Public and Private Sector

Carey Doberstein<sup>a</sup> , Étienne Charbonneau<sup>b</sup>, Geneviève Morin<sup>c</sup>, and Sarah Despatie<sup>a</sup>

<sup>a</sup>University of British Columbia; <sup>b</sup>Canada Research Chair in Comparative Public Management, École nationale d'administration publique; <sup>c</sup>École nationale d'administration publique

## ABSTRACT

Electronic performance monitoring is expanding rapidly in public and private sector environments amidst evidence that when privacy concerns are raised by employees in arbitration and judicial proceedings, there is limited empirical foundation for what constitutes a reasonable expectation of privacy among everyday citizens. This study replicates and expands on Rainie and Duggan's U.S. study of the acceptability of facial recognition-enabled camera surveillance in the workplace with three separate Canadian survey sample populations. We find that private sector workers tolerate cameras in the workplace more than public sector workers and that the younger age cohort, for both private and public sector workers, is more likely to tolerate cameras in the workplace than the older cohort. Further, through analysis of qualitative comments among those ambivalent about camera surveillance at work, we find that concerns over transparency, safety and authoritarianism were the most frequent themes. These results point to the considerations employers must face for surveillance practices to be viewed as reasonable by employees in both public and private sectors.

## KEYWORDS

Facial recognition; electronic performance monitoring; privacy; surveillance cameras; work surveillance

## Introduction

Work surveillance in various forms and for various purposes has always existed, and emerging technologies allow for a kind of electronic surveillance that is more present and intrusive than before. New technologies that track internet use, read emails with artificial intelligence to gauge office “mood,” and body sensors at desks to track presence and performance have been introduced in the private sector and likely soon to the public sector, generating considerable controversy (Ajunwa et al., 2017). Yet a classic

**CONTACT** Étienne Charbonneau  [etienne.charbonneau@enap.ca](mailto:etienne.charbonneau@enap.ca)  École nationale d'administration publique, 4750 Henri-Julien, 5th floor, Montreal, QC H2T 3E5, Canada.

This article has been republished with minor changes. These changes do not impact the academic content of the article.

surveillance tool—the video camera—continues to expand into workplaces with ever more resolution and capability, such as facial recognition. Video surveillance is most often advanced by employers to increase safety and reduce liability, protect employers' property, and monitor employee productivity (Ciocchetti, 2011, p. 322). One particular threat that can motivate the decision to deploy cameras in a professional workplace is employee theft (Hagen et al., 2018, p. 281). A 2014 survey of 790 American mid-sized cities found that 42% of municipal governments had at least one department monitored by video cameras (Fusi & Feeney, 2018, p. 1474). An American Management Association survey of over three hundred private sector firms reported more than a decade ago that 55% use video cameras to monitor employees for theft or performance purposes (AMA, 2007). The widespread deployment of video surveillance cameras in public and private workplaces in liberal democracies presents various legal, political and administrative questions around reasonableness, purpose, and effectiveness (Bennett & Bayley, 2005, p. 85).

The answers to such questions are complex, often contingent or contextual, and require a more empirically-informed analysis of the factors that shape employee reactions and behavioral responses. Privacy considerations, including those at work, rest on the conceptual foundations of the notion of “reasonable expectations” of privacy in western democracies. Arbitrators and courts are those most often tasked with reaching decisions about what constitutes invasions of privacy in the public and private spheres. That has consequences for public management, as it sets the parameters of what is reasonable or not in terms of surveillance. A recent study showed, however, for several work surveillance technologies, there is a gap, often large, between what arbitrators and courts consider reasonable or intrusive and how the typical or median person sees it (Charbonneau & Doberstein, 2020). Hence, a better understanding of what forms the foundations of employee ambivalence to workplace surveillance can help human resource managers—and ultimately arbitrators and courts in the case of serious disputes—navigate this contested terrain. Empirical data can substitute for intuitions in the calibration of HR guidelines, policies, and eventually, laws.

This research aims to address these gaps by surveying more than 3,000 Canadian public and private sector employees as part of a larger study on classic and emerging workplace surveillance technologies. In this study, we ask: *what are the personal and contextual elements that shape employee views on the reasonableness of workplace camera surveillance? How do personal and contextual elements interact to shape these views?* A recent review of this literature by Ravid et al. (2020) concluded that an understanding of the interactive effects of personal (e.g., age, level of trust) and contextual

(e.g., sector of work, purpose of surveillance) elements of electronic performance monitoring constitute a major research gap in the field. This study specifically responds to this call.

We replicate and build on a short scenario vignette involving facial recognition-enabled workplace cameras presented to Americans by researchers at the Pew Research Center meant to tests the tradeoffs that citizens see between safety and privacy at work (Rainie & Duggan, 2016). While the response fields for the vignette scenario replicated from Rainie and Duggan (2016) were limited to “Yes” (it is reasonable), “No” (it is not reasonable), and “It depends,” only the latter option permitted text-based elaboration by respondents. As we will see in this study, for Canadians this is not a clear case: 41% of Canadians agree with work cameras to prevent theft, while 41% of Canadians disagree. More importantly, 18% of Canadians say “it depends.” In this context, the median Canadian worker does not agree with the prevailing interpretation of policies and laws shaping the workplace. Thus, we are particularly interested in those who display ambivalence to this scenario, and are in a position to analyze and synthesize the source(s) of the contingent response to camera-based work surveillance in Canada. From this open-ended response field, we present a content analysis of respondents who expressed an ambivalent answer to the scenario. Understanding the contextual elements that may push undecided or ambivalent citizens into agreement or disagreement with surveillance becomes critical for human resource (HR) departments and public service associations negotiating the implementation of video cameras at work. This has important implications not only for future legal disputes but also for job satisfaction in organizations and, hence, on performance.

The expanding reach of surveillance not only has implications for public law and privacy, but also can inform human resource and public service association negotiations on surveillance policies. By exploring the reasons why some workers are ambivalent to work surveillance measures like cameras with facial recognition capability, we can identify patterns that emerge while preserving nuance and the complexity of experience in a highly contingent environment. To the extent we are better able to measure and assess the contexts in which such workplace surveillance is tolerated versus resisted, managers can avoid morale loss, work teams can build trust, and employers and employees can avoid engaging in costly arbitration or even litigation.

The article proceeds as follows. First, we review the electronic performance monitoring literature, and connect it to analytical frameworks concerned with surveillance technologies in the private and public sector from the public administration and organizational management literatures, to reveal empirical gaps in our understanding of the highly contingent

foundations of the anxieties among the surveilled. Second, we describe the research design for this study and the main hypotheses that can be answered with parallel surveys of public and private sector employees in Canada. Third, we present the quantitative comparative results of our populations of interest and following that focus on the respondents who demonstrated ambivalence to the vignette scenario with qualitative content analysis of their text-based responses. We find that the Canadian sample departs in interesting ways with the original Rainie and Duggan (2016) study with an American sample and that respondents most frequently mentioned high levels of transparency concerns, administrative and safety concerns, and authoritarian concerns as the source of their ambivalence. The final section contemplates the implications of the findings across private and public sector workplaces not only in Canada, but also in similar jurisdictions, in terms of future legal disputes and its impacts on job satisfaction, particularly in the public sector.

## Literature review

Workplace surveillance in a contemporary context in both private and public sectors is advanced for often twin goals of security and performance monitoring, extending well beyond the mere efficiency-enhancing objectives of classic Taylorism (Ciocchetti, 2011). While the private sector workplace has often been the focus of studies related to surveillance (Bhave et al., 2020; Ravid et al., 2020), the public sector is an especially critical area for investigation, as it includes not only government offices, but schools, hospitals, police services and beyond, thus introducing unique considerations for how surveillance can damage services delivered and guaranteed to the public (Kayas et al., 2019, p. 1170). Few public administration studies have considered the effects of norms or practices particular in the public sector, including greater unionization and employee protections. In this way, comparing the differences of employees' privacy calculus in the public and private sector was one of Bhave et al.'s (2020, p. 147) priorities for future research.

Analyzing the personal and contextual elements of workplace surveillance matters because monitoring deemed unfair by employees increases their stress and lowers their satisfaction (Young, 2010). It can even translate into engagements in resistance and creative avoidance (Kayas et al., 2019). In the literature, workplace surveillance tends to receive its highest support among employees when it is justified on—and targeted accordingly to—security concerns, in particular reducing theft or embezzlement (Oz et al., 1999), but can nonetheless undermine the trust employees believe they should be granted as part of their position (Botan & Vorvoreanu, 2005).

