10-2019

Privacy at work: A review and a research agenda for a contested terrain

Devasheesh P. BHAVE
Singapore Management University, dbhave@smu.edu.sg

Huei Huei TEO
Singapore Management University, hhteo.2017@pbs.smu.edu.sg

Reeshad S. DALAL

PRIVACY AT WORK: A REVIEW AND A RESEARCH AGENDA FOR A CONTESTED TERRAIN

Devasheesh P. Bhave

Laurel H. Teo

Singapore Management University

Reeshad S. Dalal

George Mason University

This version 27 September, 2019

(Accepted for publication in the ***Journal of Management***.
Not edited or formatted for publication.)

https://doi.org/10.1177/0149206319878254

***Acknowledgements*:** We are grateful to the editor, Ernest O'Boyle, and the reviewers for their insights and guidance. We also thank Michael Bashshur, Gary Greguras, and Abhijeet Vadera for generative discussions and feedback on previous iterations of this work. This research was supported by funding from Singapore Management University's Internal Research Grant (C207/MSS17B012).

Abstract

Privacy in the workplace is a pivotal concern for employees and employers. Employees expect to be in control of the personal information and access they provide to the organization. Employers, however, expect extensive information regarding their employees as well as extensive access to employees' presence. The chasm between these two often competing expectations has been magnified by regulatory and technological trends. We begin the review by integrating viewpoints from multiple disciplines to disentangle definitions of privacy and to delineate the privacy contexts of information privacy and work environment privacy. We then identify the key stakeholders of privacy in the workplace and describe their interests. This discussion serves as a platform for our stakeholders' privacy calculus model, which in turn provides a framework within which we review empirical findings on workplace privacy from organizational research and related disciplines and from which we identify gaps in the existing research. We then advance an extensive research agenda. Finally, we draw attention to emerging technologies and laws that have far-reaching implications for employees and employers. Our review provides a road map for researchers and practitioners to navigate the contested terrain of workplace privacy.

Keywords: technology; individual decision-making; information systems; employee rights; information processing

Privacy . . . was a very valuable thing. Everyone wanted a place where they could be alone occasionally. And when they had such a place, it was only common courtesy in anyone else who knew of it to keep his knowledge to himself.

—Orwell (1949: 173)

The protagonist, Winston Smith, in George Orwell's book *1984* reflects upon the seemingly reasonable expectation that employees have of privacy: "to be let alone" (Warren & Brandeis, 1890: 205).[1] The dystopian future that George Orwell envisaged is arguably a feature of the contemporary workplace and, more broadly, society. The recent Cambridge Analytica scandal where people's behavior on Facebook was used to divine their Big 5 personality traits and subsequently target them with political messages, and the enactment of the European Union's (EU's) General Data Protection Regulation (GDPR), which enhances EU-based employees' rights to their data (including job performance data) wherever the data may reside, are just two such examples of the criticality of privacy concerns (European Commission, 2018). Ever new privacy infringements are cited in the news, and prognosticators frequently proclaim that "privacy is dead" (BBC News, 2017; Mims, 2018).

Not surprisingly, employees believe that their right to privacy is under threat, and they have contested this in the legal arena. This has resulted in a string of lawsuits encompassing diverse infringements related to the use of biometric information (Kelly & Hays, 2018), to the protection of information related to a cancer diagnosis (The HR Specialist, 2018), to employers' concerns with employees "liking" unsavory content on social media even if it is after work hours and on their personal devices (Hyman, 2017), and to a now prosaic one of computer use at work for personal purposes (Bowcott & Rawlinson, 2017). But organizations

[1] First, the quotation reflects the different contexts (that we later delineate) where privacy matters: privacy of work environment, information, and autonomy. Second, many scholars cite Warren and Brandeis (1890) and define the *right to privacy* as the "right to be let alone." Gavison points out that this is an inaccurate interpretation of Warren and Brandeis's work and that they "never equated the right to privacy with the right to be let alone; [they merely] implied that the right to privacy is a special case of the latter" (1980: 437).

also have a right to collect information on their workforce. Through the course of the employment relationship, organizations need information regarding the ability, motivation, and performance of their employees (Culnan, Smith, & Bies, 1994). It is also arguably important for organizations to possess information about the integrity of their employees and institute mechanisms that deter counterproductive, unethical, and/or illegal work behavior (e.g., taking excessive work breaks, falsifying safety records, and stealing from the organization or customers; Stone-Romero & Stone, 2007). The process of collecting this information is fraught with legal challenges, with lawsuits related to using integrity tests (Karren & Zacharias, 2007), conducting credit and background checks (Nielsen & Kuhn, 2009; Ryan & Lasek, 1991), and using organizational communication technologies (Dillon, Hamilton, Thomas, & Usry, 2008). Tensions related to workplace privacy thus sit at this intersection of organizational requirements for employee information and employee considerations of individual rights (Culnan et al., 1994).

Considerations of privacy in the workplace, however, are not a budding infatuation (see Igo, 2018, for a broader, historical view of privacy in the United States). Aristotle, the Greek philosopher, drew a contrast between the public sphere of political activity (*polis*) and the private or family sphere (*oikos*; Roy, 1999; see also Farrall, 2008, regarding Ancient China). John Stuart Mill (1978), the 19th-century English philosopher, reiterated this notion of two distinct spheres of life: self-regarding activities that were justifiably out of society's purview (and within the domain of self-regulation) as opposed to other-regarding activities that were subject to governmental authority. Furthermore, one context of exerting governmental authority, as conceived by Jeremy Bentham (Mill's mentor) over two centuries ago was through the "panopticon": a prison designed such that a single authority can monitor all the inmates simultaneously without the inmates being able to detect whether (or rather when) they are being monitored (Semple, 1993). More recently, the French philosopher

Michel Foucault highlighted how the panopticon also serves as a model for contemporary workspaces and wondered, “Is it surprising that prisons resemble factories, schools, barracks, hospitals, which all resemble prisons?” (1995: 228). Foucault emphasized how thinking about the possibility that one is observable—even if not being actively observed—in effect serves as a means of social control. This notion of control—of information, workspace, and autonomy—undergirds organizational scholarship on privacy (e.g., E. F. Stone & Stone, 1990; Sundstrom, Burt, & Kamp, 1980). This body of work provides an important foundation from which to understand the current challenges of privacy in the workplace.

Demographic, public policy, and globalization trends are now at the forefront of this debate on what is private and what is not. In addition, technology is providing the sharpest thrust to bring workplace privacy issues center stage (Acquisti, Brandimarte, & Loewenstein, 2015). This includes accessing social media for employee selection (Roth, Bobko, Van Iddekinge, & Thatcher, 2016), using electronic monitoring to assess employees’ performance (Bhave, 2014), and harnessing the emergence of Big Data, the Internet of Things, and artificial intelligence in the workplace (A. K. Agarwal, Gans, & Goldfarb, 2017). Such technological advances are outpacing our understanding of the privacy implications in the workplace. For instance, estimates suggest that by 2020, over 200 billion sensor devices at home (e.g., Amazon Alexa), in cars (e.g., the Global Positioning System, or GPS), on smartphones (e.g., fingerprint scanners), and in health monitoring devices (e.g., FitBits) will be interconnected (Adams, 2017). This will generate tremendous amounts of data that can provide information on employees’ health, time use, and productivity across work and home domains. These data, however, are also susceptible to data breaches that enhance risks to employees’ privacy as well as corporate reputation (Adams, 2017).

