Stark Luke (Orcid ID: 0000-0002-2537-846X)

Title

"I don't want someone to watch me while I'm working": Gendered views of facial recognition technology in workplace surveillance

Luke Stark (Corresponding Author)
Microsoft Research Montreal
2000 McGill College Avenue, Suite #550
Montreal, QC H3A3H3
438-521-6021
luke.stark@microsoft.com

Amanda Stanhaus
University of Michigan School of Public Health
1415 Washington Heights
Ann Arbor, MI 48109-2029
(734) 764-5425
stanhaus@umich.edu

Denise L. Anthony
University of Michigan School of Public Health
1415 Washington Heights
Ann Arbor, MI 48109-2029
(734) 764-5425
deniseum@umich.edu

This is the author manuscript accepted for publication and has undergone full peer review but has not been through the copyediting, typesetting, pagination and proofreading process, which may lead to differences between this version and the Version of Record. Please cite this article as doi: 10.1002/asi.24342

Abstract
Employers are increasingly using information and communication technologies to monitor employees. Such workplace surveillance is extensive in the United States, but its experience and potential consequences differs across groups based on gender. We thus seek to identify whether self-reported male and female employees differ in the extent to which they find the use of workplace cameras equipped with facial recognition technology (FRT) acceptable, and examine the role of privacy attitudes more generally in mediating views on workplace surveillance.[1] Using data from a nationally representative survey conducted by the Pew Research Center (Madden & Rainie, 2015), we find that women are much less likely than men to approve of the use of cameras using FRT in the workplace. We then further explore whether men and women think differently about privacy, and if perceptions of privacy moderate the relationship between gender and approval of workplace surveillance. Finally, we consider the implications of these findings for privacy and surveillance via embedded technologies, and how the consequences of surveillance and technologies like FRT may be gendered.

Introduction
Surveillance by powerful actors in society, whether these are religious institutions, governments, or corporations, has a lengthy history (Beniger, 1989; Haggerty & Ericson, 2000; Igo, 2018; Lyon, 1994; Rule, 1973; Yates, 1993; Zuboff, 1988; 2019). Nonetheless, new information and communication technologies (ICTs) and their increasing saturation throughout societies around the world enable increasingly granular surveillance of an ever-expanding roster of groups, activities and spaces (Angwin, 2010; Etzioni, 1999; Lyon, 2014; Nissenbaum, 2010). From the use of cameras deployed across nearly every major street in the United Kingdom and the increasing use of facial recognition software by law enforcement (Barrett, 2013; Harmon 2019; McCahill & Norris, 2003), to the massive digital surveillance apparatus of governments (Gellman & Poitras, 2013; Greenwald, 2013; Mozur, 2019), to the increasingly recognized surveillance activities of private technology companies (Fowler, 2019; Kwet, 2019; Singer, 2019; Zuboff, 2019), nearly every person today experiences some form of surveillance in their daily lives.

Surveillance is a key tool for the exercise of power through what Anderson (2015) terms the "private government" of enterprises, and is long-standing (Ball, 2010; Stark & Levy, 2018; Zuboff, 1988, 2019), already vast (Ajunwa, Crawford, & Schultz, 2017). Early industrialists used clocks (Thompson, 1967), automation and other management tools (Simon, 1965; Taylor, 1911), and eventually digital information technologies to control workers' time and effort (Beniger, 1989; Stanton and Stam, 2003; Yates, 1993). Employers today are increasingly using new

[1] We recognize evaluations based on a binary definition of gender are invariably partial and exclusionary. As we note in our discussion of the study's limitations, we were constrained by the survey categories provided by Pew.

technologies to monitor employees via facial analytics, workstation screenshots, email and keystroke analysis, and monitoring online behavior (e.g., Solon, 2017). It has been estimated that nearly seventy-five percent of US companies monitor worker communications and on-the-job activities, and that 27 million online employees are monitored worldwide (Ball, 2010).

Workplace surveillance is often justified on grounds of productivity (Attewell, 1987; Ball, 2010), or safety and security (Ball & Webster, 2003; Zuriek, 2003). Regardless of these possibly positive effects however, workplace surveillance has other unintended impacts as well, such as increased job dissatisfaction and turnover, active resistance and even retaliation from workers (Anteby, 2018; Burawoy, 1979; Bernstein, 2012; Sewell, Barker, and Nyberg, 2012; Stanton & Stam, 2006). The effects of surveillance are often asymmetric across individuals or groups: surveillance is not directed or experienced in the same way by all (Anthony et al., 2017; Browne 2015; Levy & Barocas, 2018; Stark, 2016). In this way, surveillance activities are not only built on power differences in the workplace (Lyon, 2007; Zureik, 2003), but can and often do amplify extant social inequalities around race, class, and gender (Brayne, 2014; Browne, 2015; Conrad, 2009; Koskela, 2003). Monahan (2009) argues that in social contexts already marked by sexist and racist power relations, surveillance technologies tend to increase gender and racial inequality. For example, women in public and private spaces are increasingly scrutinized by technologies like cameras without necessarily achieving any additional protection from harassment or assault (Egan, 2004; Koskela, 2000; 2003). The cameras may see everyone, but the people who monitor the camera feeds watch selectively (Browne, 2015; Goold, 2004; Egan, 2004). In the case of biometric technologies such as FRT (Magnet, 2011; Gates, 2011), both gender and racial bias are encoded in the software (Buolamwini and Gebru, 2018; Scheuerman et al., 2019): training these systems on biased data gathered from unequal social contexts entrenches existing forms of discrimination (Browne, 2015), and the nature of the physiological classifications these systems produce inclines them towards the production of sexist and racist hierarchies (Keyes, 2018; Stark, 2019).

Research indicates that men and women think differently about surveillance technologies (Ball, Daniel, & Stride, 2012; Friedman et al., 2008). Yet there is still a need for more research on the impact of surveillance technologies across groups, as well as how marginalized and lower status groups in particular feel about, and respond to, the implementation of these technologies (Wu et al., 2019). Here we seek to identify whether men and women have different attitudes toward workplace surveillance using data from a nationally representative survey conducted by the Pew Research Center (Rainie & Duggan, 2015). The survey asks respondents about the acceptability of camera surveillance using FRT in the workplace. We conduct multivariate regression analysis to identify whether (self-identified) male and (self-identified) female employees say that the use of such FRT-enabled workplace cameras is acceptable (in response to theft in the workplace – a specific scenario we discuss in more detail below), controlling for other socio-demographic characteristics. We find that women are significantly less likely than men to approve of the use of cameras in the workplace. We then further explore whether men and women think differently

about various ways of defining privacy, and whether these privacy attitudes mediate views of camera surveillance. We supplement our quantitative analysis by leveraging Nissenbaum's (2010) Contextual Integrity (CI) framework to perform thematic coding of the qualitative responses collected in the survey. Finally, we consider the implications of these findings for privacy and surveillance more broadly, and how the consequences of embedded technologies, especially in contexts of power inequality, may be gendered.

Background: Surveillance in Workplaces

In the workplace, surveillance stem's from the employer's "ability to monitor, record and track employee performance, behaviors and personal characteristics," sometimes in real time (Ball, 2010). Histories of early large-scale organizations emphasize how the development of "information systems" gave firms the ability to police their internal structures (Beniger, 1989; Yates, 1993), typically justified in the name of productivity and quality control (Attewell, 1987). Any technology that makes monitoring and communication more efficient facilitates surveillance (Rule, 1973), and ICTs enable surveillance activities to expand the extent of monitoring, to new spaces, new activities, new groups, and new types of information, including in the workplace (Haggerty & Ericson, 2000; Lyon, 1994; Ullmann-Margalit, 2008; Zureik, 2007). ICTs not only increase the channels through which surveillance can take place, but also its extent and pervasiveness (Levy & Barocas, 2018; Rosenblat, Kneese, & boyd, 2014; Zureik, 2003), enhancing the capacities of employers to oversee and shape everyday work practices (Lee et al., 2015; Rosenblat & Stark, 2016). American workplaces, long sites of what Yates (1993) terms "control through communication," are now an epicenter for surveillance via cameras, FRTs, and other forms of electronic mediation such as keystroke monitoring (Lohr, 2014). Moreover, FRT is increasingly being deployed as part of the hiring process itself: firms such as HireVue have incorporated FRT into automated hiring questionnaires purportedly assessing everything from candidate body language to emotional expression (Ajunwa & Greene, 2019). Excessive monitoring can be detrimental to employees for a number of reasons—not least because personal privacy can be compromised if employees do not authorize disclosure.