The lowest support for workplace surveillance typically concerns performance monitoring—that is, inducing greater productivity and efficiency in employees—with many believing it has a negative effect on productivity and job satisfaction (Oz et al., 1999). However, some older experimental studies find no negative effects of performance monitoring on productivity or job satisfaction (Griffith, 1993; Nebeker & Tatum, 1993). More recent research suggests, however, that one’s opinion of electronic performance monitoring (EPM)—defined as the “now-common use of technological means to observe, record, and analyze information that directly or indirectly relates to employee job performance” (Ravid et al. 2020, p. 101)—whether positive or negative, strongly shapes the perceived effects on productivity and job satisfaction (Samaranayake & Gamage, 2012). For example, a recent quantitative study of 163 private sector employees finds that technological spatial intrusion (e.g., such as cameras or other technological monitoring) is deeply dependent upon context in terms of being seen as productivity-enhancing or alternatively as a privacy violation (Chandra et al., 2020, p. 8). They found that monitoring that was highly individualized and with no anonymity was much less favored as a performance-enhancing mechanism.

Workplace surveillance technology can be seen as caring or coercive, depending on the motivations perceived by workers; the observed ultimately have a say in what technologies are considered coercive or caring (Anteby & Chan, 2018, p. 248). These same authors, from 89 interviews with U.S. Transportation Security Administration officers, leads, and supervisors in a large urban airport, developed a model of self-fulfilling coercive surveillance where workers see surveillance as coercive, and thus find ways to disappear from camera sightlines or try to keep to themselves forgotten by supervisors (p. 254). That is, workplace surveillance cannot be equated to a fly on the wall effect—it can produce certain behaviors that would likely not manifest without the surveillance. As such, to the extent employees interpret work surveillance as coercive, workers will practice “invisibility”; managers may then use these behaviors as justifications for surveillance, and further increase surveillance, which workers may interpret as coercive (p. 258).

The classic workplace surveillance tool—the video camera—is evolving with technological advancements of facial recognition. Facial recognition can drastically reduce anonymity in video surveillance with algorithmic analysis of pictures in a database (Nunn, 2004, p. 16–17). Facial recognition is widely accepted in some forms, like in playful social media apps or when sorting photos into automated digital albums (Lyon, 2018, p. 88), and resisted in other forms (Busuioc, *forthcoming*, p. 1), such as when police forces use it. Thus, in a policing context, White and Malm (2020, p. 11)

argue that “concerns from local stakeholders should inform, if not dictate, future decisions” that contemplate facial recognition capabilities to body worn cameras. Facial recognition is a potent way in which algorithms change the rules and test guidelines, such as “reasonable suspicion,” that were developed in an analog world (Fergusson, 2017, p. 56).

Facial recognition is seldom mentioned in discussions about artificial intelligence in public administration research, and even less studied empirically. It is typically mentioned in passing in relation to policing applications (Bullock, 2019, p. 752; Wirtz et al., 2020, p. 826) or CCTV surveillance in public spaces (Henman, 2020, p. 213). Some concerns, like high error rates when comparing individuals to wide pools of stock photos, are less salient when a smaller number of employees need to be compared to a small database of ID card pictures, but the invasiveness of facial recognition is nonetheless an important development in workplaces that needs to be analyzed within a broader framework of employee surveillance.

There are several personal traits of the surveilled that have been examined in the literature that relate to their tolerance or resistance. We focus on three such characteristics: the age of employee, their trust in others, and whether they work in the public or private sector. Various studies have examined the age effects on views of privacy from the state generally, as well as specifically with respect to workplace surveillance. Chao et al. (2018), for example, in a survey of Americans on privacy in the context of police practices find that younger and older cohorts had lower privacy concerns than middle age cohorts, a finding roughly mirrored by Kugler and Strahilevitz (2016). Yet specifically on camera surveillance, others have alternative expectations, arguing that young adults tend raise more privacy concerns toward camera surveillance than the rest of the population—as older adults tend to feel less secure from crime (Leman-Langlois, 2009, p. 45)—meanwhile Rainie and Duggan (2016, p. 15) did not find that age made a difference (though they had a relatively small sample size and lower statistical power).

One’s personal trust assessment of colleagues and others in society is likewise theorized to influence toleration of camera surveillance. Social psychology research tells us that if one has little trust in others, they may support surveillance mechanisms because it creates a context that is less reliant on trust as a dynamic in that setting, and instead reliant on technology for security (Chan, 2008; Mirowsky & Ross, 2006). Furthermore, the presence of cameras itself can affect how employees perceive their employers’ views of their own trustworthiness (Christ et al., 2008). This lack of trust felt by public sector employees that were the object of video surveillance was documented in council departments in the U.K. (Kayas et al., 2019, p. 1178) and with public and private school teachers in Israel (Perry-

Hazan & Birnhack, 2019, p. 199). An Israeli female elementary teacher who transferred to a school without cameras commented that:

This feeling that you're not trusted ... to know that you're constantly under inspection is uncomfortable... You're working hard, and you're doing your job as best as you can, and you're constantly being inspected ... And suddenly, now I'm in [another school] and I don't have cameras. I supervise [school] recesses ... and I feel a relief, a huge relief. (Perry-Hazan & Birnhack, 2019, p. 199).

Finally, a comparatively under-studied dimension of workplace surveillance analysis is the public-private distinction. Most of the workplace surveillance literature is focused on private sector settings, but the public sector has not only unique dimensions but also norms that may shape how camera surveillance is perceived. For example, in the private sector the employee-employer relationship is typically employer-dominated in terms of workplace rules and norms, whereas in most public sector settings employee protections and workplace conduct is jointly determined by strong bargaining associations. Furthermore, the public sector is comprised of perhaps uniquely sensitive contexts, whether government offices, medical and social services, or educational environments, for which camera surveillance may be viewed less favorably. In this vein, Boyne (2002) hypothesizes that higher expectations of privacy may be a particular trait of publicness that demarcates public sector employees from private sector ones (p. 103). This is a critical distinction to explore given that tests of reasonableness in terms of surveillance in relation to privacy hinge on expectations and norms in particular contexts.

Based on the literature reviewed above, we posit the following hypotheses regarding our variables of interest as they relate to tolerance of workplace camera surveillance:

H1: Younger age cohorts are more likely than older age cohorts to find the camera surveillance scenario acceptable.

H2: Low trusters are more likely than high trusters to find the camera surveillance scenario acceptable.

H3: Private sector workers are more likely than public sector workers to find the camera surveillance scenario acceptable.

Beyond the personal dimensions related to tolerance of work surveillance, Ravid et al. (2020) have put forward the most theoretically-informed and comprehensive typology of the situational elements of electronic performance monitoring (EPM) from an extensive systematic review of the literature. They advance four key elements: purpose (of surveillance), invasiveness (the reach of the surveillance), synchronicity (time dimensions of surveillance and feedback), and transparency (about its use and aims), each with sub-elements and categories that usefully differentiate the



characteristics of surveillance. With this typology, Ravid et al. (2020) invite researchers and analysts to account for the multi-dimensional situational dynamics of workplace surveillance. This more exploratory analysis is conducted with qualitative data collected in this study among those who report ambivalence to camera surveillance. By using the typology, we can systematically identify what characteristics of EPM are driving ambivalence concerning workplace camera surveillance, and contribute to an empirically-informed debate around its reasonableness in private and public sector environments.

### **Study design**

This study replicates and builds on Rainie and Duggan's (2016) Pew Research Center study—and specifically a question they asked about workplace camera surveillance in the form of a vignette scenario—to examine the personal and contextual dimensions undergirding support, opposition, or ambivalence to surveillance. A vignette is a “short description of a person or a situation that contains information that is considered relevant and that is presented to respondents to obtain a judgment about that person or situation” (Rooks et al., 2000, p. 129). The question is as follows, and was replicated in our survey:

*Several coworkers 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.*

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

Rainie and Duggan (2016) reported that 54% of Americans found it acceptable, 24% unacceptable, and 21% answered that “It depends.” The researchers report that gender, age, and socioeconomic status did not impact the propensity to find the scenario acceptable (Rainie & Duggan, 2016, p. 15). After analyzing the open-ended comments, Rainie and Duggan (2016) offered eight inductively-derived themes to synthesize the comments they gathered: the arguments for the presence of the cameras (it is the employer's right; it is for the security of workers), the mitigating factors (acceptable if it is equal for everyone; acceptable if the footage is not kept indefinitely; acceptable if it is only to stop theft) and the arguments against (it should not be used to track performance; it is too intrusive by design; and it cannot solve the problem).