This brings us to a question that underpins scholarly work on privacy: why does privacy matter? Or in other words, “what is the value of privacy?” To address this difficult

question, we could conjure the hypothetical notion of "perfect privacy" (Gavison, 1980). Gavison clarifies that in perfect privacy, a person is "completely inaccessible to others . . . no one has information about X, no one pays any attention to X, and no one has physical access to X" (1980: 428). Perfect privacy is neither feasible nor desirable in society but it helps point to the associated concept of *loss of privacy* (or what is operationalized in organizational scholarship as *perceived invasion of privacy* or *perceptions of invasiveness*; Gavison, 1980). Bloustein posits that a loss of privacy is not only unsettling but also represents an insult to a person's "independence, dignity, and integrity" (1964: 971). Privacy thus possesses intrinsic value: it is essential for thinking and acting freely (Alge, Ballinger, Tangirala, & Oakley, 2006; Stone-Romero & Stone, 2007). All these factors provide a compelling rationale for a systematic review of privacy in the workplace. More importantly, they point to the need to craft a clear research agenda that outlines the multiple interfaces—legal, ethical, technological, international, and human resources, at the very least—of privacy in the workplace.

We organize the review along the following lines. First, we address definitional issues related to privacy in the workplace. Although present-day privacy concerns center on employee *data* privacy, other concerns revolve around control of one's personal space and reflecting notions of autonomy, the freedom of control by others (Stone-Romero & Stone, 2007; Sundstrom et al., 1980). We delineate these different dimensions of privacy: information privacy, work environment privacy, and autonomy privacy. Second, we identify the relevant stakeholders of privacy in the workplace. These stakeholders include different actors associated with the employment relationship: employees, employers, the state, and society at large (Budd & Bhave, 2010). Because privacy is important to each stakeholder (Rachels, 1975), problems surface when coordinating across the privacy boundaries between stakeholders (Petronio, 2002). We delineate these problems and illustrate how they could

manifest as legal contests. Third, the legal contests point out that privacy-related decisions are complex because stakeholders possess their own "privacy calculus"—a cost-benefit analysis of the returns accrued for sharing information with the associated risks of doing so (Klopfer & Rubenstein, 1977; Margulis, 2003). We develop an integrative conceptual model that considers how each stakeholder's privacy calculus is shaped and how these calculi influence relevant employee outcomes. We then identify the connections of the stakeholders' privacy calculus model to existing privacy theories. Fourth, under the aegis of this model, we review empirical findings in privacy research and identify key antecedents, mechanisms, boundary conditions, and consequences of organizational privacy. Because the privacy literature is voluminous and spans multiple disciplines (e.g., law, marketing, information systems), we primarily consider findings from, or at least particularly relevant to, organizational research. Fifth, we delineate an expansive agenda for future research. Finally, we conclude with implications for employees and organizations. Each of these endeavors requires additional details that for reasons of readability and space constraints, we furnish in an online supplement to the paper. Overall, we update and extend prior reviews that either explicitly (e.g., Linowes & Spencer, 1997; Stone-Romero & Stone, 2007) or implicitly (e.g., Alge & Hansen, 2014; Bernstein, 2017) focus on workplace privacy.

WHAT IS PRIVACY?

Defining privacy is a thorny issue. Philosophers, economists, psychologists, sociologists, and jurists, among others, have had protracted, and as yet not completely resolved, debates about its definition (e.g., Nissenbaum, 2004; Prosser, 1960; Schoeman, 1984; see also the online supplemental material, in which we draw from conceptualizations in philosophy and law to provide an extensive discussion of definitional issues). One reason for these disagreements is that different conceptualizations of privacy (Solove, 2002) do not take into account the role of contextual norms—norms that exist based on the law, history, culture,

or convention (Nissenbaum, 2004). For instance, requiring each employee to swipe an organizational identity card for security purposes when entering one's workplace may not violate privacy norms. On the other hand, if the organizational identity card is embedded with a radio frequency identification (RFID) tag that can detect and record an employee's movements throughout the workday, and if this information is subsequently compiled to provide a detailed picture of an employee's time spent in the organization across different activities over several months, then it could violate privacy norms (see Francis & Francis, 2017). Put simply, privacy intrusions are perceived when contextual norms are believed to be violated (Nissenbaum, 2004; Solove, 2002).

Privacy: Prevailing Context-Based Definitions from Organizational Research

Over the last three decades, Stone and Stone-Romero (E. F. Stone & Stone, 1990; Stone-Romero & Stone, 2007) have been the primary catalysts for organizational research on privacy. Because they focus on privacy in a specific context—the employment context—their definition of privacy, fittingly, is a contextual one. E. F. Stone and Stone drew on Westin's (1967) pioneering work and defined privacy as:

> a state or condition in which the individual has the capacity to (a) control the release and possible subsequent dissemination of information about him or herself, (b) regulate both the amount and nature of social interaction, (c) exclude or isolate him or herself from unwanted (auditory, visual, etc.) stimuli in an environment, and, as a consequence, can (d) behave autonomously (i.e., free from the control of others). (1990: 358)[2]

This definition has served as the backbone for privacy research in the fields of organizational behavior and human resources (e.g., Alge, 2001; Zweig & Webster, 2002). Furthermore, E. F. Stone and Stone's (1990) definition identifies three specific organizational

[2] The last portion of E. F. Stone and Stone's (1990) definition indicates that "*as a consequence*" of information privacy and work environment privacy, employees could work in an autonomous fashion. That is, information privacy and work environment privacy are preconditions for employee autonomy. This portion of their privacy definition links the question "what is privacy" with the question "what is the value of privacy for employees" and reinforces the intrinsic value of privacy—an aspect that we outlined earlier.

contexts where employees' privacy matters: their information (information privacy), their workspace (work environment privacy), and their capacity to work in an autonomous fashion (autonomy privacy). We draw on other disciplines to elaborate upon and to clarify the definitions for each of these three *privacy contexts* (see the online supplemental material).

E. F. Stone and Stone (1990) clarified that there is inevitably some overlap between these three privacy contexts (also referred to as dimensions of privacy by some scholars). As they pointed out, if employees are unable to exert control over their physical workspace (work environment privacy), they may be unable to exert control over whether (and when) to interact with their coworkers (autonomy privacy), and thereby may be unable to exert control over any information collected about them (information privacy). Put simply, these three privacy contexts are intermingled to a degree. In accordance, Ball, Daniel, and Stride (2012) observed that there existed positive correlations between the three dimensions ($r \approx .30$), yet the moderate magnitude of the correlations also indicates that these dimensions are unique. Because technological developments are spurring the overlap of privacy contexts, we will elaborate upon this aspect later in the review.

Working Definitions of Information Privacy and Work Environment Privacy

We now delineate our working definitions of information privacy and work environment privacy—the two privacy contexts considered in this review.[3] The definitions include two distinct *conceptualizations* of privacy: privacy as control and privacy as state (see the online supplemental material). In practical terms, from the standpoint of organizational research, the distinction between conceptualizing privacy as control versus as a state reflects the difference between "actual privacy" and "perceived privacy" (e.g., Hajli &

[3] Given the substantial research on autonomy in the workplace (for reviews, see Gagné & Bhave, 2011; Kanfer, Frese, & Johnson, 2017; Latham & Pinder, 2005), we will consider autonomy privacy only to the extent that it directly informs information privacy and work environment privacy. That is, in our review, we will focus on information privacy (which includes the bulk of organizational privacy research) and on work environment privacy (which includes a small body of work that is now reinvigorated).

Lin, 2016; Stone-Romero & Stone, 2007). For example, when organizations are considering collecting information about employees or making changes to their work environment, they are concerned with "actual" levels of *control* that they intend to exercise; employees' views of these informational and work environment aspects, on the other hand, reflect their "perceptual" *state*. In the definitions we discuss below, we incorporate the conceptualizations of privacy as both control and a state.