Excessive monitoring can also be detrimental to employees because such surveillance technologies can exhibit 'function creep.' Monitoring technologies can sometimes yield more information than intended, and management often finds it challenging to avoid the temptation to extend monitoring practices without consulting employees first (Zureik, 2003; Zimmer, 2007; Lyon, 2014). This can produce 'anticipatory conformity,' whereby employees change their behavior to comply with perceived rules (Ball, 2010, p. 98). In his study of TSA employees, Anteby (2018) found that the more employees were watched, the harder they tried to avoid being watched, and the harder management tried in turn to watch them. Workers in such environments not only lose trust in their employers (Levy, 2015), but also are also more likely to experience stress and job dissatisfaction (Stanton & Stam, 2006). Employers with disgruntled workers who

perceive violations of their own privacy can see increased turnover and even retaliation (Stanton & Stam, 2006).

Gender and Surveillance

Though many types of workplaces are surveilled (e.g., Anteby, 2018; Levy, 2015), some industries and particular types of workers are more often subject to surveillance. The retail sector, made up of historically low-wage workplaces in which high proportions of minority and female workers are employed (Ruetschlin & Asante-Muhammad, 2015), is also a site of significant surveillance (Bernstein, 2017; Levy & Barocas, 2018; Zuboff, 1988). Similarly, video and other surveillance technologies are often used to control the appearance and behavior of waitresses, especially those in hyper-hetero-sexualized spaces such as casinos and strip clubs (Bayard de Volo, 2003; Egan, 2004). Hospital administrators have increasingly used technologies like RFID tags to track not only use of hospital equipment, but also the personnel who use such equipment, e.g., nurses (Fisher & Monahan, 2008; Timmons, 2003). Technologies for enabling employers to find nannies can end up exacerbating the inequalities of power and controlled experienced by these workers (Ticona & Mateescu, 2018), part of a broader trend towards lateral surveillance by consumers at home and at work (Andrejevic, 2006; Stark and Levy, 2018). Finally, surveillance is exacerbated not only by digital technologies, but also by new genres of employment, e.g., Uber/Lyft drivers (Rosenblat, Kneese & boyd, 2014; Rosenblat & Stark, 2016; Rosenblat, 2019) and other precarious workplaces in the "gig" or "on-demand" economy (Zuboff, 2019).

Historically, women have expressed concerns about privacy differing from mainstream, often masculine-dominated opinion. Sarah Igo notes observes that in nineteenth-century America, the privacy of the family sphere, "offered women too much of the wrong kinds of privacy," because such privacy protections privileged men as the head of the household (Igo, 2018, p. 23). As the jurisprudence around privacy emerged and changed over this period, women were more likely to be plaintiffs in privacy cases than in any other type (Lake, 2016). Today, women are still more likely to be subjects to unwanted attention (Allen, 1988; MacKinnon, 1979; 2005; Martin, 2016; Ortiz & Roscigno, 2016; Zerubavel, 2006). Indeed, though minority and low-income women are most likely to experience harassment (Adib & Guerrier, 2003; Berdahl & Moore, 2006), women at all levels of power in work organizations are likely to experience at least some harassment at work (McLaughlin, Uggen, & Blackstone, 2012). Research on gender and power suggests that men and women may think differently about surveillance, particularly in the workplace. For example, Ball et al. (2012) found that privacy perceptions among call center workers were gendered: women respondents complained of excessive or intrusive forms of personal information collection, such as via email and CCTV camera monitoring. Similarly, in ethnographic observations and interviews in a workplace moving to an open-plan office space, Hirst and Schwabenland (2017) found that workers were more aware of their visibility to senior management, and that women in particular `felt anxious about the idea of being constantly

watched.' Monahan (2009) argues that surveillance systems operate via logics of disembodied control at a distance, which have gendered implications for embodied actors.

Given the extent of workplace surveillance in the United States, as well as the potential differential experience and consequences of surveillance across groups based on gender, we seek to identify whether self-identified male and female employees differ in the extent to which they find the use of workplace cameras equipped with FRT acceptable. In addition, we examine the role of privacy attitudes more generally in mediating views on workplace surveillance.

Materials & Methods

We use data from a Pew Research Center survey conducted between January 27 and February 16, 2015, of a sample of 461 U.S. adults ages 18 or older, drawn from the GfK Group KnowledgePanel, a nationally representative online research panel (for more details on the study design, sample and overall results, see Rainie and Duggan (2015)). The survey asked respondents about privacy tradeoffs related to new technologies, including whether use of technology would be acceptable or not in seven different scenarios. Here we analyze the responses to one of those scenarios, whether an employer's use of camera surveillance with facial recognition software is acceptable in the workplace (coded as 1) or not (coded as 0, including responses of "it depends"). The full scenario presented in the survey states:

> 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 (Rainie & Duggan 2015, p. 14)

One important feature of the scenario is that it describes a specific reason for the surveillance, identifying perpetrators of theft, though it also notes that the company can ultimately decide to do whatever it wants with the data, including retain it for as long as it chooses. Although most people resent privacy violations (Nippert-Eng, 2010; Stark, 2016), and often resist surveillance (Marx, 2003; 2009), people are generally more accepting of monitoring that promises to increase security or appears to target "others" like terrorists or criminals (Brooks & Manza, 2013; Goold, 2004). Framing a question about surveillance in the workplace as a response to *theft* may increase the likelihood that respondents find it acceptable, despite the note that it would be retained by the employer and could be used for other types of monitoring. However, the increased likelihood toward acceptability should not differ between men and women.

We restrict our analysis to the subset of respondents who were employed at the time of the survey and who provided complete data on all variables (n=257). In addition to the scenarios, the survey asked about more general perceptions of privacy (see Table 1). For each of the nine statements (randomized order across respondents), we recoded the response categories so that responses of "very important" are coded as 1, and all others (somewhat important, not very

important and not at all important) are coded as 0. Our multivariate models also control for socio-demographic information, including age, education, income, race/ethnicity, and marital status (see Table 2, described below). We also include measures for general familiarity with technology, based on use (using a smartphone) and self-perceived knowledge (i.e., whether the respondent felt confident making decisions about information sharing in the past month).

Table 1. Privacy Perceptions

Variable	Statement
Privacy Perceptions: Responses coded as 1=very important, 0=somewhat important, not very important, not at all important	Introduction: "Privacy means different things to different people today. In thinking about all of your daily interactions – both online and offline – please tell me how important each of the following are to you."
	Being in control of who can get information about you
	Not having someone watch you or listen to you without your permission
	Controlling what information is collected about you
	Having individuals in social and work situations not ask you things that are highly personal
	Being able to have times when you are completely alone, away from anyone else
	Being able to share confidential matters with someone you trust
	Not being monitored at work
	Not being disturbed at home
	Being able to go around in public without always being identified

Source: Pew Research Center, Internet Survey Privacy #4: http://www.pewinternet.org/2016/01/14/privacy-and-information-sharing/

We use bivariate ANOVA and multivariate logistic regression analyses in STATA 15 to identify whether self-reported male and female respondents differ in finding workplace surveillance via cameras with facial recognition software acceptable or not. In addition, we examine gender differences in perceptions of privacy (Table 1) and then determine whether such attitudes moderate gender differences in the acceptability of workplace camera surveillance. We conducted the study using weighted models (to make estimates representative of the national adult population) and present results using weighted population estimates.

To supplement the quantitative analysis, we also perform thematic coding of the qualitative responses from the respondents who said workplace surveillance via cameras with facial recognition software was unacceptable. All who said it was unacceptable were asked an open-ended question of "why" (respondents who said surveillance *was* acceptable were not asked follow-up questions). A total of 81 percent of those who said workplace camera surveillance was unacceptable gave an open-ended response (89/110). We thematically code all qualitative responses from respondents into categories consistent with Nissenbaum's Contextual Integrity framework (Nissenbaum, 2010; 2011), and then compare the elements and proportions of responses in each between men and women.