This replication study in a Canadian context is comprised of three identical surveys released in March 2020 focused on different target populations



and survey modes, which together aim to assess public and private sector workers' perspectives on work surveillance and explore the nature of feelings of ambivalence to it. The total number of respondents is 3,355. The first target population is a sample of Canadian public servants from the *Canadian Public Sector Research Panel* (CPSRPanel). That panel, created and managed by the authors, includes federal and provincial public servants throughout Canada who volunteer to be surveyed for academic research. Of the 1,206 CPSRPanel members, 346 replied to this survey, for a response rate of 27% response rate. The second target population is a sample of  $n=2,001$  Canadians surveyed online with the help of Léger Marketing, a national polling company. In this sample, we intentionally oversampled ( $n=1,005$ ) young adults (aged 18–30) to evaluate hypotheses that younger citizens have lower expectations of privacy and higher degrees of comfort with surveillance technologies (Chao et al., 2018), as part of an analytical blocking strategy (Mutz, 2011). We believe it is worthwhile to oversample young respondents in the second survey to lend additional data to this contested question. The remainder of the sample of Canadians ( $n=1,000$ ) collected by Léger in the online survey was a nationally representative sample.

The final target population is also a representative sample of another 1,008 Canadians, but it was administered by phone by Mainstreet Research, a national polling company. Survey respondents via web panels self-select twice: once to register to a panel, and then again to complete a specific survey. Survey respondents via phones self-select once: by deciding to answer (or not) a survey, seconds after being cold-called by a pollster. Previous research also reveals discrepancies between web panelists responses and respondents asked the same questions by phone (Boivin & Cordeau, 2017; Herian & Tomkins, 2012). Taking the digital-divide seriously, we wanted to address a limitation identified by previous studies relying exclusively on web surveys to assess perspectives on digital surveillance (Abraham et al., 2019; Chao et al., 2018).

The identical surveys sent to each of the three target populations and survey modes explore multiple aspects and dimensions of emerging workplace surveillance technologies in terms of intrusiveness and reasonableness. Yet the results in this article focus solely on reporting the replication of the Rainie and Duggan (2016) inquiry on workplace camera surveillance with facial recognition capability for both security and performance monitoring purposes, using both quantitative and qualitative analysis. The quantitative data analysis explores the link between demographics, work sector, trust variables, and the tolerance for the cameras in their workplace, whereas the qualitative data analysis that follows allows us to examine the interactive effects of surveillance characteristics among those who are ambivalent.

The main independent variables that relate to the core hypotheses articulated above are measured with direct questions related to sector of work and age. Trust in this context, however, is typically measured with different scales in the literature. Our first scale is adapted from Yin et al.'s (2013) "Trust in Colleagues Scale." Some workers might find their particular colleagues undeserving of trust, and hence might be more supportive of work video surveillance. Our second measure is the generalized trust scale, a one item question used in the European Social Survey and the World Values Survey, that asks respondents if, "generally speaking, would you say that most people can be trusted, or that you can't be too careful in dealing with people?" That question is a mainstay of research on trust (Kääriäinen & Sirén, 2012; Van de Walle & Lahat, 2017). Some individuals are just less trusting to others by default, and we would expect that they would be more tolerant of worker surveillance.

This vignette scenario is particularly useful to explore as a replication, as it provides comparative data in a Canadian context, but also because the design of the question offers the opportunity for respondents to explain their position on the issue if they select the option "It depends" when asked whether that vignette scenario is acceptable to them (as done in Rainie & Duggan, 2016). The total sample of respondents from all three surveys is  $n = 3,355$  and of those, 465 respondents who answered "It depends" offered an open-ended response further articulating the nature of their ambivalence. The supplementary qualitative analysis does not lend itself to hypothesis testing, but rather is an exploration of the interactive effects of personal attributes and contextual variables, as informed from Ravid et al.'s (2020) typology.

## Data

The respondents' demographic characteristics of our three survey samples are summarized in Table 1, but there are a few points worth emphasizing before presenting the quantitative analysis results. First, while one of the three surveys targeted Canadian public servants from a panel that the authors created and manage, we nonetheless captured additional public servants in the other two surveys. As such, we have  $n = 967$  public servants in our global sample and  $n = 2,388$  private sector workers. Second, since we intentionally oversampled young people (age 18–30) in one survey, but also captured young people in the other surveys, we have a total of  $n = 1,228$  in that age bracket and  $n = 2,217$  in the above-31 age bracket. Finally, in terms of other variables that we will be drawing on in the analysis, there is some variation in the public servant sample versus the other two general population surveys on the question of "trust in others," with those in the public sector more trusting than the general population.

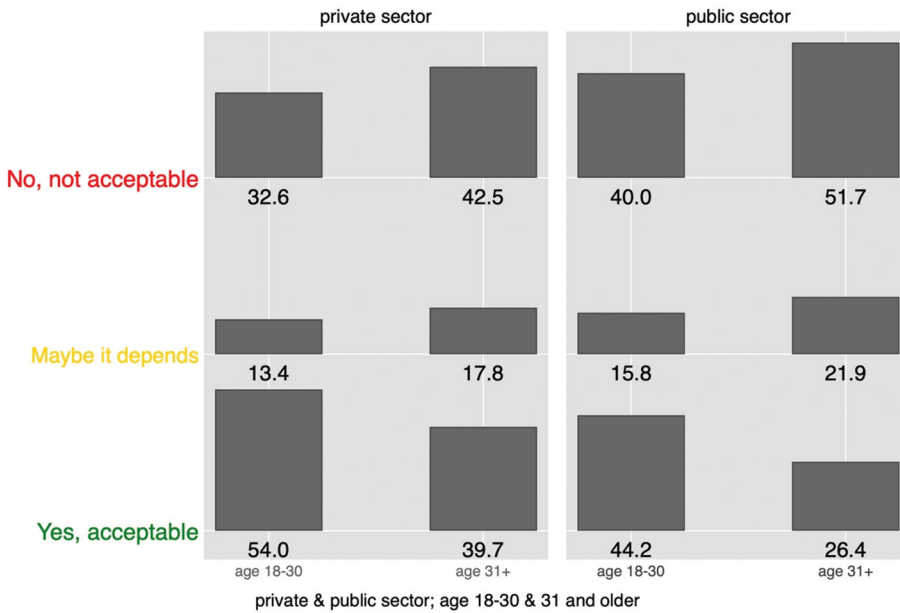
**Table 1.** Descriptive Statistics for the Three Identical Surveys in Canadian Context Replicating Rainie and Duggan's (2016) U.S. Study.

	Citizens Web survey ( <i>n</i> = 2,001) Representative sampling; young oversampled	Citizens Phone survey ( <i>n</i> = 1,008) Weighted representative sampling	Public servants Web panel ( <i>n</i> = 346)
Public sector employee?			
Yes	18.3% (366)	25.3% (255)	100% (346)
No	81.7% (1635)	74.7% (753)	0% (0)
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)
Non-binary, transgender, rather not say	1.4% (18)	6.6% (66)	2.0% (7)
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)
Trust in colleagues			
Five-question mean index	<i>m</i> = 4.5	<i>m</i> = 4.4	<i>m</i> = 4.9
1 strongly disagree to 6 strongly agree			
Trust in others			
0 You can't be too careful to	<i>m</i> = 5.8	<i>m</i> = 5.4	<i>m</i> = 6.9
10 Most people can be trusted			

## Results

### Quantitative analysis

Our results depart from the U.S. study from Rainie and Duggan (2016), in which 54% viewed the surveillance vignette as acceptable and 24% unacceptable. In our Canadian sample of more than 3,300 respondents, they split with 41% finding the situation depicted in the vignette as acceptable, 41% not acceptable, with 18% in the “It depends” category. Given the



**Figure 1.** Differences of agreement of camera work surveillance, by sector of employment and age category, in percentages. Private sector:  $\chi^2(2) = 47.2$ ,  $Pr = 0.000$ ; Public sector:  $\chi^2(2) = 28.5$ ,  $Pr = 0.000$ .

even split in acceptable/not acceptable, and the fact that neither constitutes a majority, we are especially interested in the “It depends” respondents, as probing those ambivalent to this situation can inform the contexts in which a majority may find the surveillance practice reasonable.