Information privacy entails (perceptions of) control over the acquisition, storage, use, dissemination, and dispersal of employees' data. That is, it concerns control over the information that could be made available to others. *Work environment privacy* entails (perceptions of) control over the sensory stimuli (visual, space, acoustic, olfactory) in employees' work environment. That is, it concerns control over the extent and nature of employees' interpersonal interactions and, more broadly, access to employees' presence.[4]

We offer two concluding thoughts on definitional issues: First, in clarifying what privacy is, researchers have attempted to clarify what privacy is not (i.e., secrecy, confidentiality, anonymity, de-identification, or the right to be forgotten). This, too, involves expansive and as-yet-unresolved debates across disciplines. We will skirt these inconclusive debates by referring the interested reader to other sources that have attempted to distinguish privacy from these constructs (Francis & Francis, 2017; H. J. Smith, Dinev, & Xu, 2011) and by instead emphasizing the existing organizational research on, or at least closely connected to, privacy. Second, as we note above, defining privacy implicitly involves acknowledging why it matters. Integral to this "why" question is the related one of "for whom does privacy matter?" This brings us to the different stakeholders of privacy and how their interests inform concerns of information privacy and work environment privacy.

[4] In the sections that follow, wherever applicable, we specify whether we are referring to information privacy or work environment privacy. If the discussion pertains to both, we use the terms *privacy* or *workplace privacy* or *organizational privacy* for simplicity.

WHO ARE THE STAKEHOLDERS OF PRIVACY IN THE WORKPLACE?

Our focus is on the employment relationship—the "connection between employees and employers through which individuals sell their labor" (Budd & Bhave, 2010: 51). The key stakeholders (or actors) in this relationship are employees, employers, and the state. Each actor possesses unique interests. For employees, these include income and fulfilment; for employers, they include profit maximization and ensuring stakeholder value; for the state, they include safeguarding freedom and ensuring the rule of law (see Budd & Bhave, 2008). The interests of these actors are often incompatible.

Consider, for instance, the use of drug testing in the workplace (Arthur & Doverspike, 1997). Employers could claim that drug testing is essential to ensure that the work environment is safe; conversely, employees could claim that conducting such tests requires them to reveal their medical information. That is, what employers consider to be a process of collecting relevant employee information—a form of monitoring—could be viewed by employees as a loss of control over their information, or a personal infringement, and may lead them to contest this testing in the legal arena. This then brings in the third actor: the state. The state—through the legal system—would adjudicate the competing claims of the two parties. Beyond ensuring the rule of law, the state also has a role to protect the citizenry. In the aforementioned drug testing instance, the state's protective rights come to the fore in the event of employee or employer infringements that impinge upon the general public (e.g., a drug-impaired nurse injuring a patient constitutes both an employee lapse and an employer one of negligent hiring; Fiesta, 1993). This is just one example of how privacy is a contested terrain in the employment relationship.

We have included citations to contemporary legal cases that surface employees' and employers' privacy-related tensions in the online supplement.[5] As noted, privacy issues surface on account of the incompatibility of the interests of employees and employers. Differences in employees' and employers' interests signal differences in how they each value privacy. There are, however, inconsistencies in this valuation process. For instance, at times, employees willingly engage in self-disclosure, which then compromises their privacy (Altman, 1975). Yet providing personal information in interpersonal interactions is also helpful in establishing strong interpersonal connections and fulfilling employees' relatedness needs (Gagné & Deci, 2005). A broader question, then, is when do employees and employers choose to provide information or access, and when do they choose to limit it? Put simply, how do stakeholders make privacy-related decisions?

STAKEHOLDERS' PRIVACY CALCULUS MODEL

An answer proffered by the field of privacy economics is that privacy-related decisions involve tradeoffs (Acquisti, 2009). Stakeholders need to decide when to permit sharing their information (or their access) and when to protect it (Acquisti, 2009; D. L. Stone & Stone-Romero, 1998). Specifically, stakeholders possess a *privacy calculus*: they engage in a cost-benefit analysis where they weigh the risks of providing information (or access) versus the benefits of doing so (Culnan & Armstrong, 1999; Laufer & Wolfe, 1977). A privacy calculus essentially considers privacy in rational, economic terms (Klopfer & Rubenstein, 1977). Stakeholders balance their perceived risks of disclosing or withholding information (or access) to other stakeholders with their perceived benefits of doing so; perceived risks are associated with withholding information, and perceived benefits are associated with disclosing information (Dinev & Hart, 2006; Petronio, 2000; White, 2004).

[5] Because of our focus on organizational scholarship, we primarily consider the interests of employers and employees. The state's interests, however, are implicitly incorporated through the specific legal provision and its subsequent enforcement.

For example, as studies on preemployment drug testing (e.g., D. L. Stone & Bowden, 1989; D. L. Stone & Kotch, 1989) indicate, a job applicant needs to weigh the consequences of undergoing a drug test. Specifically, the applicant needs to balance perceptions of invasion of privacy with the possible benefit of securing the job. In seeking this information from the job applicant, the organization also needs to balance perceptions regarding its employment brand (i.e., if it is perceived as an employer that invades its employees' privacy) with the possibility of making a negligent hire. Both organizations and employees thus need to make such deliberations that inform their respective privacy calculi.

For employees (or applicants), key risks involved in providing information (or access) are perceptions of invasion of privacy associated with the potential loss of control of one's information (E. F. Stone & Stone, 1990; Stone-Romero & Stone, 2007). A key benefit for employees in providing relevant information is a reduction in the information asymmetry that exists between them and their employer—a reduction that helps them in securing pertinent employment outcomes (e.g., getting hired, establishing their integrity, showcasing their performance; Eisenhardt, 1989; Pepper & Gore, 2015). A consideration of these risks and benefits shapes the *employee's privacy calculus*.

For an organization, the key risk when collecting employees' (or job applicants') information is the potential for invading the privacy of its employees and the associated detrimental effects on employees' morale and/or on the organization's employment brand (see D. G. Allen, Mahto, & Otondo, 2007). The key benefit for the organization is that possessing superior information on its employees can help it make better employment-related decisions that enhance the organization's security and mitigate its legal liability (Culnan et al., 1994). A consideration of these risks and benefits shapes the *organization's privacy calculus*.

However, the privacy calculus is not just a rational assessment of risks and benefits. The privacy calculus is also subject to "social norms, emotions, and heuristics" and associated inconsistencies in estimation (Acquisti et al., 2015: 510). For instance, even though Canada and the United States are considered virtually identical in terms of societal culture (Hofstede, 1980), they differ in levels of tolerance toward drug and alcohol testing in the workplace: Canadians consider such policies to be less fair and are less tolerant of them compared to Americans (Seijts, Skarlicki, & Gilliland, 2002). Similarly, although both Europeans and Americans are concerned about information privacy, Europeans are more concerned about information privacy with respect to corporations, whereas Americans are more concerned about information privacy with respect to the government (Francis & Francis, 2017). These differences speak to underlying differences in social norms, national culture, and/or the legal environment that influence employees' privacy calculus.

In sum, each stakeholder's privacy calculus illuminates that stakeholder's interests. The privacy calculus thus facilitates an integrative frame to connect the interests of different stakeholders. For this reason, the privacy calculus is a focal construct in the model we develop (see Figure 1). The model considers two levels of context—omnibus and discrete (Johns, 2006)—and unfolds as follows. We consider the organization's privacy calculus to be shaped primarily by the *omnibus* context represented by the macrofactors of social norms, national culture, and the legal system. The organization's privacy calculus then shapes the *discrete* privacy contexts of information and the work environment. Employees experience the privacy contexts through explicit (e.g., an organization's data storage policy) or implicit (e.g., an organization's office layout) organizational practices and policies. Thus, the privacy contexts directly influence employees' behavioral and cognitive-affective work outcomes.