Nissenbaum's Contextual Integrity framework (Nissenbaum, 2010; 2011) defines privacy as the appropriate flow of information (often digital data) within a given social context (Nissenbaum, 2015), and indicates that appropriateness is related to 5 factors: data subjects, data senders, data receivers, transmission principles, and data types. Given that the data subjects (respondents/employees) are the same as the data senders in the scenario examined here, we collapse those two categories. In addition, these categories are not mutually exclusive, so respondent statements could be coded with more than one category. The data subject/sender category includes references to concern about the subject of the surveillance, including the respondent specifically (e.g., "I" statements) or to employees in general, as well as to relationships among employees. For example, responses coded as data subject/sender include, "I do not like being recorded or constantly watched," and "I work with people I highly trust." The data recipient category includes references to employers specifically, including bosses and managers, as well as to unspecified recipients who might have access to the data. For example, statements like, "I do not want my boss watching me at all times" and "it is very uncomfortable to feel that people are or can watch your every move" were coded as data recipient. Note that both of these are also coded as data subject since they say something about how the respondent feels about being the subject of the surveillance. An example of a statement coded as data recipient but not data subject is, "big brother is watching." Responses coded as data type/purpose include any reference to the type of information collected (including based on where the cameras are located) or the purpose of the data, including the potential purpose for which it could be used. For example statements like, "It depends on where the cameras were," "Over intrusive in terms of capturing everyone's facial recognition," and "As long as they don't use the footage for any other purpose" were coded as data type/purpose. Finally, responses coded as data transmission principles are those that reference policies to govern the data capture or information retention, or to surveillance concerns more generally, and include statements such as, "I don't want the info about me retained indefinitely," "How secure is the storage of the footage," and "too invasive." Responses that did not fit into any of the contextual integrity categories were those that offered alternative actions to thwart theft in the workplace, such as "Rather just have lockable space for personal belongings" and "I don't think it's needed to prevent theft." Only 10 of 89 responses could not be coded into contextual integrity categories.

Results

Table 2 shows the descriptive statistics (unweighted) of all variables in the models for the sample of employed respondents. Overall, just over half of respondents say that workplace surveillance via cameras with facial recognition software, in response to recent theft, is acceptable. Slightly less than half of the sample are (self-identified) female. Almost 20 percent of the sample is under the age of 30, less than one-third are between 30 and 44 years of age, one-third are between 45 and 59 years of age, and about 13 percent are over the age of 60. About one-quarter of the sample has a high school education or less, while 44 percent has at least a bachelor's degree. Almost one-third of the sample has an income of $49,999 or less, one-third has income between $50,000 and $99,999, and about one-third has annual income of $100,000 or more. About 75 percent of the sample is white non-Hispanic and over half are married. Most (79%) have a smart phone, and nearly half reported feeling confident in the past month when making decisions about sharing personal information with companies.

Table 2. Unweighted Descriptive Statistics for Employed Respondents, N=257

Variable	%
Workplace camera surveillance is acceptable	58.2
GENDER	
Female	44.2
AGE	
18 – 29 years	19.3
30 – 44 years	31.3
45 – 59 years	35.9
60+ years	13.6
EDUCATION	
High school or less	26.0
Some college	29.8
Bachelor's degree or higher	44.2

ANNUAL INCOME	
$49,999 or less	32.5
$50,000 - $99,999	33.9
$100,000 and up	33.6
RACE/ETHNICITY	
White non-Hispanic	75.5
MARITAL STATUS	
Married	59.5
TECHNOLOGY	
Uses Smart phone	79.2
Confident in making decisions about sharing information with companies in past month	47.5

Source: Pew Research Center, Internet Survey Privacy #4: http://www.pewinternet.org/2016/01/14/privacy-and-information-sharing/

Comparing men and women respondents' views of the acceptability of workplace surveillance via cameras with facial recognition software (see Figure 1), a simple unweighted bivariate Anova test shows that whereas nearly 2/3 of employed men say it is acceptable, only half of employed women do (65% vs. 50%, ANOVA $F=5.78$, $p<.02$, see Figure 1). Using multivariate logistic regression and sample weights, we analyze whether this gender difference persists after controlling for socio-demographic characteristics (age, education, income, race/ethnicity, marital status), and technology familiarity (smart phone use and confidence making decisions about information sharing). Table 3 shows that after controlling for these factors the relationship holds and becomes somewhat stronger, such that women are 49% less likely than employed men to say workplace surveillance via cameras with facial recognition software is acceptable (53% vs. 67%, Odds ratio = 0.51, $p<.05$).

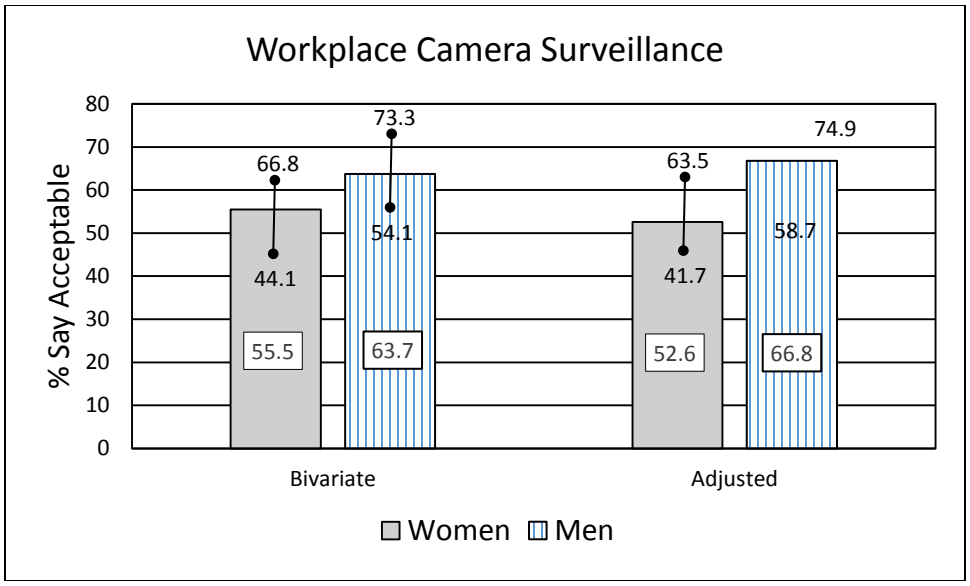

Table 3. Bivariate[1] and Adjusted[2] Acceptability of Workplace Camera Surveillance by Gender, Employed respondents, weighted analyses

[1] Anova F = 5.78 ($p<.05$).

[2] Adjusted for age, education, income, race/ethnicity, marital status, smart phone use, confidence in information sharing decisions. Odds ratio = 0.51, $p<.05$, CI: 0.27, 0.97.

Next we considered whether different perceptions of privacy might be part of the reason that men and women differ on the acceptability of workplace camera surveillance. To test this explanation, we examine whether men and women differ on perceptions of privacy for each measure asked in the survey (Table 1). In multivariate regression analyses of each of the nine privacy statements (data not shown), we find no statistically significant differences between men and women. So, including these privacy measures in logistic regression models (separately) of the acceptability of workplace camera surveillance has no meaningful effect on the association of gender to acceptability (data not shown). That is, women are still significantly less likely than men to find workplace camera surveillance acceptable, regardless of perceptions of privacy. These analyses did reveal, however, that one measure of privacy, not wanting to be monitored at work, is, not surprisingly, associated with views of the acceptability of workplace camera surveillance. That is, those who think it is very important not to be monitored at work are much less likely to say that camera surveillance in the workplace is acceptable. Though men and women are no more or less likely to say that not wanting to be monitored at work is very important, we test whether there is an interaction between gender and not wanting to be monitored at work on views of workplace camera surveillance. Table 4 shows that of women who think it is very important not to be monitored at work, less than 20 percent say that workplace surveillance via cameras with facial recognition software is acceptable. These women

are significantly less likely to say camera surveillance in the workplace is acceptable, not only compared to all men, but also to other women who are less concerned about monitoring at work (Odds ratio=0.12, p<.01, CI: .03, .52). When the interaction between gender and not wanting to be monitored at work is included in the multivariate logistic regression, the direct effects for women and not wanting to be monitored at work are no longer statistically significant, but the interaction (i.e., women who are concerned about monitoring at work) is statistically significant. This finding indicates that women who are more concerned about monitoring at work are the ones who are least likely to say FRT- equipped cameras are acceptable in the workplace, even for the case of monitoring theft.