Figure 1 presents the descriptive results of the acceptability measure, differentiated jointly by age cohorts and work sector for respondents. It shows that private sector workers tolerate cameras in the workplace more than public sector workers and that the younger age cohort, for both private and public sector workers, is more likely to tolerate cameras in the workplace than the older cohort.

Before exploring our main qualitative analyses in detail, summary quantitative analyses can help set the table and establish the broad parameters of the results. Table 2 presents the relative importance of predictors to the acceptance of camera surveillance in the workplace when all other independent variables are controlled. Table 2 features regression coefficients following a multinomial logit regression. There are no statistically significant differences on the four variables between respondents who are ambivalent and those who find the vignette “not acceptable.” However, respondents who find the vignette acceptable are different than the ones who do not find it acceptable. All reported coefficients here are for a one standardized deviation increase of the independent variable. All things being held equal,

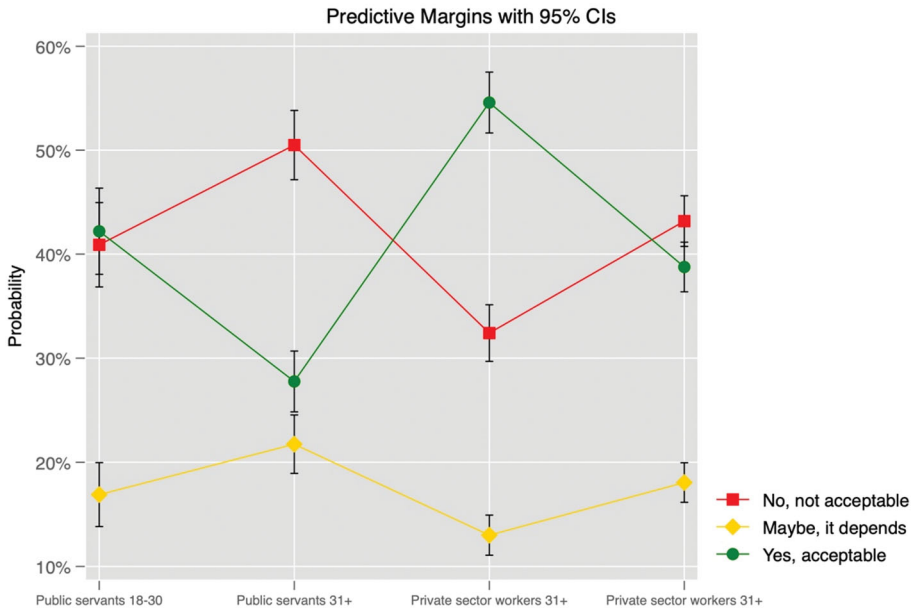
**Table 2.** The Relative Importance of Predictors to Agreeing That Cameras at Work Are Acceptable, After a Multinomial Logit Regression, “No, Not Acceptable” as Based Outcome, Standardized Coefficients.

	Percent change in odds vs “no, not acceptable,” for SD increase in X
“yes, acceptable” vs “no, not acceptable”	
Public servants (1 = yes)	−20.0%** (0.09)
Age 31+ (vs age 18–30)	−26.3%** (0.08)
Trust in colleagues	−9.8% (0.04)
Trust in others	−12.0%* (0.02)
“maybe, it depends” vs “no, not acceptable”	
Public servants (1 = yes)	1.3% (0.11)
Age 31+ (vs age 18–30)	1.9% (0.11)
Trust in colleagues	0.4% (0.05)
Trust in others	−11.8% (0.02)

\* $<0.01$ , \*\* $<0.001$ .

public servants are 20% less likely than private sector employees to find the vignette acceptable, as opposed to not acceptable. Respondents older than 30 years old are 26% less likely than respondents aged between 18 and 30 to find the vignette acceptable. Respondents that are more trusting of others are 12% less likely than less trusting respondents to find the vignette acceptable. In absolute terms, the largest effect size for predicting the lack of acceptance of cameras in the workplace is the respondent being in the older age cohort, followed by working in the public sector, both of which are consistent directionally with hypotheses H1 and H3. General trust, but not trust in one’s colleagues, is statistically significant at the 0.01 level from the analyses reported in Table 2.

Figure 2 illustrates the joint effect of being younger or older than 30 years old with being a private sector worker or a public servant, after controlling for one’s trust in colleagues and trust in others. It shows the marginal coefficients of a regression analysis. The so-called ambivalent respondents selecting the “It depends” answer are not systematically derived from particular age cohorts or sector of work. The results show, however, that public servants older than thirty-one are the ones most opposed to cameras at work, followed by older private sector workers,



**Figure 2.** Marginal effect of age and sector of employment on the agreement of camera work surveillance, holding trust in colleagues and others constant.

public servants younger than 31 years old, and lastly, younger private sector workers.

With the quantitative data parsed out statistically, the next section analyzes the open-ended comments from those who selected “It depends” in response to the workplace camera surveillance vignette. This allows for the exploration of the contextual elements that are important to those ambivalent Canadians regarding workplace camera surveillance. These represent the contextual elements that must be understood as part of an empirically-informed framework that can help evaluations of the reasonableness of workplace surveillance practices.

### **Qualitative analysis**

Based on Ravid et al.’s (2020) typology, in Table 3, we present the coded frequencies of comments provided by respondents who indicated in their response to the surveillance question that “It depends” in terms of the vignette scenario’s acceptability. The open-ended responses were all coded independently by two coders using Dedoose software according to Ravid et al.’s (2020) EPM typology. Any initial differences in coding were arbitrated by the authors to come to an agreement, which was required for 30 of 465 responses. In the paragraphs below, we identify and describe the most

**Table 3.** Ravid et al.'s (2020) Typology of Electronic Performance Monitoring (EPM) Characteristics, With Coded Responses from Open-Ended Field for Those Who Were Ambivalent About the Facial Recognition-Enabled Work Camera Scenario.

EMP element/Subelement	Categories	Comments			First-order codes (quotes with respondent ID)
		<i>n</i>	<i>Fq</i>		
Transparency	High	171	36.4%		"Transparent about possible uses." (# 291); "In any case, the important thing is to notify the employees because if it is not done, I am against it. Otherwise, for me, it's an invasion of privacy." (# 100); "If it was only used for security purposes." (# 97)
Transparency	Low	17	3.6%		"They shouldn't overuse and take advantage of the employees." (#381); "Reduce use after thief is caught." (#12)
Purpose	Administrative and safety	160	34.0%		"Only if it is used for the identity of crooks." (#5); "Usage should be restricted to evidence in event of a crime, not used for employee tracking." (# 207); "Cameras for the purpose of security is reasonable." (# 177)
Purpose	Surveillance and authoritarian	94	20.0%		"It depends. If they are using it for anything other than the security of the employees, then it seems that we should at least consent to it." (#430); "Long term retention is a significant issue and against current privacy regulations." (# 184); "In most cases, the invasion of privacy is too extreme" (# 486)
Purpose	Performance appraisal, loss prevention, and profit	26	5.5%		"Questionable for attendance and performance—what problems will this address?" (# 267); "I do not believe security and performance evaluations should be tied together" (# 409); "If it's used to analyze employee performance, then I'm totally against it" (# 6)
Purpose	Development, growth, and training	1	0.2%		"Sensory measures do not adequately inform personal process and productivity. Creativity cannot be measured or scripted on a person-to-person basis." (# 321)
Invasiveness /Target	Person and location	62	13.2%		"It depends on whether the security cameras are hidden or not." (# 355); "If the employed has to sign a confidentiality form, and where the cameras are placed." (# 187); "It depends on where the cameras are installed. In entrances, that would be completely okay" (# 14)
Invasiveness/Target	Task	9	1.9%		"If it is directed in such a way to monitor my keystrokes (passwords) or what I am working on, not acceptable." (# 251); "Using it to track performance feels uncomfortable and I think it infantilizes workers and shows distrust." (# 98); "I am being paid to work. My