--See Figure 1--

Furthermore, the organization's privacy calculus indirectly influences employees' privacy calculus via the privacy contexts. Employees' privacy calculus is also independently influenced by the macro factors and by individual factors (personality and demographics). Employees' privacy calculus then affects their work outcomes. Finally, these work outcomes serve as a form of feedback that informs the organization's privacy calculus and, in turn, the privacy contexts. That is, the privacy contexts are not only antecedents to employees' privacy calculus and employees' outcomes but also, over time and indirectly (through the organization's calculus), outcomes of them.

The model fulfils two objectives. First, as we elaborate in the next section, the model serves as an organizing framework to discuss empirical organizational research on privacy. Specifically, we summarize findings on both information privacy and work environment privacy from the existing organizational research on privacy. We supplement these findings with relevant research from other disciplines (e.g., marketing, information systems, environmental psychology). Furthermore, we discuss the relevance of recent technological trends (e.g., Big Data and artificial intelligence) and regulatory changes in several parts of the world (e.g., the EU's GDPR) that have implications for privacy in the workplace. In so doing, we also build on narrative reviews that focus either directly or indirectly on workplace privacy (e.g., Alge & Hansen, 2014; Bernstein, 2017; Stone-Romero & Stone, 2007).

Second, the model integrates across, and offers connections to, different theories of privacy. For instance, the model is consistent with the work of early theorists Westin (1967) and Altman (1975), who noted that privacy functions as both a *dynamic process* and one that operates at *specific levels*. Altman clarified that privacy as a *dynamic process* entails managing interpersonal boundaries between the individual and the group. People regulate how open or closed they are when they interact with others (Margulis, 2003). Through the communication privacy management theory, Petronio (2002) further explained that boundary

management exists on a continuum from open boundaries (where people are comfortable providing information or access) to those that are closed (where people protect their information or limit their access). Legal tussles could be conceptualized as instances of boundary turbulence: situations when employees or employers do not protect the other party's information to an extent believed adequate by the other party (Margulis, 2003; Petronio, 2002). Taking legal recourse is thus an avenue to establish or resurrect effective boundaries.

Because people have expectations regarding specific levels of privacy (i.e., differences between desired and actual levels of privacy), privacy also functions at *specific levels* (Margulis, 2003). Such expectations are partially derived from people's internal motivation and external role requirements (Altman, 1975; Westin, 1967). People's decisions to disclose or withhold information (or access) thus involve regulating their external interpersonal boundaries in concert with their internal states (see Petronio, 2002). Integral to this endeavor is a tradeoff—one that is encapsulated by the privacy calculus in our model.

Across two frameworks, Stone and Stone-Romero also highlight the salience of the privacy calculus. In their organizational privacy model, E. F. Stone and Stone (1990; see also Stone-Romero & Stone, 2007), invoke the privacy calculus to derive an expectancy theory–based model. This model primarily focuses on employees' motivations to protect their privacy and identifies a discrepancy between actual and desired levels of privacy (i.e., expectations about *specific levels*) that influences employees' perceptions of invasion of privacy as well as subsequent work outcomes. Furthermore, in their multiple stakeholder model of privacy, D. L. Stone and Stone-Romero (1998) capture the heart of the privacy calculus, namely, how each stakeholder's values and objectives shape its ability to control information.

Our model incorporates this stakeholder perspective and the role of the macro factors and individual factors that influence the privacy calculus. In addition to dovetailing with other theoretical perspectives in privacy research, our model extends multiple theories in several ways. We distill abstract conceptualizations of privacy into discrete privacy contexts of information privacy and work environment privacy. These privacy contexts have clear operationalizations, thus facilitating the testability of this model (Klein & Zedeck, 2004). Relatedly, by integrating perspectives from information economics (which views privacy as a commodity; Davies, 1997) with those from environmental psychology (which is concerned about privacy in terms of one's workspace; Sundstrom, 1986), we create a bridge between these disciplines that permits an examination of the two privacy contexts independently as well as when they are intermingled (i.e., similar to information, employees' workspace could also be viewed as a commodity; e.g., coworking spaces, which are rented workspaces shared by employees across different organizations; Bouncken & Reuschl, 2018.). We delineate the privacy calculus of each stakeholder to provide an integrative lens through which one could examine employees' and employers' privacy calculi and their interplay. We clarify that there are two pathways that shape employees' privacy calculus: a direct pathway (influenced by macro factors and individual differences factors) and an indirect pathway (influenced by macro factors that shape the organization's privacy calculus and subsequently the privacy contexts). In so doing, we "[organize and thus simplify] a set of previously unorganized and scattered observations" into a cohesive model that captures the complexity of employees' privacy-related decision-making—their privacy calculus—as it exists in contemporary workplaces (Klein & Zedeck, 2004: 932).

REVIEW OF EMPIRICAL FINDINGS IN ORGANIZATIONAL PRIVACY RESEARCH

As mentioned previously, we use the model (see Figure 1) as an organizing framework to discuss empirical organizational research on privacy. In the section below, for each link in the model, we first *review findings from organizational research*. We then *assess* this body of work, drawing on organizational research as well as research *from other disciplines* (e.g., marketing, information systems) that provides insight on the topic but from the perspective of stakeholders who are generally not considered in organizational research (e.g., consumers, the general public). In so doing, we preview our subsequent suggestions for future research.

Findings Related to Macro Factors, the Organization's Calculus, and Employees' Calculus

We considered three macro factors that will influence both calculi: national culture, social norms, and the legal environment. We detail findings related to these aspects, and extensions to related work, in the online supplement (*Note: In this pre-publication manuscript, we have included the supplement as Appendix 1*).

Findings Related to Privacy Contexts

In this section, we focus on the two privacy contexts of information and the work environment. In reviewing findings for both these contexts, we primarily emphasize the perceptions of invasiveness that are integral to employees' (and applicants') privacy calculus.

Information privacy: Summary of findings. Information privacy encompasses the type of information on employees that is collected by organizations, the purpose of information collection, the source of information collection, and how the data are stored and used (or are likely to be used; H. J. Smith, Milberg, & Burke, 1996; E. F. Stone & Stone, 1990; Woodman, Ganster, Adams, McCuddy, Tolchinsky, & Fromkin, 1982). Concerns with

applicant perceptions of invasiveness are a long-standing issue in employee selection research and are important because they influence applicants' attraction to hiring organizations, their job acceptance intentions, and the likelihood of them recommending the employer to others (Hausknecht, Day, & Thomas, 2004; McCarthy, Bauer, Truxillo, Anderson, Costa, & Ahmed, 2017). Specifically, the concerns center on *what* (i.e., type or content of questions) is asked of applicants and *how* (i.e., the specific method) that information is gleaned during the selection process. Implicit to both the what and how questions is the *why*: applicants' considerations of the purpose of the information sought (E. F. Stone & Stone, 1990).

In terms of the *type* of questions (i.e., the *what*), items related to family background (e.g., religious observance), medical history (e.g., pregnancy-related details), and credit history are viewed as more invasive than items related to educational background (e.g., grade point average in math), professional experiences (e.g., job loss), professional achievements (e.g., sales and bonuses), and interests and hobbies (Mael, Connerley, & Morath, 1996; Rosenbaum, 1973). On integrity tests specifically, items asking participants to admit actual counterproductive behaviors were perceived to be more invasive than items on participants' inclination to engage in counterproductive behaviors, to protect misbehavior of friends or coworkers, or to be lenient towards others' wrongdoings (Dwight & Alliger, 1997).