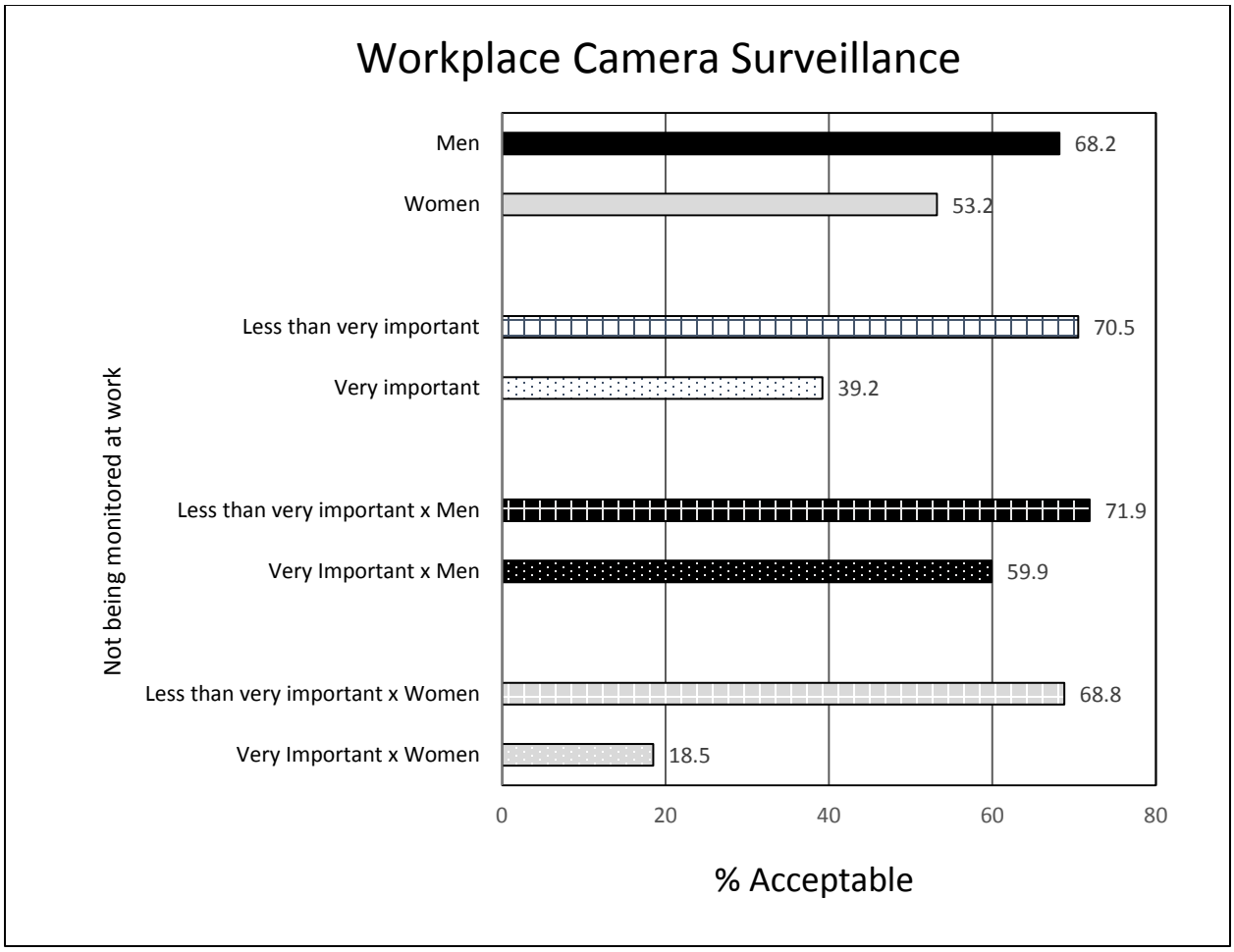

Table 4. Acceptability of Workplace Camera Surveillance by Gender and Importance of Not being monitored at Work, Employed respondents, weighted multivariate logistic regression analysis[1]

[1] Adjusted for age, education, income, race/ethnicity, marital status, smart phone use, confidence in information sharing decisions. Odds ratio for women*not being monitored at work interaction = 0.12, p<.01, CI: 0.03, 0.52.

Table 5 shows the comments of men and women who said that workplace surveillance using cameras with facial recognition software was not acceptable. We performed thematic coding using the five main analytic categories drawn from Nissenbaum's (2010) Contextual Integrity framework: data subjects/senders, data recipients, data types/purpose and data transmission principles. Overall, 81 percent of respondents who said workplace camera surveillance was unacceptable provided a statement of why they thought so. Women and men were equally likely to provide a response (47 of 58 women and 42 of 52 men). On three of the four categories (data recipients, data types/purpose, and data transmission principles), men and women make very similar types of statements, and at similar frequencies. For the category of data subject/sender, however, more than twice as many female respondents (30%) as male respondents (12%) made a comment that included a concern for themselves as data subjects. The content of the statements about data subjects are very similar between men and women. We did not see any evidence of women expressing particularly gendered concerns about being the data subject, for example related to being sexualized or targeted as weak or vulnerable. Rather, female respondents were simply more likely than male respondents to express concerns related to being the subject of FRT-enabled camera surveillance in the workplace.

Contextual Information Norms: Concerns/reasons not acceptable to have cameras in workplace	WOMEN	MEN
Data Subjects/Senders (reference to respondent, employees in general)	• I don't think I would want to work in a place that would need something like that • As long it involves all departments and employees not just a particular group • Any person who is in a victim protection program would be compromised by this invasion of privacy. • If I am being accused of a crime I did not do • I do not like being recorded or constantly watched.[1] • I would not work for a company that would install such a system. [1] • There are 6 employees in my office. If I	• Additionally, the feeling of constantly being watched/monitored would not make for a good work environment. [1] • If it was only used for the purposes stated and not as a way to monitor every single thing we are doing at work. [1] • This idea just bothers me. The workplace should not feel like a prison in which you have everyone watching your every move, basically breathing down your neck at all times. [1] • I hate cameras watching me. • That's like spying on me

Contextual Information Norms: Concerns/reasons not acceptable to have cameras in workplace	WOMEN	MEN
	can't trust even one of them I'm out of here. • I don't like the thought of being watched all day[1] • I work with people I highly trust. So on the one hand, there really is no need for a security system like that. On the other, if there was a security system like that in place, none of us are doing anything suspicious and have nothing to hide • It invades my privacy • I don't want the info about me retained indefinitely.[1] • I don't want to be monitored • I don't want someone to watch me when I'm working. Especially if I want to pick my nose or scratch my butt • [T]oo personal. [I] do not want every time I take bathroom breaks, etc. embarrassing	

Contextual Information Norms: Concerns/reasons not acceptable to have cameras in workplace	WOMEN	MEN
Data Receivers (reference to employer, boss, or other unspecified recipients)	• I do not like being recorded or constantly watched. [1] • I would not work for a company that would install such a system. [1] • I don't like the thought of being watched all day[1] • I don't like my company video taping me and being able to keep it indefinitely[1] • I do not want my boss watching me at all times. Especially not if my movements stay on a file. [1] • Big brother is watching. [1] • It is very uncomfortable to feel that people are or can watch your every move. • How secure it is and who can access it. [1] • Who has access to it. [1] • Who would have access to the footage and how securely it would be stored. [1]	• If the company has money to waste on that, they could try paying their employees a little more so they wouldn't have to steal Most people are just trying to make an honest living & to feed their families. • This idea just bothers me. The workplace should not feel like a prison in which you have everyone watching your every move, basically breathing down your neck at all times. [1] • There would be much opportunity for the employers to abuse certain privileges that the employees have. • No trust • Sounds like big brother would be watching more than for thieves. I do not agree with this type of monitoring and control[1] • This could too easily be abused. Too much power in the hands of people who may or may not have everyone's best interest in mind. [1]