Invasiveness/Target	Thoughts, feelings, and physiology	3	0.6%	<p>deliverables can be used to measure outcomes and performance. Let's not be afraid to have a face to face conversation, and lean on technology to 'prove' something about performance." (# 299)</p> <p>"I wouldn't appreciate not being trusted as an employee." (# 438);</p>
Invasiveness/Constraints	High	44	9.4%	"It requires a protocol of use and confidentiality that is quite limited." (# 551); "If they promised to only look at footage when something went wrong and not to spy." (# 159); "Once the thieves are identified, the footage must be destroyed and should not be kept on file for other uses." (# 517)
Invasiveness/Constraints	Low	11	2.3%	"If it's intended for one purpose, why should they have permission to use it for other purposes?" (# 569); I don't like the idea of being mechanically monitored. I'd rather be watched by my boss directly walking around. (# 379)
Invasiveness/Scope	Specificity	31	6.6%	"Cameras should only be installed on a temporary basis while the issue persists and cameras should only be in areas of comings and goings such as the entrances and elevators." (# 237); "I would not approve if I were a personal counselor and having a camera running with talking to a client." (# 412); "If it were in public areas such as cafeterias, or corridors, or anything like that, according to me it would be okay. But if they were in the washrooms, employees' offices, change rooms or something like that, it would be more of an invasion of privacy." (# 497)
Invasiveness/Scope	Breadth	12	2.6%	"It should be made known to the employees that there are surveillance cameras in order to foster trust." (# 494); "It's important that all employees know about the cameras and their locations." (# 141); "Where would the video be stored? Would staff be constantly surveilled, or would just common areas and exits be monitored?" (# 277)
Invasiveness/Target Control	Low	6	1.3%	"How the employer communicates the use of the technology is key to whether it is acceptable or not. In secret, it's not acceptable. If it's widely communicated, it's more acceptable." (#326)
Invasiveness/Target Control	High	4	0.9%	"All employees would need to consent to being videoed." (# 114)
Synchronicity/Collection	Low	36	7.7%	"If it is temporary then maybe, yes." (# 405); "I don't feel comfortable with it over the long term." (# 436)
Synchronicity/Collection	High	8	1.7%	"Use for the primary purpose of catching the theft seems reasonable, however ongoing surveillance seems intrusive and purposeless." (# 270)
Synchronicity/Feedback delivery	High	10	2.1%	

(continued)

Table 3. Continued.

EMP element/Subelement	Categories	Comments			First-order codes (quotes with respondent ID)
		n	Fq		
Synchronicity /Feedback delivery	Low	6	1.3%		"Once the culprit is caught, the footage should be destroyed." (#90); " Depends on how long the footage is actually stored, and the accountability of whether or not the true purpose of the technology is warped to benefit the employer and take advantage of employees." (# 48) "If they inform employees when they are tracking productivity, I would be more comfortable." (# 62)
Others	Vague	26	5.5%		"It would be acceptable on a case by case basis." (# 226); "It depends on the situation." (# 454)
Others	Theft	20	4.3%		"It depends on what was being stolen." (# 415); "If the theft is constant and the items stolen are highly valuable." (# 74)
Others	Work place	16	3.4%		"It depends on what job you are doing." (# 363); "Only in a high security environment; most workplaces are not." (# 512)
Others	People	14	3.0%		"Depends on who is doing it." (# 566); "It depends on if this is actively happening and who it will affect." (# 138); "It depends on the people involved on the evaluation." (# 533)
Others	Facial recognition	13	2.8%		"Security cameras are fine but without facial recognition" (# 145); "Each employee should be allowed to consent or not to the facial recognition program." (# 247.)
Others	Use and storage of data	13	2.8%		"It depends upon how long they want to use it for." (# 477); "It depends on what the purpose for keeping it after the theft has been stopped." (# 372)
Others	Previous measures	7	1.5%		"The employer would have to demonstrate that other steps have been taken and that they were unsuccessful." (# 8); "There are other means of security that can be used without the use of the same use of technology that is reserved for our highest levels of security." (# 295)
Others	Consent	2	0.4%		

"It depends because if they are using it to anything other than the security of the employees, then it seems that we should at least consent to it." (# 430)

> 10%	
5-10%	
2-5%	
< 2%	

n = 465 respondents who answered "It depends."

\*The % is greater than 100% because a code can be used more than once in a comment.

Purpose: The explicit or perceived rationale for EPM use

Invasiveness: The amount, target, and systematic constraints placed on EPM use

Synchronicity: The temporal aspects of EPM use, including frequency and regularity of monitoring

Transparency: The extent to which employees are provided information about the characteristics of monitoring

frequent themes from the responses and present representative excerpts from our respondents. This section is not focused on hypothesis-testing in the same way as the quantitative analysis, but rather on mapping our respondents onto Ravid et al.'s (2020) typology to ascertain which dimensions (and their relationships) emerge as most consequential to the ambivalent respondents. In this way it builds on Ravid et al. (2020) by differentiating the major characteristics of surveillance that are foundational to their ambivalence from the minor considerations.

The analysis of 465 comments from respondents reveals that the most frequently mentioned theme in Ravid et al.'s (2020) typology is *transparency—high* concerns (171 codes; 36% of comments). The main reservations among these respondents were associated with the lack of clarity on the terms of use of the data collected, as well as employee knowledge of the location of cameras. These comments highlight employees' demand for more specific knowledge of the use of the footage collected, what activities might be monitored through the location of the camera, and employee awareness of constraints on the use of the footage collected. A representative sample of the comments in this realm reveals these dimensions of concern:

There would need to be a fairly limited protocol for use and confidentiality. (Translated from French) (Public servant aged 31+)

If there is actually an issue and co-workers are aware of the facial recognition cameras, yes. Workers should be made aware about these cameras. (Private sector employee aged 31+)

I would need to know all the details for when and why the system would be recording, and in what location. (Public servant aged 31+)

There are noteworthy demographic dimensions associated with comments regarding transparency concerns. The percentage data presented in this section was normalized to weigh both age (18–30: 29%; 31+: 71% of total sample) and public/private sector employment groups (public sector: 34%; private sector: 66% of total sample) equally. Respondents aged 18–30 and 31+ years responded in roughly equal measure expressing overall (high *and* low) transparency concerns (59% and 41%, respectively). However, among respondents whose comments were coded for high levels of transparency concerns, the weighted majority were aged 18–30 years (62%). Similarly, among respondents whose comments were coded for low levels of transparency concerns, the weighted majority were aged 31 and over (76%). Yet similar levels of public servants and public sector employees reported high transparency concerns, while public sector employees expressed lower levels of concern for transparency issues than private sector employees.

For excerpts coded *transparency—high* (i.e., respondents indicating that high levels of transparency around the purpose and process of surveillance is important to them), the majority of respondents ( $n = 143/171$ , 84%) agreed with the use of surveillance cameras in the workplace under certain conditions. These conditions include use of surveillance cameras solely for the proposed scenario or for security purposes ( $n = 69$ , 48%) but not for other scenarios ( $n = 39$ , 27%). To many respondents ( $n = 82$ , 57%), acceptable use also requires constraints on the use of the data collected. However, even by adding these positive comments from ambiguous respondents to the 41% of total respondents who agree with workplace cameras, the majority of Canadian workers in our sample (46%) does not support workplace cameras in the manner described in the vignette.

The second most frequent type of comment in response to the scenario as categorized by Ravid et al.'s (2020) typology is related to *administrative and safety* concerns (160 codes; 34% of comments). Within this category, respondents typically suggested that video surveillance would be acceptable so long as it is used to prevent theft, other criminal acts, and freeloading by some employees. This is consistent with the literature above in both Canada and the United States that finds safety and theft prevention and detection are typically viewed as a legitimate use of cameras. The following representative comments indicate as much:

It's okay for security purposes, but to maintain it on file, no. (Private sector employee aged 31+)

It makes sense to protect other employees, but data can be collected on employees' other behaviours which is wrong. (Private sector employee aged 31+)

I think that the cameras to catch theft is okay, but to carry on beyond that is not OK. (Public servant aged 31+)

Of the 160 responses coded for *administrative and safety* concerns, both younger and older age groups (54% and 46% respectively) and public and private sector employment groups (45% and 55% respectively) expressed similar levels of concern. The third most frequent comment type from respondents is aligned with surveillance and authoritarian concerns in Ravid et al.'s (2020) typology (94 codes; 20% of comments). The specific comments in this realm are diverse, but they generally reflect employee concerns about employers' intentions in setting up and using surveillance systems in the workplace. In particular, employees can be suspicious of their employers' stated use for captured footage, as well as the invasion of privacy associated with constant surveillance. This is likewise consistent with findings in the literature that point to the purpose and motive of surveillance by employers as an important concern among employees. The following comments are representative of such concerns:

It should only be used to catch a thief, not for malign purposes. (Public servant aged 31+)

Is the need for security being used as an excuse for employee surveillance? (Public servant aged 31+)

I'm not sure I would want a camera looking at me all the time; Big Brother watching you all the time. (Private sector employee aged 31+)

Among the 94 respondents whose comments were coded for *surveillance and authoritarian* concerns, 61% were aged 18–30 years, while 39% were aged 31 years and over, indicating significantly higher levels of concerns related to employer surveillance and authoritarianism for younger workers. However, public and private sector employees' responses were coded in similar levels.