One option for applicants who perceive specific questions to be invasive is to choose not to answer them. However, D. L. Stone and Stone (1987) observed that prospective applicants who intentionally did not answer some questions (e.g., prior criminal convictions) on application blanks were viewed less favorably in terms of their job suitability compared to those who reported no prior conviction. Notably, there were no statistical differences in job suitability ratings of applicants who reported *prior convictions* compared to those who had left this information missing. This finding is in line with judgment and decision-making

research suggesting that decision makers view missing information negatively (almost as negatively as they view negative information), especially when it is on important topics (Bonaccio & Dalal, 2010). In other words, nonresponse by applicants to potentially invasive items is not an effective privacy protection strategy.

Research findings regarding applicants' perceptions of the specific *methods of selection* (i.e., the *how*) and the *purpose of information collection* (i.e., the *why*) are interwoven. Stone-Romero, Stone, and Hyatt (2003) compared the levels of invasiveness associated with 12 selection procedures. They reported that lie detector tests, medical exams to assess potential for disease, and drug tests were perceived as being higher on levels of invasiveness, whereas application blanks, work samples, and interviews were perceived to be less so. Thibodeaux and Kudisch (2003) found that applicants' reactions regarding the test's job relatedness (there was an integrity test, a math test, and a battery that comprised cognitive ability, personality, and situational judgement tests) mattered: if applicants perceived the tests to be weakly related to the job, they felt greater invasion of privacy. Comer and Buda (1996) found that employees who were aware that drug tests can neither assess impairment to work performance nor address workplace drug usage were more likely to perceive such tests as being invasive. A study by Nielsen and Kuhn (2009) yielded similar results: participants felt that using credit history in selection procedures was not related to the job, invaded their privacy, and negatively affected their fairness perception of the procedure. Finally, Woodman and colleagues (1982) found that employees reacted more favorably when personal data were used for relevant organizational decision making (e.g., hiring decisions, promotion, job assignments, and layoffs) but not when the data were used for other purposes such as research, charity drives, and auditing.

Emerging methods of selection such as online testing (Bauer et al., 2006), digital interviews (Langer, König, & Krause, 2017), and social media (Stoughton, Thompson, &

Meade, 2015) are also perceived by applicants to be invasive; these perceptions of invasiveness are attenuated to a degree if applicants perceive that providing information through those methods is advantageous in terms of securing the job—consistent with early theorizing (E. F. Stone & Stone, 1990) and empirical findings (Fusilier & Hoyer, 1980; Tolchinsky, McCuddy, Adams, Ganster, Woodman, & Fromkin, 1981) of the instrumental value of these methods. Awareness of monitoring and potential privacy invasion can also modify applicants' behavior. For instance, Roulin (2014) found that participants were less likely to make faux pas postings (e.g., potentially inappropriate content such as pictures of drinking alcohol, pictures with sexual props, or comments on illegal drug use) on social networking websites when they were informed that a high proportion of employers use such websites for selection and that employers' strategies could invade applicants' privacy (e.g., asking for applicants' social media log-ins during an interview or asking applicants to "friend" human resources managers). Overall, though, employees are seemingly pragmatic regarding (or resigned to) the use of such selection methods: surveys of employees in the United Kingdom and Australia reveal that a sizable minority (approximately 40%) acknowledge the legitimacy of employers' rights to collect and use applicants' online information for hiring (McDonald, Thompson, & O'Connor, 2016).

Beyond employee selection, information collected in a number of other contexts is perceived to be invasive. These include organizational email policies (Paschal, Stone, & Stone-Romero, 2009), the human resource information system (Eddy, Stone, & Stone-Romero, 1999), and performance appraisal sessions where performance information is shared beyond the supervisor and subordinate (Mossholder, Giles, & Wesolowski, 1991). The advent of electronic performance monitoring has arguably enhanced perceptions of invasiveness. In a survey conducted across multiple organizations, participants reported that privacy infringements could occur if organizations did not have clear monitoring practices

(e.g., monitoring employees without informing them; 34%), monitored personal communications (e.g., outside the workplace, or via personal emails; 24%), did not have a clear rationale for monitoring (e.g., avoid monitoring to discriminate; 13%), utilized intrusive technologies (e.g., genetic screening for hiring, 11%), and monitored personal places (e.g., restrooms, breakrooms; 8%; M. W. Allen, Coopman, Hart, & Walker, 2007). These results were consistent with those from experimental and field studies and with findings from employee selection research. For electronically monitored participants, perceptions of invasiveness of privacy were lower if they believed that they could control the type of information, how it was collected, and the reasons for collecting it (i.e., if the information was job related; Alge, 2001). Similar results were observed for awareness monitoring systems (i.e., systems that are used to perform collaborative work in geographically distributed teams; Zweig & Webster, 2002) and location sensing technologies (i.e., devices relying usually on GPS, RFID, and other telecommunication technologies to provide real-time location tracking of employees; McNall & Stanton, 2011). The type of monitoring system used could also influence perceptions of privacy invasion, with computer monitoring seen to be least invasive, followed by visual surveillance (typically via video cameras) and finally eavesdropping (via telephonic equipment to track telephone discussions or messages on voicemail; McNall & Roch, 2007). Finally, participants reported lower privacy concerns when they anticipated that electronic monitoring of their behaviors would yield them financial gains (e.g., paying less rent on dorm rooms, paying lower car insurance premiums, and earning a bonus); conversely, their privacy concerns were greater if they perceived electronic monitoring to generate additional costs (Bolderdijk, Steg, & Postmes, 2013). This finding illustrates an empirical assessment of the privacy calculus.

Disclosure of medical and health-related information, especially involving changes in employees' health conditions, is another critical area of sensitivity. For example, employers

reported being circumspect about discussing information on work-related injuries with employees on account of privacy concerns; these concerns hindered the development of a shared understanding with injured employees and devising effective return-to-work plans (Stergiou-Kita, Mansfield, Daiter, & Colantonio, 2015). Similar to concerns of disclosure between employees and employers, disclosure between coworkers involves subtleties. For example, only employees who possessed strong interpersonal trust relationships with colleagues who were diagnosed with cancer were able to discuss their treatment and emotional well-being with them; conversely, those with weak interpersonal trust relationships learned about the focal employee's cancer diagnosis only from a third party (Wittenberg-Lyles & Villagran, 2006). Along similar lines, treatments involving assisted reproductive technologies invoked significant workplace disclosure concerns due to the intensely intimate nature of such procedures (van den Akker, Payne, & Lewis, 2017).

Information privacy: Assessment of empirical findings and connections to related work in other disciplines. Most studies discussed above assess perceptions of invasion of privacy. The specific measures used to assess the construct of invasion of privacy differ widely. We identified more than 10 different scales to measure the construct. On the basis of their setting (e.g., employee selection, electronic performance monitoring), scholars generate unique items to assess the construct, and they provide limited information on scale validation. Consequently, there is little convergence across these measures.

The lack of detail on scale validation procedures is also present for broader measures of information privacy. An exception is the work of Alge and colleagues (2006), who provide detailed scale validation information in operationalizing information privacy (see H. J. Smith et al., 1996, for a related measure from the information systems perspective). They identify three dimensions of information privacy: information gathering control (employees' perceived control over the collection and storage of personal information by the

organization), information handling control (employees' perceived control over the organization's use and dissemination of personal information that has already been collected), and perceived legitimacy (employees' beliefs that the organization's gathering and handling of personal information has "violated [their] expectations of legitimate conduct, given the situation"; Alge et al., 2006: 223). One concern with this third dimension of perceived legitimacy is that the items to assess it seemingly focus on perceptions of invasiveness (e.g., "I feel that my organization's information policies and practices are an invasion of privacy"; Alge et al., 2006: 224) rather than, as intended, perceived legitimacy. On that note, similar items have explicitly been used elsewhere to assess perceptions of invasiveness (e.g., Alge, 2001; Eddy et al., 1999). This results in an unnecessary conflation of the constructs of perceived legitimacy (with its connection to the purpose of information collection) and perceived invasion of privacy (with its connection to employees' experience of the loss of their information privacy).