Contextual Information Norms: Concerns/reasons not acceptable to have cameras in workplace	WOMEN	MEN
Data/Information Types & Purpose (types, location, expansion of purpose)	• Once cameras installed very difficult to go back. Over intrusive in terms of capturing everyone's facial recognition • Not sure how I feel about facial recognition technology. • It depends on where the cameras were. • Cameras to track people coming in and out of a building, locker room area, or entering an office area are just fine; actually a good thing for security. • Depends on the type of work setting • [Depends] On where the cameras are located • Depends where the cameras are placed. • Where the cameras are located • Use for safety ok but should not extend to attendance /performance under the guise of safety • They say that it will only be used to see who has been stealing but the reality is we all know that is not the truth. • It could be used in hiring and firing and used for other reasons that it was not originally being used for. • As long as they don't use the footage for any other purpose other than to retroactively see if they can identify suspects for crimes. • The use of the camera and it's purpose would have to be outlined and a statement signed by employees saying that they are aware of the cameras and agree to being monitored • If this was just for use to make my workplace more secure that's fine. However I don't like the idea of the company keeping this to judge my job performance in the future • This could very easily be abused and would hinder performance if every employee felt surveilled all the time. • They then could use that footage for whatever they wanted to. Selectively using it as they choose. Footage could be taken out of context.	• The camera should be in the entry/exit points only and not over workers' work spaces. • Where they put these cameras. • There should be limits on how long the employer can keep the records, or what they are allowed to do with the records. • It would depend on whether or not I could get a guarantee that it would just be used to identify theft. [1] • Tracking performance via cameras is very intrusive. There are other effective, non-intrusive means of tracking performance. [1] • I would like to know "why" the footage would stay on file if I have never been identified as an offender. [1] • Because the company could save a lot of different feeds and then use them all at once to make a person look bad so they could just terminate them. [1] • One problem has nothing to do with the other. Use of cameras to deter theft is one thing, but to track employee is another. Fake excuse. • The total use of the system is unacceptable. Identifying thieves is one thing, but this would be used in ways not intended. • Sounds like big brother would be watching more than for thieves. I do not agree with this type of monitoring and control[1] • If it was only used for the purposes stated and not as a way to monitor every single thing we are doing at work[1] • fear of misuse of intended purpose • For security purposes only • Only to solve problem • This could too easily be abused. Too much power in the hands of people who may or may not have everyone's best interest in mind. [1] • I don't think they should be using it for employee attendance and performance, just for security • If they just tracked employee attendance and performance for statistical purposes I would be fine with it. But if they used that footage to

Contextual Information Norms: Concerns/reasons not acceptable to have cameras in workplace	WOMEN	MEN
Data Transmission Principles (policies governing use, retention of data)	• The use of the camera and it's purpose would have to be outlined and a statement signed by employees saying that they are aware of the cameras and agree to being monitored[1] • Because it's not for a limited purpose/time. [1] • I don't like my company video taping me and being able to keep it indefinitely[1] • I do not want my boss watching me at all times. Especially not if my movements stay on a file. [1] • The footage should have a shelf life and should not be maintained once an employee has separated. [1] • I don't want the info about me retained indefinitely. [1] • 1984.Hitler • Big brother is watching. [1] • Too invasive • It is spooky • Freedom • How secure it is and who can access it.[1] • How secure is the storage of the footage. [1] • It is a good thing in a way to be able to track down thieves but would be invading privacy of the people working there too. • This could very easily be abused and would hinder performance if every employee felt surveilled all the time. [1] • Who would have access to the footage and how securely it would be stored. [1]	• I would like to know "why" the footage would stay on file if I have never been identified as an offender. [1] • Policy is too intrusive and I wouldn't want the company to keep the footage forever. [1] • The anti-crime aspect is good, but the lack of restrictions on how the company can use the footage (and lack of control on data retention) bothers me. [1] • There should be limits on how long the employer can keep the records, or what they are allowed to do with the records[1] • Because the company could save a lot of different feeds and then use them all at once to make a person look bad so they could just terminate them. [1] • Footage could stay on file forever. • Policy is too intrusive and I wouldn't want the company to keep the footage forever. [1] • It would depend on what they would do with it if I left the company • Totalitarianism big brother bullshit • Monitoring work by camera is insane • Invasion of privacy • Sounds like big brother would be watching more than for thieves. I do not agree with this type of monitoring and control • Seems too invasive • Invasion of privacy in the workplace • Intrusive • More Big Brother Bullshit.

Contextual Information Norms: Concerns/reasons not acceptable to have cameras in workplace	WOMEN	MEN
Alternative solution to theft problem in prompt	• Under-inclusive in terms of actually taking steps to identify and stop the [theft] • Rather just have lockable space for personal belongings • There are other ways to deal with theft that do not involve photographing me throughout my time in my workplace. • Is there a different way to go about it? • If our things could be protected from being stolen by having lockers. • I think other ways could be done • Employees should be held accountable but video footage is not the way to do this.	• There are other effective, non-intrusive means of tracking performance. • Less invasive security measures available • Not all that important • I don't think it's needed to prevent theft.

Table 5. Qualitative responses among employed respondents who said employer surveillance with cameras using facial recognition software is unacceptable, coded by Nissenbaum's elements of contextual integrity
Notes: [1] denotes statements that are coded into more than one category

Discussion

Using data from a nationally representative survey, we found that just over half of all employed respondents said that it was acceptable for employers to use camera surveillance with facial recognition software in the workplace to identify cases of theft, and potentially retain the information for other purposes. However, women are significantly less likely than men to say workplace camera surveillance is acceptable, consistent with previous studies of specific groups (e.g., Ball et al., 2012) that women are more likely than men to have concerns about workplace privacy and being monitored via workplace video surveillance. Surprisingly, we found no gender differences in perceptions of privacy more generally. However, we found that although employed women are no more likely than men to say not being monitored at work is important, of those women who did, significantly fewer than any other group (including other women or other men who said not being monitored at work is important) said that camera surveillance in the workplace is acceptable.

Our qualitative analysis of written responses from both men and women who said that workplace surveillance using cameras with facial recognition software was not acceptable showed some differences between male and female respondents. Unsurprisingly given the sample, both men and women chaffed at the notion of being surveilled at work, noting it diminished their sense of individual autonomy ("That's too personal"), compromised their sense of trust in their co-workers and employer ("I don't think I would want to work in a place that would need something like that"), and was reminiscent of totalitarianism ("Big Brother is watching"). Using Nissenbaum's framework of Contextual Integrity (CI) to identify various aspects of data flows that are normatively acceptable or not in the workplace, we found women did not differ from men in the *content* of statements expressing concerns. Both male and female respondents also flagged concerns around the fairness of such systems if deployed ("As long it involves all departments and employees [and] not just a particular group"), and noted the permanence of surveillance technologies after being deployed ("Once cameras installed very difficult to go back"). Overall, commentators agreed, in the words of one male respondent, that such a system "[…] could too easily be abused," and that the use of FRT seemed excessive and unnecessary.

However, in one coding category, that of being the data subjects of workplace surveillance, female respondents differed in the frequency of concern related to being a data subject, expressing concern at higher frequency than male respondents. Together with the quantitative findings that women are less accepting of workplace surveillance using cameras with facial recognition software, and that it is specifically women who do not want to be monitored at work who say such surveillance is unacceptable, these qualitative findings indicate that women may have particular concerns about workplace surveillance. According to scholars like Zureik (2003), the unwanted male gaze often underlies concerns about workplace surveillance: "In the case of the workplace, surveillance and privacy are associated with authority structures, body representation and consequent sexual harassment and discrimination" (Zureik, 2003:50). We also know that women at all levels and types of employment are likely to experience harassment at work (McLaughlin et al., 2012), so concern about being the subject of surveillance is not surprising, because, in the words of surveillance expert David Lyon (2007), "whatever the purpose of surveillance…some kind of power relations are involved." Women may be more aware of their status as targets of both the gaze of male coworkers and superiors, leading to a heightened awareness of the self as particularly affected by surveillance—and thus a higher rate of self-description as a data subject—in response to the question of why such surveillance is unacceptable.

Pew's workplace surveillance scenario had the highest level of acceptance of the seven scenarios presented in the 2015 survey (Raine & Duggan, 2015). Combined with its focus on theft, this "surveillance-friendly" scenario is thus something of a "best case" for situations in which individuals find surveillance, including surveillance with FRTs, acceptable. Yet the fact that

women were significantly less likely than men to say workplace camera surveillance is acceptable even in such a rosy scenario suggests a large and potentially durable bloc of opposition to surveillance.