Of particular interest are 26 comments directly linked to performance appraisal. That is not a large proportion of comments (6% of total sample). However, the vignette mentioned only one purpose for the camera: to curb theft. The respondents who referred to performance in their comments did so thinking that the employer was less than forthcoming in their approach, and that curbing theft was an excuse to use the cameras to track performance.

I am being paid to work. My deliverables can be used to measure outcomes and performance. Let's not be afraid to have a face to face conversation, and lean on technology to "prove" something about performance. (Public servant aged 31+)

Only if it was just to make the place more secure or in fact would also be used for tracking purposes with respect to attendance and performance. (Public servant aged 31+)

This would be reasonable to identify theft. But would not be an accurate representation of employee and attendance and performance unless the job requires the employee to sit at a desk for a specified period of time each day. (Public servant aged 31+)

I do not believe security and performance evaluations should be tied together. (Public servant aged 31+)

It would be OK for theft/mischief, but from there to analyzing employee performance, well, I'm totally against that.... (Translated from French) (private sector employee aged 18–30)

A few respondents found that performance monitoring could be reasonable in certain conditions, like this private sector employee aged 18–30: "it depends on how transparent the company is with how they are using the data. If they inform employees when they are tracking productivity, I would be more comfortable." [Table 4](#) combines EPM subelements' coded responses to provide an overall snapshot of areas of concern for respondents, presented by age and employment sector groups.

**Table 4.** Areas of Concern for Respondents by Age and Employment Sector.

EPM element/ Subelement	Age (%)		Public servants (%)	Private sector workers (%)
	18–30	31+		
Purpose/Performance appraisal, loss prevention, and profit	31	69	89	11
Purpose/Development, growth, and training	100	0	100	0
Purpose/Administrative and safety	54	46	45	55
Purpose/Surveillance and authoritarian	61	39	54	46
Invasiveness /Scope	57	49	56	44
Invasiveness/Target	57	43	65	35
Invasiveness/Constraints	50	50	60	40
Invasiveness/Target Control	38	63	56	43
Synchronicity/Collection	31	69	55	45
Synchronicity/Feedback	52	47	31	69
Transparency	59	41	49	51

Note: The percentage values are normalized. Although some EMP elements demonstrate a very high percentage (notably development, growth, and training), these only incorporate a relatively small number of comments.

Finally, 111 coded sections that could not easily be accounted for in Ravid et al.'s (2020) typology were coded as “other.” These comments could not be coded often because they were too vague, or because they raised concerns not captured by the typology. Notably, within the “other” category, twenty comments highlighted concerns about the characteristics of the thefts used to justify installing cameras, such as if the items were highly valuable or thefts were constant. A further sixteen comments highlighted characteristics of the workplace in which the cameras were to be installed, such as the nature of the work and if there were particular privacy needs (e.g., a personal counselor). Thirteen respondents were concerned specifically about facial recognition as part of camera surveillance, and an additional thirteen comments highlighted issues with employers keeping surveillance data stored (e.g., its use afterwards, for how long it is kept, etc.).

## Discussion

In this study, we analyzed large representative samples of Canadians to explore their views on being filmed continuously at work. The American and Canadian panelists depart from each other in the aggregate, with the acceptability among Canadians less than that observed in Rainie and Duggan's (2016) U.S. sample. The quantitative results make it clear that younger employees in the public and private sectors are more tolerant of cameras in the workplace than those over age 30. That is especially true for those working in the private sector. This might reflect the slow erosions of expectations of privacy of new members of the workforce who have grown accustomed to being filmed while at work or broader trends in surveillance capitalism. Our qualitative insights derived from open-ended comments



among those with ambivalent attitudes toward camera surveillance allow us to present an original portrait of the contextual elements that are crucial for ambivalent Canadians' dispositions toward work surveillance via cameras.

These results are informative, as installing cameras at work for theft has been presented as a clear-cut justification in legal debates and disputes and judged nearly unambiguously as "reasonable." Further, all the other objectives beyond theft prevention tend to undermine support for the use of cameras among the ambivalent respondents, although private sector workers were slightly more tolerant of other objectives than public sector workers. Ultimately, there are a few signals we can read from the ambivalent respondents reported in [Table 3](#) above that might tell us what conditions or employer adaptations might generate majority support.

Ravid et al.'s (2020) typology highlights many concerns that are held by surveilled employees, and our data confirm the general suitability of the typology to a diverse Canadian empirical sample. We also found that among those who were ambivalent, when asked to explain why, most focused on concerns over transparency, safety, and authoritarianism in this scheme. The results from the "It depends" answer option (with open-ended comments) indicates that younger respondents make up the majority of the comments coded for high transparency concerns, as well as surveillance and authoritarianism concerns. So, while the results of the quantitative analyses indicate that younger employees accept cameras at higher rates, the qualitative data (those who lean to approve from among the ambivalent) make it clear that they do not so do unquestioningly, raising concerns about transparency and motives of employers. These results indicate that the typology, while a comprehensive framework for understanding electronic performance monitoring, has elements that are systematically of more paramount concern for employees than other elements of the typology, and some of these elements are conditional on the personal characteristics of the employee, such as age and level of trust.

Thus, it is important to note that while some categories of concern were mentioned with relatively high frequency, others received very few mentions among the ambivalent respondents. Overall, ten codes each made up less than five percent of total comments from our respondents. The least frequent comments in our sample overlaid onto Ravid et al. (2020) scheme are associated with "Development, growth and training" (i.e., Surveillance used for constructive feedback and skill acquisition), "Target control" (i.e., Do employees have some control over the timing of surveillance), "Feedback delivery" (i.e., Do employees hear about the results of monitoring). The low prevalence of these codes among respondents in our sample is as telling as the high prevalence of others.

For example, the low frequency of comments related to “Target control,” compared with the high frequency of comments associated with “Transparency,” indicates that employees surveilled may be more interested in knowing the parameters of the surveillance than being able to control them. This may be an implicit recognition of the right of the employer to surveil a workplace with a camera, but that it must come with full disclosure on the purpose of the monitoring and its intended use. The relative infrequency of comments associated with “Feedback delivery” as defined by Ravid et al. (2020) may, however, be more due to the nature of the scenario presented; cameras were presented less as a means of monitoring performance (although the vignette hinted at this possibility of use), and more as a means of providing security or preventing theft. Thus, assuming data would not be principally collected for performance evaluation, there would be no feedback. It is also likely a function of video camera data being ill-equipped alone to deduce performance metrics that can be used for feedback to employees. Similarly, the relative infrequency of the “Development, growth and training” category may also be due to the nature of the scenario presented, which did not appear focused on providing constructive feedback and skill acquisition. Lastly, facial recognition was front and center to our analysis, as it was mentioned in the short vignette. However, it rarely came out as an independent object of discussion in the comments of the ambivalent respondents.

The design and results of this study are responsive to the call from Ravid et al. (2020), who after their systematic review of the electronic performance monitoring literature, invited researchers to examine the interactive effects of surveillance practices with personal and contextual characteristics of employees. It also compares public and private sector employee’s calculus about privacy, one of Bhawe et al.’s (2020) suggestions for future research. This study contributes to that end in several ways. First, we have established that in our sample, there is an interactive effect of age and sector of work on one’s acceptance of this surveillance scenario but age is the larger driver. There is, it is important to note, evidence that public sector employees are less tolerant of such surveillance when other characteristics are controlled in the analysis. Second, we have been able to discern from open-ended responses among those struggling with whether the scenario is acceptable or not that they are most concerned about how the data is used, that it be used as a tool for safety (not performance evaluation), and that the clear intentions of the employer matter a great deal to them.