Related to this, because information privacy encompasses different elements (purpose, collection, use, etc.), perceptions of invasiveness can differ across these elements. Evidence suggests that there is a hierarchy of such information privacy concerns across multiple countries, with secondary use of data being the top concern (Milberg, Burke, Smith, & Kallman, 1995). For all these reasons, assessing perceptions of invasiveness using a common set of construct-valid items (e.g., Alge, 2001), and assessing perceptions of specific elements of information privacy, is essential for future research. Furthermore, given that invasion of privacy is the most widely assessed construct in the organizational privacy literature, a meta-analysis that considers its antecedents and outcomes would be timely.

On a different note, although organizational research has begun to examine privacy issues on emerging platforms (e.g., social media), scholarship in this area is still lagging and could find inspiration from information systems research where the topic is more widely

examined. For instance, Suen (2018) found that Facebook users who perceived privacy violations from potential employers (who had used Facebook to screen applicants) had lower perceptions of procedural justice and a greater likelihood of withdrawing from the selection process. Examining whether similar concerns are likely to surface for other platforms (e.g., LinkedIn) that are increasingly used by recruiters will be helpful.

Work environment privacy: Summary of findings. In contrast with research on information privacy (which primarily considers the construct of invasiveness), work environment privacy encompasses privacy related to the senses: for instance, visual, acoustic, personal space, and olfactory. Sundstrom (1986) defined visual privacy as being free from optical stimuli and undesired notice by others. Similarly, acoustic privacy (also referred to as auditory or sound privacy) is considered as isolation from noise (Sundstrom, 1986)—that is, the extent to which workspaces are perceived to be private with regard to speech or verbal conversations (Paschal et al., 2009). Personal space privacy is the physical area around an employee into which others cannot intrude without causing discomfort (Ashkanasy, Ayoko, & Jehn, 2014). Olfactory privacy, rarely defined explicitly, has been alluded to as the absence of bad smells (Dul, Ceylan, & Jaspers, 2011). The preponderance of organizational research on work environment privacy is on office layouts, where visual, acoustic, and space privacy are intertwined (Sundstrom et al., 1980). As such, we discuss these three aspects together.

There are three broad categories of office layouts: closed (walled) offices, cubicles, and open workspaces (Khazanchi, Sprinkle, Masterson, & Tong, 2018). These three categories represent differences in the levels of barriers and enclosures from high (closed offices) to low (open-plan workspaces; Ashkanasy et al., 2014; Elsbach & Pratt, 2007). Despite almost four decades of research on barriers and enclosures, controversies persist regarding their purported advantages (e.g., allow fewer interruptions, signal helpful status differences, allow more confidential and meaningful interactions) and their purported

disadvantages (e.g., inhibit interpersonal communication and collaboration, signal unhelpful status and power differences; see Elsbach & Pratt, 2007, for a review). Findings related to privacy, however, are less equivocal.

In cubicles and open workspaces, employees are in closer physical proximity. This workspace feature is objectively assessed as spatial density (i.e., the average space, in square feet or other metrics, available to each employee), and is subjectively assessed as crowding (i.e., employees' perceptions that their workspace is crowded; May, Oldham, & Rathert, 2005; Sundstrom et al., 1980). Higher spatial density and greater crowding are excessively stimulating to employees—employees find such overstimulation undesirable and a form of information overload—and this influences their adverse privacy reactions (Greenberg & Firestone, 1977; Oldham, 1988; Oldham & Rotchford, 1983). For instance, almost half a century ago, a study of 600 Canadian government employees revealed that participants working in cubicles perceived low personal space and acoustic privacy; these adverse reactions were attributed to employees perceiving a loss of control over their work environment (McCarrey, Peterson, Edwards, & von Kulmiz, 1974). Across three studies, Sundstrom and colleagues (1980) reported similar results: employees working in workspaces that were more accessible to others (without partitions or walls, in closer proximity to coworkers, visible to supervisors) reported lower visual, acoustic, and personal space privacy.

Beyond these correlational results, in a quasi-experimental study that tracked employees' move from a closed office to an open-plan office, employees reported lower levels of visual, personal space, and acoustic privacy associated with the move (Zalesny & Farace, 1987). Recent work from environmental psychology and real estate research reports convergent findings linked to different aspects of office layouts. Compared to working in closed offices, employees working in open-plan offices report lower levels of visual, personal space, and acoustic privacy (e.g., Haapakangas, Hongisto, Varjo, & Lahtinen, 2018; Kim &

De Dear, 2013). There are also broader concerns regarding employees' work environment privacy. Privacy was a key managerial concern involving workplace discipline and punishment (Butterfield, Trevino, & Ball, 1996): for instance, Brett, Atwater, and Waldman (2005) found that disciplining employees in private spaces was related to less employee defensiveness and fewer negative workplace outcomes such as a deteriorating relationship with one's supervisor.

Work environment privacy: Assessment of empirical findings and connections to related work in other disciplines. Organizational research has largely investigated the impact of office layouts. However, there are additional features of the work environment (e.g., window and door positions, lighting, use and positioning of plants) that are salient for employees' privacy and that are examined in environmental psychology research. For instance, locations of windows and doors were related to work environment privacy, which influenced how participants decided to position workstations as well as armchairs for working and relaxing (Wang & Boubekri, 2010). Office plants could serve as partitions and regulate traffic around an employee's workspace and could thereby improve work environment privacy perceptions; two studies, however, did not find evidence that office plants improved privacy perceptions (A. Smith & Pitt, 2009; A. Smith, Tucker, & Pitt, 2011).

Another trend in organizations is that employees can choose work stations in different locations (multiple times through the day if necessary) according to the task at hand rather than being assigned to a permanent space (Appel-Meulenbroek, Groenen, & Janssen, 2011; Brunia, De Been, & van der Voordt, 2016). Along with the increase in mobile, knowledge workers, this trend has resulted in low occupancy of assigned spaces, and for this reason organizations have attempted to maximize the utility of workspaces (Appel-Meulenbroek et al., 2011). Real estate research, which has explored such questions on activity-based or flexi-concept offices, reveals that workstations were not always used as intended because people

chose workspaces according to their personal preferences rather than functional demands (Appel-Meulenbroek et al., 2011). Furthermore, employees working in premises with activity-based designs tended to report that such designs did not afford sufficient levels of work environment privacy (Appel-Meulenbroek et al., 2011; Brunia et al., 2016; De Been & Beijer, 2014). Such emerging forms of employees' workspaces, including related ones such as coworking spaces, are likely to become ever more salient with the ubiquity of mobile technology, proliferation of flexible work arrangements, and an economic model that focuses on a "shared economy" (Bouncken & Reuschl, 2018)—and thereby need to be investigated in organizational research.

Findings Related to Individual Factors and Employees' Privacy Calculus

Individual differences. As discussed, the privacy calculus reflects an employee's decisions regarding disclosure of information based on associated risks and benefits. The notion of privacy preferences considers how people differ in this decision-making process. Across surveys conducted over 30 years, Westin identified three broad segments of how the general public varied in their privacy preferences (Westin, 2003; see also Kumaraguru & Cranor, 2005; Woodruff, Pihur, Consolvo, Schmidt, Brandimarte, & Acquisiti, 2014). "Privacy fundamentalists" (about 25% of the population) were dogmatic about not exchanging their privacy for any possible benefits and desired complete protections, "privacy unconcerned" (about 20% of the population) willingly disclosed their information and were indifferent regarding its protection, and "privacy pragmatists" (about 55% of the population) were concerned about privacy and the potential of misuse of their data and weighed the benefits that providing their data offered in relation to the intrusion involved in collecting it (Francis & Francis, 2017; Kumaraguru & Cranor, 2005). Left unaddressed by Westin was the possibility, particularly germane in our social media age, of a potential fourth segment of the population—perhaps labeled "disclosure fundamentalists"—which, motivated by the need for

social recognition (Igo, 2018), goes beyond being unconcerned with privacy violations and instead actively seeks out disclosure.