The source of surveillance is power differences (Lyon, 2007), and so the impact of surveillance varies across individuals and groups (Anthony et al., 2017; Levy & Barocas, 2018; Stark, 2016). In this way, as Monahan (2009) argues, surveillance technologies tend to increase gender inequality in social contexts already marked by sexist power relations. The imposition of such surveillance, which often has negative consequences for employees generally, could exacerbate existing gender-based inequalities in workplaces in a variety of ways. Being less comfortable with, and potentially seeking to manage privacy more actively in the face of surveillance can potentially be understood as a cost in time and attention borne disproportionally by women. Misogyny is already recognized as a negative structural impediment to women, and even worse for women of color (Gilliom, 2001; Conrad, 2009); the cost of mitigating privacy harms within workplaces might be another way in which women's time and attention are unequally diverted from their careers.

The survey data used here were gathered by the Pew Research Center in 2015, a point in time prior both to the emergence of the #MeToo movement (Edwards et al., 2017) and to increasing public attention to the workplace automation and surveillance enabled by artificial intelligence (AI) technologies (Citron, 2008;Pasquale, 2015; O'Neil, 2017; Eubanks, 2018). In addition, one such technology, facial recognition software, is mentioned in the scenario but has become far more common, and controversial, since the survey was released (Gates, 2011; Stark, 2019). Scholars have noted the disproportionate impact on biometric technologies on women, as these technologies further exacerbate existing forms of discrimination; the impact of such surveillance can be analyzed using an intersectional approach that address the interlocking ways such systems compound vectors of oppression, particularly against women of color (Magnet, 2011; Dubrofsky and Magnet, 2015; Browne, 2015). As noted, the survey scenario's focus on workplace theft as the reason for the surveillance emphasizes concerns related to workplace safety and security generally, not sexual harassment or broader civil liberties concerns around the collection and use of biometric data such as the face. Additional studies would be valuable for determining whether these various public controversies have changed opinions, generally or by gender, regarding the acceptability of workplace surveillance.

Nonetheless, our finding that women are significantly more likely to consider workplace camera surveillance unacceptable, and their concern around being the data subjects of facial recognition technologies, has salience for interest in using cameras as a response to sexual misconduct in the workplace. While it might be possible to imagine video surveillance as a tool against workplace sexual harassment, such technologies also have the potential to exacerbate concerns around workplace privacy and power (Anthony et al., 2017). Given the distribution of power in the

workplace in which managers and supervisors are more likely to be male, the application of workplace camera surveillance technologies would be controlled by precisely those likely to be the harassers (Ball et al., 2012; Martin, 2016; Monahan, 2009). Broader concerns around the use of facial recognition software for misogynist purposes such as creating prurient "deepfake" virtual simulations of real individuals and doxxing or shaming women online also suggest the ubiquitous collection of such data in settings including the workplace may pose broader threats.

Limitations

This study is not without limitations. First, the Pew survey identifies respondents as either men or women, effacing the perspectives of any non-binary or genderqueer participants. This omission is particularly unfortunate given the ways digital systems tend to efface gender difference (Hicks, 2019), and in particularly how facial recognition technologies adversely impact, and frequently misgender, queer and trans people (Keyes, 2018; Scheuerman et al., 2019). Second, the survey did not ask respondents about their occupation; as such, we cannot analyze or control for the type of work or industry of respondents, which leaves questions regarding how structural differences in various types of workplace shaped participant reactions. Some occupations are more surveilled by cameras than others (such as manufacturing, retail and care-giving in institutions such as nursing homes); some, but not all, of these occupations are socially and culturally "gendered," with varying internal hierarchies of power which are themselves often divided by gender. Unfortunately, we cannot account for these factors in our study. Third, the survey presents very little detailed data about other critical identify features such as race, making it difficult to analyze how these factors might impact attitudes towards surveillance. Fourth, FRTs are now significantly more common in both deployment and public discussions, and increasing awareness of the impacts of these technologies may have changed opinions. It would be useful to have longitudinal data to see how opinions may vary while being able to account for broader social and technical changes that may affect individual opinions at any time. Finally, the relatively brief qualitative responses included in the survey are suggestive of participants' wide, complex and sophisticated set of opinions around workplace surveillance. Further qualitative data from different types of workers would help contextualize the gender differences we found among employed respondents, and potentially provide further insights around the specific contextual reasons for these differences.

Conclusion

Concerns about use of technology for surveillance have varied across cultures and over time (Anthony et al., 2015; Rule, 1973; Westin, 2003; Zureik et al., 2010). Surveillance in the workplace is not a new phenomenon, but the scale and scope of digital technologies such as facial recognition systems now enabling continuous, granular employer oversight of workers are novel, and deserving of attention. Workplace surveillance has the potential to further exacerbate already existing forms of inequality, and to entrench longstanding forms of discriminatory practice behind the veneer of technological opacity. In this paper, we have found that women are

much less likely than men to approve of the use of cameras equipped with facial recognition software in the workplace, even in what might be considered a "surveillance-friendly" scenario (that of safety). We take this finding as broad evidence that groups traditionally disadvantaged in Western societies, in this case women, will be more sensitive to the dynamics of surveillance—a dynamic supported by the wider literature in the topic—even if many of them acquiesce to it. Our qualitative findings are further evidence that privacy is contextual, articulated in different ways by different social factors including gender. Social norms govern expectations about appropriate access and flows of information, and women seemed to exhibit a heightened awareness of themselves as data subjects exposed to workplace surveillance.

Our findings in this paper leave considerable room for further research on the granular ways surveillance and privacy are experience and understood in the contemporary digitally mediated workplace, both by employers and employees. Detailed quantitative and qualitative surveys making comparisons both across job sectors and over time would be a valuable extension of these research themes; moreover, comparative analysis grounded in more detailed survey questions could examine how intersectional factors (including gender and racial identity, sexual orientation, socioeconomic status, disability, and others) interact with profession/job status around attitudes towards the wide variety of digital surveillance technologies now available to employers, and the deployment of FRT in particular, would be invaluable. Video surveillance may prompt less discomfort precisely because workers are so inured to it, while the use of more novel technologies such as FRT in workplaces settings might raise more pointed privacy concerns.

Finally, it is worth asking whether the recent prominence of the #MeToo movement has sharpened public opinion regarding workplace surveillance, either as means of warding off sexual harassment and assault or as a means by which such abuses are enabled. We speculate that women are particularly sensitive to the contextual nuances of such surveillance, including its tendency to reinforce existing power dynamics and asymmetries, but further research is needed to ground these assertions. We hope the increased attention and censure of the harassment and abuse by the powerful will prompt empirical diagnoses of the ways in which digital surveillance can help, and not hinder, movements like #MeToo.

References

Adib, A., & Guerrier, Y. (2003). The Interlocking of Gender with Nationality, Race, Ethnicity and Class: Narratives of Women in Hotel Work. *Gender, Work Organization*, *10*(4), 413–432.

Ajunwa, I., Crawford, K., & Schultz, J. (2017). Limitless Worker Surveillance. *California Law*

Review, *105*, 735–776. http://doi.org/10.15779/Z38BR8MF94

Ajunwa, I., & Greene, D. (2019). Chapter 3: Platforms at Work: Automated Hiring Platforms and Other New Intermediaries in the Organization of Work. In *Work and Labor in the Digital Age* (Vol. 33, pp. 61–91). Emerald Publishing Limited. http://doi.org/10.1108/S0277-283320190000033005

Allen, A. L. (1988). Uneasy Access: Privacy for Women in a Free Society. New York: Rowan & Littlefield.

Anderson, E. (2015). Liberty, Equality, and Private Government (pp. 1–62). The Tanner Lectures in Human Values.

Andrejevic, M. (2006). The Discipline of Watching: Detection, Risk, and Lateral Surveillance. *Critical Studies in Media Communication*, *23*(5), 391–407. http://doi.org/10.1080/07393180601046147

Angwin, J. (2010). The What They Know Series. Retrieved January 27, 2019, from http://juliaangwin.com/the-what-they-know-series/

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.

Anthony, D., Campos-Castillo, C., & Horne, C. (2017). Toward a Sociology of Privacy. *Annual Review of Sociology*, *43*(1), 1–21. http://doi.org/10.1146/annurev-soc-060116-053643

Anthony, Denise, Timothy Stablein, and Emily K. Carian.(2015). Big Brother in the Information Age. *IEEE Security & Privacy* 13(4):12-19.