There are practical and analytical implications to these findings. The practical implications are that we are able to discern patterns in ambivalent employees’ responses to this scenario that are suggestive of relatively simple measures employers can take to satisfy employee concerns: be clear about

the purpose of the surveillance with employees, and make sure that the surveillance approach is logically related to its goal. That is, camera surveillance is generally a poor tool to evaluate performance alone, but employees feel it could reasonably serve administrative or safety objectives. Our analysis of the open-ended responses of the ambivalent respondents shows that the hint of using the camera footage for performance measurement was the major factor holding them back from finding it acceptable. The importance of clear communication that formally sets the boundaries on the use of the data or footage is reinforced in our findings. The risk of poor communication in this realm is that employees may assume the employer has a punitive objective (Tomczak et al., 2020). Future research about electronic performance monitoring and facial recognition research should ask employees if they are subjected to video surveillance in their work, as this might affect their beliefs of its broader acceptability. Another dimension of interest would be to factor in the complexity of one's job (Tomczak et al., 2020), and thus the limits of video surveillance, as a factor to disentangle from age.

The analytical implications from this study's findings point back to the Ravid et al. (2020) typology of electronic performance monitoring. This impressive theory-based typology sets forth the main characteristics we should consider when examining workplace surveillance practices, and now researchers must leverage this to generate and test hypotheses that account for these characteristics in relation to each other and the personal characteristics of the surveilled. The totality of our quantitative and qualitative evidence suggests, for example, that certain concerns, such as transparency on the use of the data, is conditional on age, but not especially strongly by sector of work. There are many more angles to explore through the use of experimental vignettes to test the effects of various characteristics in relation to each other, such as highly invasive but lowly synchronous surveillance versus highly transparent surveillance but lowly constrained use of data across various types of performance monitoring. Thus, there are ample opportunities to leverage this typology to make more sophisticated theoretical statements and empirical examinations regarding various methods of workplace surveillance.

## Conclusion

In a piece titled "Law and Public Administration: A Love–Hate Relationship?," Dragos and Langbroek (2018) commented that typically,

Managers in public administration focus on cost reduction, externalities, political feasibility, performance, and more flexibility in the implementation of regulations. Administrative law from that perspective means limitations as to the freedom of the administration to make choices and this eventually leads to slower responses to societal problems. (Dragos & Langbroek, 2018, pp. 1068–1069).

In the analyses we presented, we find the opposite. Case law in Anglo-American contexts is fairly permissive of video surveillance at work. A Canadian court decision from 1974 explicitly mentioned the “real and substantial suspicion that an individual is guilty of theft” as an exception for work surveillance not covered by a collective agreement (Khullar, 2011, p. 382). A more recent case was settled by the Office of the Privacy Commissioner of Canada (2015) where the plaintiff in an unnamed federal government agency alleged that a video surveillance camera was pointed toward her work area without being informed of the installation or purpose; the employer said that the camera was placed overtly, and that “the purpose of the surveillance cameras in its facilities was to deter theft and property damage and promote employee safety, but not to monitor employee performance” (Office of the Privacy Commissioner of Canada, 2015). Thus, courts and administrative tribunals have reinforced the “threat of theft” exception to broad-based camera surveillance in the public sector workplace in Canada.

Furthermore, there are yet to be litigated cases where public or private sector employees are surveilled at work with facial recognition-enabled cameras, a game-changing technology in terms of surveillance’s capabilities. The first Supreme Court case in Canada about surveillance in particular was *R v. Wong* [1990]. The court decided that the appropriate test should not be based on specific technologies but whether a person had a “reasonable expectation of privacy” in a particular context. In that vein, what the court suggested is another standard for privacy: what people might expect in a “free and democratic society” (Bennett & Bayley, 2005, p. 67). That implies a crucial role for public opinion in determining a reasonable expectation of privacy.

The empirical measurement from a representative sample of a large population offers solid parameters from which to engage in evidence-based analysis. This type of evidence is critical not only for future court and arbitration proceedings, but also for future negotiations between HR teams and public service associations to fine-tune their work surveillance policies to include an empirically-informed picture of prevailing views of reasonableness. The majority views may not be determinative on judgements on these questions, but it is clear that courts are increasingly interested in evaluating the evolving expectations of privacy in free and democratic societies.

A steady stream of Personal Information Protection and Electronic Documents Act (PIPEDA) related complaints related to work camera surveillance has been received by the Office of the Privacy Commissioner of Canada since the law was enacted in 2000,<sup>1</sup> signaling a sustained discomfort among some with the state of video surveillance in the workplace. Before and after the Clearview AI scandal in 2020, a handful of cities, mostly in the United States, and the State of California, put forward partial

bans on the use of facial recognition by their police departments, and sometimes by any other government services. Some advocacy groups, like the Electronic Frontier Foundation, call for total bans for government facial recognition, but not for its use by private firms and individuals (Schartz & Sheard, 2021). Some police departments like the New Orleans police department and the Norfolk police department lied or hid the use of facial recognition from their elected officials. In popular media and in the academic literature, there are few discussions about the use of facial recognition outside of airports and police forces.

Government surveillance can be directed at citizens but also at its own employees. As observed in this study, the median Canadian worker does not clearly agree with the legal terrain shaping their workplace, and thus delimiting the contours of what surveillance practices enjoy greater support becomes important for HR departments and unions negotiating the implementations of cameras at work in Canada and abroad. Our quantitative and qualitative empirical analyses from large representative samples enable us to draw the jagged line of what practices are consistent with broadly acceptable understandings of reasonable expectations of privacy as it relates to facial-recognition-enabled camera surveillance at work.

## Note

<sup>1</sup>Among them are PIPEDA Cases #2003-114, #2004-264, #2004-265, #2004-273, #2004-279, #2005-290, #2009-001, #2010-008.

## Acknowledgments

The authors would like to thank the members of the *Canadian Public Sector Research Panel* for their participation in this study.

## Notes on contributor

Carey Doberstein is an Associate Professor of Political Science at the University of British Columbia in Vancouver, Canada. Étienne Charbonneau is the Canada Research Chair in Comparative Public Management at École nationale d'administration publique in Montreal, Canada. Geneviève Morin is a graduate student at École nationale d'administration publique in Montreal, Canada. Sarah Despatie is a graduate student in the Department of Political Science at the University of British Columbia in Vancouver, Canada.