Building on Westin's work, which primarily focused on *consumers'* privacy preferences, and which represented a broad-level segmentation of privacy preferences, Stone and colleagues devised an organizational analogue of such privacy preferences, which they labeled as privacy values (i.e., the extent to which employees valued having control over their information vs. letting the organization control it; E. F. Stone, Gueutal, Gardner, & McClure, 1983). They observed that participants who had strong privacy values perceived that they had lower control over their information and were dissatisfied about this lack of control. Subsequently, D. L. Stone (1986) observed that employees' privacy values influenced their perceptions of invasion of privacy; those who had stronger privacy values viewed restrictive policies related to email use in organizations (e.g., ban against personal email use) to be more invasive (Paschal et al., 2009).

Oldham (1988) considered a similar individual differences variable in the context of work environment privacy. Oldham observed that employees with a high need for privacy (a person's "need for physical isolation from stimuli": 255) preferred office layouts that had partitions and afforded greater personal space. Taking this further, and aligning with Altman's (1975) view of privacy as a dynamic boundary management process, Haans, Kaiser, and de Kort (2007) developed a 25-item measure of the need for privacy, which assessed employees' behaviors to withdraw from various social interactions in their workplace (e.g., "I wear headphones when I am at the office"; "I take my break at other times than my colleagues").

Beyond the limited research on employees' privacy needs and preferences, scholars have identified some individual differences and their connections to a specific element of the privacy calculus: perceptions of invasiveness. In the studies cited above regarding the type of

questions posed to participants, Rosenbaum (1973) observed that participants who were high on sociability and dominance (facets of extraversion; DeYoung, Quilty, & Peterson, 2007) and emotional stability had lower perceptions of invasiveness. In a similar vein, Mael et al. (1996) observed that participants who were higher on self-disclosing propensity (i.e., people who have greater tendency to provide personal information about themselves) and had a lower need for privacy (i.e., people who prefer less privacy across different domains of their life) found fewer items to be invasive of their privacy. In a sample of Turkish students, Bilgiç and Acarlar (2010) reported that participants' goal orientation influenced their perceptions of invasiveness related to the selection method. Specifically, compared to performance prove–oriented participants, learning-oriented participants perceived greater invasion of privacy from personality tests, presumably because such tests do not have "correct" responses and therefore do not provide an opportunity to improve.

For existing employees rather than job applicants, perceptions of invasiveness typically focus on ongoing monitoring methods. Alder, Schminke, and Noel (2007) considered the role of employees' ethical orientation, an ethical predisposition that consists of two independent dimensions of formalism (which focuses on the morality of the actions regardless of the outcomes and is characterized by traits such as being principled and trustworthy) and utilitarianism (which focuses on morality of the outcomes regardless of the actions and is characterized by traits such as being resourceful and results oriented). They found that employees with a formalist orientation perceived programs such as background tests, drug testing, and Internet monitoring as an invasion of their privacy.

In subsequent work, Alder, Schminke, Noel, and Kuenzi observed that the negative relationship between perceptions of privacy invasion and a number of cognitive-affective work outcomes (perceptions of organizational trust, supervisor trust, organizational support, and fairness of such monitoring practices) was stronger for employees with a low (vs. high)

formalist orientation because they "are less concerned with adherence to and enforcement of rules and will therefore be less accepting of monitoring rules and associated invasion of privacy" (2008: 488). Relatedly, Winter, Stylianou and Giacalone (2004) reported that people who scored higher in Machiavellianism were more accepting of behaviors that violated others' privacy (e.g., using medical data for a purpose other than for which it was collected). In terms of other dispositional variables, Snyder (2010) observed that employees with higher dispositional paranoia (which reflects a lower propensity to trust) reported greater concerns of invasiveness related to email privacy.

Demographics: Sex, age, and race/ethnicity. Investigations of sex differences in privacy are guided by two distinct reasons that yield opposite predictions: (a) physical security concerns are less prominent for men than women, so men should prefer privacy to a greater extent than women; and (b) women prefer to limit access to close others such as friends and family, so women should prefer privacy to a greater extent than men (Pedersen, 1987). Although there is no clear pattern of such sex differences in privacy preferences (Pedersen, 1987, 1999), some research has considered sex differences in perceptions of invasiveness. In Rosenbaum's (1973) study (discussed above), women (vs. men) found items related to their employment history, interests and hobbies, and "social adjustment" (e.g., criminal record, drug use, relationships with work colleagues) to be more invasive; conversely, men found items related to their financial history to be more invasive. Similarly, in one sample of the study by Mael and colleagues (1996) discussed above, women found biodata items to be more invasive than men did; there were no differences in the second sample. Connerley, Mael, and Morath (1999) observed that compared to women, men preferred to know more potentially invasive information about prospective coworkers. Similarly, female computer professionals in Taiwan reported higher self-efficacy than men in protecting information privacy of customers (e.g., improper use, accidental public disclosure)

and in nonacquisition of private information (e.g., resist acquiring and using private information before being authorized to do so; Kuo, Lin, & Hsu, 2007).

Few studies have considered other demographic characteristics. Although there are competing explanations for whether older employees would be less (i.e., lower impression management considerations) or more (i.e., higher privacy considerations) concerned about invasiveness, results revealed that age was not related to perceptions of invasiveness for biodata items (Mael et al., 1996). For work environment privacy, too, results from a sample of Finnish employees revealed that there were no differences in work environment (i.e., office layouts) preferences in terms of privacy across employees of different age groups (Rothe, Lindholm, Hyvönen & Nenonen, 2012). Haans et al. (2007) reported similar results for Dutch bank employees. In terms of race, compared to ethnic minorities, White participants found fewer biodata items to be invasive (Mael et al., 1996) and preferred to know more potentially invasive information about their prospective coworkers (Connerley et al., 1999).

Assessment of empirical findings and connections to related work in other disciplines. Information systems research has identified two additional segments that reflect people's privacy preferences that were not identified by Westin. These include "information sellers" (those people who are motivated to sell personal information for financial gain or savings) and "convenience seekers" (those people who are motivated to disclose information primarily because it is convenient and helps them save time; Hann, Hui, Lee, & Png, 2007; Hui, Tan, & Goh, 2006; Krasnova, Spiekermann, Koroleva, & Hildebrand, 2010). Put simply, the benefits element of the privacy calculus is more nuanced than is currently documented. Considering the benefits of information disclosure more broadly, another potentially important benefit, largely unstudied in organizational research but alluded to in historical as well as information systems research on privacy (e.g., Hui et al., 2006; Igo, 2018), is social

approval and recognition. This perspective suggests that employees are motivated not only to be let alone but also to be known, not only to diminish exposure but also to heighten disclosure, not only to prevent intrusion but also to promote visibility, and not only by the fear of being watched but also by the fear that nobody cares enough to watch (Igo, 2018). Organizational research on the "benefits" portion of the privacy calculus could thus profit from studying not just the professional necessity of but also the social recognition or approval accruing from disclosure (Hui et al., 2006; Igo, 2018). In addition, the relative importance of risks and benefits on the set of employee cognitive-affective and/or behavioral outcomes should be examined in a comprehensive manner. For instance, following the principle of "bad is stronger than good" (Baumeister, Bratslavsky, Finkenauer, & Vohs, 2001), are perceived risks more important than perceived benefits? Another neglected issue involves the interplay of risks and benefits vis-à-vis outcomes. For instance, the impact of risks on employee outcomes may depend on the level of benefits and vice versa (i.e., the two may interact statistically). In addition, the levels of risks and benefits can be in alignment such that both levels are high or both levels are low; yet there is little research on whether employee outcomes differ across these two cases.