Attewell, P. (1987). Big Brother and the Sweatshop: Computer Surveillance in the Automated Office. *Sociological Theory*, *5*(1), 87–100.

Ball, K. (2010). Workplace surveillance: an overview. *Labor History*, *51*(1), 87–106. http://doi.org/10.1080/00236561003654776

Ball, K., & Webster, F. (Eds.). (2003). The Intensification of surveillance: crime, terrorism and warfare in the information era. London: Pluto Press.

Ball, K., Daniel, E. M., & Stride, C. (2012). Dimensions of employee privacy: an empirical study. *Information Technology and People*, *25*(4), 376–394.

http://doi.org/10.1108/09593841211278785

Barrett, D. (2013, July 10). One surveillance camera for every 11 people in Britain, says CCTV survey. *The Daily Telegraph*. Retrieved from https://www.telegraph.co.uk/technology/10172298/One-vsurveillance-camera-for-every-11-people-in-Britain-says-CCTV-survey.html

Bayard de Volo, L. (2003). Service and Surveillance: Infrapolitics at Work among Casino Cocktail Waitresses. *Social Politics: International Studies in Gender, State & Society*, *10*(3), 346–376. http://doi.org/10.1093/sp/jxg019

Beniger, J. (1989). The Control Revolution: Technological and Economic Origins of the Information Society. Cambridge, MA: Harvard University Press.

Berdahl, J. L., & Moore, C. (2006). Workplace harassment: Double jeopardy for minority women. *Journal of Applied Psychology*, *91*(2), 426–436. http://doi.org/10.1037/0021-9010.91.2.426

Bernstein, E.S. (2012). The Transparency Paradox: A Role for Privacy in Organizational Learning and Operational Control. *Administrative Science Quarterly*, *57*(2), 181-216. https://doi.org/10.1177/0001839212453028

Bernstein, E. S. (2017). Making Transparency Transparent: The Evolution of Observation in Management Theory. *Academy of Management Annals*, *11*(1), 217–266. http://doi.org/10.5465/annals.2014.0076

Brayne, S. (2014). Surveillance and System Avoidance: Criminal Justice Contact and Institutional Attachment. *American Sociological Review*, *79*(3), 367–391. http://doi.org/10.1177/0003122414530398

Browne, S. (2015). Dark Matters: On the Surveillance of Blackness. Durham NC and London: Duke University Press.

Brooks, C., & Manza, J. (2013). A Broken Public? Americans' Responses to the Great Recession. *American Sociological Review*, *78*(5), 727–748. http://doi.org/10.1177/0003122413498255

Burawoy M. (1979). *Manufacturing Consent*: *Changes in the Labor Process under Monopoly Capitalism*. Chicago, IL: University of Chicago Press.

Citron, D. K. (2008). Technological Due Process. *Washington University Law Review*, 85, 1249–1313.

Conrad, K. (2009). Surveillance, Gender, and the Virtual Body in the Information Age. *Surveillance & Society*, *6*(4), 380–387. http://doi.org/10.24908/ss.v6i4.3269

Dubrofsky, R. E. and Magnet, S. A. (2015). "Introduction: Feminist Surveillance Studies: Critical Interventions" in *Feminist Surveillance Studies*, edited by R. E. Dubrofsky and S. A. Magnet, Durham, NC : Duke University Press.

Edwards, S., Dockterman, E., and Sweetland, H. (2017) "TIME Person of the Year 2018: The Silence Breakers" *Time*. https://time.com/time-person-of-the-year-2017-silence-breakers/. Retrieved August 30, 2019.

Egan, R. D. (2004). Eyeing the Scene: The Uses and (RE)uses of Surveillance Cameras in an Exotic Dance Club. *Critical Sociology*, *30*(2), 299–319. http://doi.org/10.1163/156916304323072125

Eubanks, V. (2018). Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor. New York: St. Martin's Press.

Etzioni, A. (1999). The Limits of Privacy. New York, NY: Basic Books.

Fisher, J. A., & Monahan, T. (2008). Tracking the social dimensions of RFID systems in hospitals. *International Journal of Medical Informatics*, *77*(3), 176–183. http://doi.org/10.1016/j.ijmedinf.2007.04.010

Fowler, G.A. (2019). The spy in your wallet: Credit cards have a privacy problem. *The Washington Post*, August 26. Retrieved from https://beta.washingtonpost.com/technology/2019/08/26/spyyour-wallet-credit-cards-have-privacy-problem/

Friedman, B., Höök, K., Gill, B., Eidmar, L., Prien, C. S., & Severson, R. (2008). Personlig Integritet: A Comparative Study of Perceptions of Privacy in Public Places in Sweden and the United States (pp. 142–151). Presented at the Proceedings of the 5th Nordic Conference on Human-computer Interaction: Building Bridges, New York, NY, USA: ACM. http://doi.org/10.1145/1463160.1463176

Gates, K. (2011). Our Biometric Future: Facial Recognition Technology and the Culture of Surveillance. New York: New York University Press.

Gellman, B., & Poitras, L. (2013, June 7). U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program. *Washington Post*. Retrieved from https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html?utm_term=.83e3f6c31983

Gilliom, J. (2001). Overseers of the Poor. Chicago & New York: University of Chicago Press.

Goold, B. J. (2004). CCTV and Policing. Oxford: Oxford University Press.

Greenwald, G. (2013, June 7). NSA collecting phone records of millions of Verizon customers daily. *The Guardian*. Retrieved from https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order

Haggerty, K. D., & Ericson, R. V. (2000). The surveillant assemblage. *British Journal of Sociology*, *51*(4), 605–622. http://doi.org/10.1080/00071310020015280

Harmon, A. (2019). As Cameras Track Detroit's Residents, a Debate Ensues Over Racial Bias. *The New York Times*, July 8. Retrieved from https://www.nytimes.com/2019/07/08/us/detroit-facial-recognition-cameras.html.

Hicks, M. (2019). Hacking the Cis-tem. *IEEE Annals of the History of Computing*, *41*(1), 20–33. http://doi.org/10.1109/MAHC.2019.2897667

Hirst, A., & Schwabenland, C. (2017). Doing gender in the "new office." *Gender, Work & Organization*, *25*(2), 159–176. http://doi.org/10.1111/gwao.12200

Igo, S. (2018). *The Known Citizen: A History of Privacy in Modern America*. Cambridge MA: Harvard University Press.

Keyes, O. (2018). The Misgendering Machines. *Proceedings of the ACM on Human-Computer Interaction*, *2*(CSCW), 1–22. http://doi.org/10.1145/3274357

Koskela, H. (2000). "The gaze without eyes": video-surveillance and the changing nature of urban space. *Progress in Human Geography*, *24*(2), 243–265. http://doi.org/10.1191/030913200668791096

Koskela, H. (2003). "Cam Era" — the contemporary urban Panopticon. *Surveillance & Society*, *1*(3), 292–313. http://doi.org/10.24908/ss.v1i3.3342

Kuo, F.-Y., Lin, C. S., & Hsu, M.-H. (2007). Assessing Gender Differences in Computer Professionals' Self-Regulatory Efficacy Concerning Information Privacy Practices. *Journal of Business Ethics*, *73*(2), 145–160. http://doi.org/10.1007/s10551-006-9179-1

Kwet, M. (2019). In Stores, Secret Surveillance Tracks Your Every Move. *The New York Times*, 14 June. https://www.nytimes.com/interactive/2019/06/14/opinion/bluetooth-wireless-tracking-privacy.html

Lake, J. (2016). *The face that launched a thousand lawsuits: the American women who forged a right to privacy*. New Haven, CT: Yale University Press,

Lee, M. K., Kusbit, D., Metsky, E., & Dabbish, L. (2015). Working with Machines (pp. 1603–1612). Presented at the the 33rd Annual ACM CHI Conference, New York, New York, USA: ACM Press. http://doi.org/10.1145/2702123.2702548

Levy, K. (2015). The Contexts of Control: Information, Power, and Truck-Driving Work. *The Information Society*, *31*(2), 160-174.