## ORCID

Carey Doberstein  <http://orcid.org/0000-0001-5106-8484>

## References

- Anteby, M., & Chan, C. K. (2018). A self-fulfilling cycle of coercive surveillance: Workers' invisibility practices and managerial justification. *Organization Science*, 29(2), 247–263.
- American Management Association. (2007). *Electronic Monitoring & Surveillance Survey*. EPolicy Institute. <http://www.epolicyinstitute.com/2007-electronic-monitoring-surveillance-survey-article>.
- Bennett, C. J., & Bayley, R. M. (2005). Video surveillance and privacy protection law in Canada. In S. Nouwt, B. R. de Vries, & C. Prins (Eds.), *Reasonable expectations of privacy? – Eleven country reports on camera surveillance and workplace privacy* (pp. 61–89). T.M.C. Asser Press.
- Bhave, D. P., Teo, L. H., & Dalal, R. S. (2020). Privacy at work: A review and a research agenda for a contested terrain. *Journal of Management*, 46(1), 127–164. <https://doi.org/10.1177/0149206319878254>
- Boivin, R., & Cordeau, G. (2017). Do Web surveys facilitate reporting less favourable opinions about law enforcement? *Security Journal*, 30(2), 335–348.
- Botan, C., & Vorvoreanu, M. (2005). What do employees think about electronic surveillance at work? In *Electronic monitoring in the workplace: Controversies and solutions* (pp. 123–145). IGI Global.
- Boyne, G. A. (2002). Public and private management: What's the difference? *Journal of Management Studies*, 39(1), 97–122. <https://doi.org/10.1111/1467-6486.00284>
- Bullock, J. B. (2019). Artificial intelligence, Discretion, and bureaucracy. *The American Review of Public Administration*, 49(7), 751–761. <https://doi.org/10.1177/0275074019856123>
- Busuioc, M. (forthcoming). *Accountable artificial intelligence: Holding algorithms to account* (pp. 1–12). *Public Administration Review*.
- Chan, J. (2008). The lateral surveillance and a culture of suspicion. In M. Deflem (Ed.), *Surveillance and governance: Crime control and beyond* (pp. 223–239). Emerald Group Publishing Limited.
- Chandra, S., Shirish, A., & Srivastava, S. C. (2020). Theorizing technological spatial intrusion for ICT enabled employee innovation: The mediating role of perceived usefulness. *Technological Forecasting & Social Change*, 161, 1–15.
- Chao, B., Durso, C., Farrell, I., & Robertson, C. (2018). Why courts fail to protect privacy: Race, age, bias, and technology. *California Law Review*, 106(2), 263–324.
- Charbonneau, É., & Doberstein, C. (2020). An empirical assessment of the intrusiveness and reasonableness of emerging work surveillance technologies in the public sector. *Public Administration Review*, 80(5), 780–791. <https://doi.org/10.1111/puar.13278>
- Christ, M. H., Sedatole, K. L., Towry, K. L., & Thomas, M. A. (2008). When formal controls undermine trust and cooperation. *Strategic Finance*, 89(7), 39.
- Ciocchetti, C. A. (2011). The eavesdropping employer: A twenty-first century framework for employee monitoring. *American Business Law Journal*, 48(2), 285–369. <https://doi.org/10.1111/j.1744-1714.2011.01116.x>
- Dragos, D. C., & Langbroek, P. M. (2018). Law and public administration: A love-hate relationship? In: *The Palgrave Handbook of Public Administration and Management in Europe* (pp. 1067–1085). London, UK: Palgrave Macmillan.
- Ferguson, A. G. (2017). *The rise of big data policing: Surveillance, race, and the future of law enforcement*. New York University Press.

- Fusi, F., & Feeney, M. K. (2018). Electronic monitoring in public organizations: Evidence from US local governments. *Public Management Review*, 20(10), 1465–1489. <https://doi.org/10.1080/14719037.2017.1400584>
- Griffith, T. L. (1993). Monitoring and performance: A comparison of computer and supervisor monitoring. *Journal of Applied Social Psychology*, 23(7), 549–572. <https://doi.org/10.1111/j.1559-1816.1993.tb01103.x>
- Hagen, C. S., Bighash, L., Hollingshead, A. B., Shaikh, S. J., & Alexander, K. S. (2018). Why are you watching? Video surveillance in organizations. *Corporate Communications: An International Journal*, 23(2), 274–291. <https://doi.org/10.1108/CCIJ-04-2017-0043>
- Henman, P. (2020). Improving public services using artificial intelligence: Possibilities, pitfalls, governance. *Asia Pacific Journal of Public Administration*, 42(4), 209–221. <https://doi.org/10.1080/23276665.2020.1816188>
- Herian, M. N., & Tomkins, A. J. (2012). Citizen satisfaction survey data: a mode comparison of the derived importance–performance approach. *The American Review of Public Administration*, 42(1), 66–86.
- Kääriäinen, J., & Sirén, R. (2012). Do the police trust in citizens? European comparisons. *European Journal of Criminology*, 9(3), 276–289. <https://doi.org/10.1177/1477370811435737>
- Kayas, O. G., Hines, T., McLean, R., & Wright, G. H. (2019). Resisting government rendered surveillance in a local authority. *Public Management Review*, 21(8), 1170–1190. <https://doi.org/10.1080/14719037.2018.1544661>
- Khullar, R. (2011). Influence of oakes outside the charter, specifically labour arbitration jurisprudence. *Ottawa Law Review*, 43(3), 377–394.
- Kugler, M. B., & Strahilevitz, L. J. (2016). Actual expectations of privacy, fourth amendment doctrine, and the mosaic theory. *The Supreme Court Review*, 2015(1), 205–263. <https://doi.org/10.1086/686204>
- Leman-Langlois, S. (2009). Public perceptions of camera surveillance. In W. Deisman (Ed.), *A report on camera surveillance in Canada: Part one* (pp. 41–58). Queens' University.
- Lyon, D. (2018). *The culture of surveillance*. Polity Press.
- Mirowsky, J., & Ross, C. (2006). Social structure and psychological functioning: Distress, perceived control, and trust. In J DeLamater (Ed.), *Handbook of social psychology* (pp. 411–447). Springer.
- Mutz, D. C. (2011). *Population-based survey experiments*. Princeton University Press.
- Nebeker, D. M., & Tatum, B. C. (1993). The effects of computer monitoring, standards, and rewards on work performance, job satisfaction, and stress. *Journal of Applied Social Psychology*, 23(7), 508–536.
- Nunn, S. (2004). Thinking the inevitable: Suicide attacks in America and the design of effective public safety policies. *Journal of Homeland Security and Emergency Management*, 1(4), 1–21. [Database] <https://doi.org/10.2202/1547-7355.1063>
- Office of the Privacy Commissioner of Canada. (2015). *Employers subject to PIPEDA should inform employees about the existence of, and purpose for, video surveillance in the workplace*. Settled case summary #2015-001.
- Oz, E., Glass, R., & Behling, R. (1999). Electronic workplace monitoring: What employees think. *Omega*, 27(2), 167–177. [https://doi.org/10.1016/S0305-0483\(98\)00037-1](https://doi.org/10.1016/S0305-0483(98)00037-1)
- Perry-Hazan, L., & Birnhack, M. (2019). Caught on camera: Teachers' surveillance in schools. *Teaching and Teacher Education*, 78(1), 193–204. <https://doi.org/10.1016/j.tate.2018.11.021>
- Rainie, L., & Duggan, M. (2016). *Privacy and information sharing*. Pew Research Center.



- Ravid, D. M., Tomczak, D. L., White, J. C., & Behrend, T. S. (2020). EPM 20/20: A review, framework, and research agenda for electronic performance monitoring. *Journal of Management*, 46(1), 100–126. <https://doi.org/10.1177/0149206319869435>
- Rooks, G., Raub, W., Selten, R., & Tazelaar, F. (2000). How inter-firm co-operation depends on social embeddedness: A vignette study. *Acta Sociologica*, 43(2), 123–137. <https://doi.org/10.1177/000169930004300203>
- Samaranayake, V., & Gamage, C. (2012). Employee perception towards electronic monitoring at work place and its impact on job satisfaction of software professionals in Sri Lanka. *Telematics and Informatics*, 29(2), 233–244. <https://doi.org/10.1016/j.tele.2011.08.003>
- Schartz, A., & Sheard, N. (2021). *Why EFF doesn't support bans on private use of face recognition*. Electronic Frontier Foundation.
- Tomczak, D. L., Behrend, T. S., Willford, J. C., & Jimenez, W. P. (2020). I didn't agree to these terms: Electronic performance monitoring violates the psychological contract. *Society for the Improvement of Psychological Science (SIPS) & the Center for Open Science (COS)*, 1–37. <https://doi.org/10.31234/osf.io/qax9u>
- Van de Walle, S., & Lahat, L. (2017). Do public officials trust citizens? A welfare state perspective. *Social Policy & Administration*, 51(7), 1450–1469. <https://doi.org/10.1111/spol.12234>
- White, M. D., & Malm, A. (2020). *Cops, cameras, and crisis: The potential and the perils of police body-worn cameras*. NYU Press.
- Wirtz, B. W., Weyerer, J. C., & Sturm, B. J. (2020). The dark sides of artificial intelligence: An integrated AI governance framework for public administration. *International Journal of Public Administration*, 43(9), 818–829. <https://doi.org/10.1080/01900692.2020.1749851>
- Yin, H., Biao, L., John, C.-K., Jin, Y.-L., & Zhang, Z.-H. (2013). The effect of trust on teacher empowerment: The mediation of teacher efficacy. *Educational Studies*, 39(1), 13–28. <https://doi.org/10.1080/03055698.2012.666339>
- Young, K. (2010). Policies and procedures to manage employee Internet abuse. *Computers in Human Behavior*, 26(6), 1467–1471. <https://doi.org/10.1016/j.chb.2010.04.025>

Copyright of Public Performance & Management Review is the property of Taylor & Francis Ltd and its content may not be copied or emailed to multiple sites or posted to a listserv without the copyright holder's express written permission. However, users may print, download, or email articles for individual use.