Levy, K., & Barocas, S. (2018). Refractive Surveillance: Monitoring Customers to Manage Workers. *International Journal of Communication*, *12*, 1166–1188.

Lohr, S. (2014). Workplace Surveillance and the "Transparency Paradox." *The New York Times*, 14 June. Retrieved April 12, 2015, from http://bits.blogs.nytimes.com/2014/06/21/workplace-surveillance-and-the-transparency-paradox/?_r=0

Lyon, D. (1994). The Electronic Eye: The Rise of Surveillance Society. Minneapolis, MN: University of Minnesota Press.

Lyon, D. (2007). Data, Discrimination, Dignity. In Surveillance Studies: An Overview (pp. 179–197). Malden, MA: Polity.

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

MacKinnon, C. A. (1979). Sexual Harassment of Working Women. New Haven, CT: Yale University Press.

MacKinnon, C. A. (2005). Women"s Lives, Men"s Laws. Cambridge, MA: Belknap

Press/Harvard University Press.

Madden, M., & Rainie, L. (2015). *Americans' Attitudes About Privacy, Security and Surveillance* (pp. 1–49). Pew Research Center. Retrieved from http://www.pewinternet.org/2015/05/20/americans-attitudes-about-privacy-security-and-surveillance/

Magnet, S. A. (2011). *When biometrics fail: gender, race, and the technology of identity*. Durham, NC : Duke University Press.

Martin, P. Y. (2016). `Mobilizing Masculinities": Women"s Experiences of Men at. *Organization*, *8*(4), 587–618. http://doi.org/10.1177/135050840184003

Marx, G. (2003). Some Information Age Techno-Fallacies. *Journal of Contingencies and Crisis Management*, *11*(1), 25–31. http://doi.org/10.1111/1468-5973.1101005

Marx, G. T. (2009). A Tack in the Shoe and Taking off the Shoe Neutralization and Counter-neutralization Dynamics. *Surveillance & Society*, *6*(3), 294–306. http://doi.org/10.24908/ss.v6i3.3286

McCahill, M., & Norris, C. (2003). Estimating the Extent, Sophistication and Legality of CCTV in London. In M. Gill (Ed.), *CCTV*. Leicester, UK: Perpetuity Press.

McLaughlin, H., Uggen, C., & Blackstone, A. (2012). Sexual Harassment, Workplace Authority, and the Paradox of Power. *American Sociological Review*, *77*(4), 625–647. http://doi.org/10.1177/0003122412451728

Monahan, T. (2009). Identity theft vulnerability: Neoliberal governance through crime construction. *Theoretical Criminology*, *13*(2), 155–176. http://doi.org/10.1177/1362480609102877

Mozur, P. (2019). One Month, 500,000 Face Scans: How China Is Using A.I. to Profile a Minority. *The New York Times*, April 14. Retrieved from https://www.nytimes.com/2019/04/14/technology/china-surveillance-artificial-intelligence-racial-profiling.html

Nippert-Eng, C. (2010). Islands of Privacy. Chicago and London: University of Chicago Press.

Nissenbaum, H. (2010). Privacy in Context: Technology, Policy, and the Integrity of Social Life. Palo Alto, CA: Stanford Law Books.

Nissenbaum, H. (2011). A Contextual Approach to Privacy Online. *Daedalus*, *140*(4), 32–48.

Nissenbaum, H. (2015). Respecting Context to Protect Privacy: Why Meaning Matters. *Science and Engineering Ethics*, *109*(4), 1–22. http://doi.org/10.1007/s11948-015-9674-9

O'Neil, C. (2017). Weapons of Math Destruction. New York: Broadway Books.

Ortiz, S. Y., & Roscigno, V. J. (2016). Discrimination, Women, and Work: Processes and Variations by Race and Class. *The Sociological Quarterly*, *50*(2), 336–359. http://doi.org/10.1111/j.1533-8525.2009.01143.x

Pasquale, F. (2015). The Black Box Society. Cambrige, MA: Harvard University Press.

Rainie, L., & Duggan, M. (2015). *Privacy and Information Sharing*. Pew Research Center. Retrieved from http://www.pewinternet.org/2016/01/14/privacy-and-information-sharing/

Rosenblat, A., & Stark, L. (2016). Algorithmic Labor and Information Asymmetries: A Case Study of Uber's Drivers, *The International Journal of Communication 10*, 3758–3784.

Rosenblat, A., Kneese, T., & boyd, D. (2014). *Workplace Surveillance* (pp. 1–19). Data & Society Working Paper.

Ruetschlin, C. & Asante-Muhammad, D. (2015). "The Retail Race Divide: How the Retail Industry Is Perpetuating Racial Inequality in the 21st Century." Retrieved August 30, 2019 from https://www.naacp.org/latest/retail-race-divide-the-retail-industry-is-perpetuating-racial-inequality/

Rule, J. B. (1973). Private Lives and Public Surveillance. London: Allen Lane.

Scheuerman, M. K., Paul, J. M., & Brubaker, J. R. (2019). How Computers See Gender. *Proceedings of the ACM on Human-Computer Interaction*, *3*(CSCW), 1–33. http://doi.org/10.1145/3359246

Sewell, G., Barker, J.R., & Nyberg, D. (2012). Working under intensive surveillance: When does 'measuring everything that moves' become intolerable? *Human Relations*, *65*(2), 189-215.

Simon, H. A. (1965). *The shape of automation for men and management*. New York : Harper & Row.

Singer, N. (2019). Amazon flunks children's privacy, advocacy groups charge. *The New York Times*, 9 May. Retrieved from https://www.nytimes.com/2019/05/09/technology/amazon-childrens-privacy-echo-dot-kids.html

Stanton, J.M. & Stam, K. (2003). Information Technology, Privacy, and Power within Organizations: a view from Boundary Theory and Social Exchange perspectives. *Surveillance & Society 1*(2), 152-190.

Stanton, J.M. & Stam, K. (2006). The visible employee : using workplace monitoring and surveillance to protect information assets--without compromising employee privacy or trust. Medford, N.J.: Information Today.

Stark, L. (2016). The emotional context of information privacy. *The Information Society, 32*(1), 14–27. http://doi.org/10.1080/01972243.2015.1107167

Stark, L., & Levy, K. (2018). The surveillant consumer. *Media, Culture & Society*, *105*(5), 016344371878198–19. http://doi.org/10.1177/0163443718781985

Stark, L. (2019). Facial recognition is the plutonium of AI. XRDS: Crossroads, the ACM Magazine for Students, 25(3), 50–55. http://doi.org/10.1145/3313129

Taylor, F. (1911). The Principles of Scientific Management. New York, NY: Harper & Brothers.

Thompson, E.P. (1967). Time, Work-Discipline, and Industrial Capitalism. *Past & Present*, *38*(December), 56-97.

Ticona J., & Mateescu, A. (2018). Trusted strangers: Carework platforms' cultural entrepreneurship in the on-demand economy. *New Media & Society*, *20*(1), 4384–4404

Timmons, S. (2003). Nurses resisting information technology. *Nursing Inquiry*, *10*(4), 257–269.

Ullmann-Margalit, E. (2008). The case of the camera in the kitchen: Surveillance, privacy, sanctions, and governance. *Regulation & Governance*, 2(4), 425-444.

Wu, P.F., Vitak, J., & Zimmer, M.T. (2019. A Contextual Approach to Information Privacy Research. *JASIST* 0(0), 1-6.

Yates, J. (1993). Control Through Communication. Baltimore, MD: The Johns Hopkins University Press.

Zerubavel, E. (2006). The Elephant in the Room. New York: Oxford University Press.

Zimmer, M. (2007, June 30). Function Creep 101: Surveillance Cameras and Social Norms. Retrieved April 12, 2018, from http://www.michaelzimmer.org/2007/06/30/function-creep-101-surveillance-cameras-and-social-norms/

Zuboff, S. (1988). In The Age Of The Smart Machine. New York: Basic Books.

Zuboff, S. (2019). The Age of Surveillance Capitalism. New York: PublicAffairs/Hachette.

Zureik, E. (2003). Theorizing surveillance: the case of the workplace. In D. Lyon (Ed.), *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination* (pp. 31–56). London and New York: Routledge.

Zureik, E. (2007). Surveillance Studies: From Metaphors to Regulation to Subjectivity. *Contemporary Sociology*, *36*(2), 112–115.