There is also surprisingly little organizational research on Big Five personality traits and privacy. However, the broader literature on workplace technology, including work on electronic performance monitoring, offers insight. For instance, using an experimental design, Zweig and Webster (2003) found that introverts (vs. extraverts) exhibited a stronger negative relationship between perceptions of privacy invasion and fairness. Maltseva and Lutz (2018) found that participants higher on conscientiousness and lower on emotional stability were more likely to "self-quantify" (i.e., use body sensors and mobile applications to track fitness activities, work performance, and leisure experiences). Contrary to expectations, those with higher privacy concerns were more likely to self-quantify; however, the researchers did not

directly investigate relationships between privacy concerns and the Big Five personality traits.

In a similar vein, the technology literature (as opposed to the organizational literature) has examined demographic differences in privacy in social media and online settings. For instance, Hargittai and Litt (2013) reported that when contemplating job search, compared to men, women were more likely to initiate actions to guard their privacy online (e.g., by changing settings or the content of their online profiles). Hajli and Lin (2016) reported that women (American students) were more cognizant of the information they shared on social networking sites (SNSs) and that their privacy risk perceptions regarding information collection on these sites adversely influenced their information sharing. In accordance with these findings, a recent meta-analytic study by Tifferet (2019) on gender differences in privacy tendencies on SNSs showed that women tended to display greater privacy concerns, were more likely to activate privacy settings and "untag" themselves from photographs on SNSs, and were less likely to disclose personal information on their SNS profiles. Risk assessment (and, thus, the privacy calculus) may also be involved in such strategies. A study on women who identified as sexual minorities found that they weighed role risk (impact on employment status, professional image, etc.) and relational risk (impact on quality of interpersonal relationships with peers and clients) before deciding whether and how to reveal their minority sexual identity at the workplace (Helens-Hart, 2017).

There is also some evidence that perceptions and use of social media vary across different ethnicities and that these perceptions subsequently influence privacy. Because of the prospect of future employers checking social media sites, compared to other ethnicities (i.e., African Americans, Asian American, and Hispanics), Whites were far more likely to adjust the privacy settings of their sites (possibly guided by impression-management motives; Hargittai & Litt, 2013). Collectively, these findings suggest that there is an opportunity to

better clarify differences in privacy perceptions based on demographic characteristics. Furthermore, the interplay of demographic characteristics and personality traits also deserves examination. This includes the issue of whether personality traits mediate the effects of demographic characteristics on perceptions of invasiveness.

Findings Related to Privacy Contexts and Employee Outcomes

We detail findings related to privacy contexts and employees' cognitive-affective and behavioral outcomes in the online supplement.

Research Directions Based on the Current State of Research on Privacy at Work

In the section above (and in the online supplemental material), for each element of the stakeholders' privacy calculus model, we have outlined our assessment of the state of organizational privacy research and have offered avenues for future research while drawing on empirical findings from other disciplines (e.g., marketing, information systems, environmental psychology). On the basis of this discussion, for each aspect of the stakeholders' privacy calculus model, we include an extensive list of questions for future research (see Table 1).

TWO BROAD DOMAINS FOR FUTURE RESEARCH

In the previous section, we identified a number of future research ideas (summarized in Table 1) connected to each specific link outlined in the stakeholders' privacy calculus model. Because the privacy calculus is the conceptual fulcrum of this model, to better understand its mechanics, we now identify two broad domains for future research: (1) how the privacy calculus informs different organizational practices, and (2) how various factors influence employees' privacy-related preferences, attitudes, and behaviors. Investigating questions in these domains will help better understand employees' privacy-related decisions.

How the Privacy Calculus Informs Organizational Practices

The privacy calculus is a conceptual tool to understand employees' privacy decisions. Developing a scale to assess the privacy calculus will help not only to better understand the neglected interplay between risks and benefits but also to further understand a range of decisions with privacy implications: disclosure of information related to employment history, academic background, health information, sexual orientation, and religious beliefs, among others. Admittedly, developing such a scale is complex; for instance, job applicants' estimations of risks and benefits could differ across settings where information is directly sought (e.g., face-to-face interviews) or indirectly gleaned (e.g., social media). Research on the work-family interface, which has developed measures of work-life trade-offs (a calculus-based construct) across domains could provide guidance (see, e.g., Dahm, Kim, & Glomb, 2019). An alternative perspective, adapted from the judgment and decision-making literature on risk attitudes (e.g., Weber, Blais, & Bettz, 2002), would emphasize a specific list of privacy-relevant occurrences and would assess respondents' perceptions of the amount of risk as well as the expected benefit from each such occurrence. This would permit an examination of whether risk and benefit judgments are characterized more by differences across domains (e.g., employee selection vs. performance monitoring) or by individual differences—an issue of some contention in the judgment and decision-making literature (Highhouse, Nye, Zhang, & Rada, 2017).

More generally, similar to research that assesses the value that consumers place on their data, organizational research could examine employees' privacy valuations (e.g., Acquisti, John, & Loewenstein, 2013; Hann et al., 2007). For instance, Hann and colleagues (2007) examined the tradeoffs participants made between the privacy protections offered by websites and the potential benefits of personal information disclosure to these websites; they observed that American participants assigned a value of about $30 to $45 for protection against errors, improper access, and secondary use of personal information. Quantifying such

valuations could similarly provide a different perspective on employees' privacy-related decisions that could aid organizations when designing systems geared toward information collection (e.g., web-based application blanks).

Existing empirical assessments of the privacy calculus are largely from experimental studies from marketing and information systems research, which have provided insight on consumers' privacy decisions (e.g., Adjerid, Peer, & Acquisti, 2018). As we discuss below, multiple situations in the employment relationship—using online job boards, using social media for hiring, conducting 360-degree feedback, among others—lend themselves to similar explorations to better understand job applicants' and employees' privacy decisions. To begin with, employees' decision-making biases and their associated consequences offer many research avenues. For instance, job applicants' "present bias" (a preference to seek instant gains such as making a favorable impression on a recruiter and securing the job) and their subsequent information disclosure could pose longer-term consequences that may be inadvertently discounted (Acquisti, 2004). Similarly, although opt-out systems (implied consent) generally increase retirement savings compared to opt-in systems (explicit consent; Beshears, Choi, Laibson, & Madrian, 2009), the use of defaults in other aspects of employment such as web-based application blanks and computerized performance appraisal systems could result in greater information disclosure and associated concerns of invasiveness.

Along similar lines, experimental work has revealed that consumers are more likely to disclose intrusive information when privacy cues were dampened (e.g., when websites looked unprofessional due to spelling errors and bad design as opposed to when websites looked professional), and such work suggests that "consumers will be especially forthcoming with information when sensitive questions are asked informally" (John, Acquisti, & Loewenstein, 2010: 868). This finding has implications for a number of employment contexts—web-based

application blanks, e-recruitment, and using the Internet for selection decisions (e.g., Davison, Maraist, Hamilton, & Bing, 2012)—where privacy cues can be similarly manipulated to influence job applicants' information disclosure. Relatedly, participants were more likely to disclose information and exhibit lower impression management in a clinical interview if they thought they were interacting with a computer rather than a human operator (Lucas, Gratch, King, & Morency, 2014). It is pertinent to investigate whether newer employee selection methods such as virtual employment interviews and use of business games for assessment (i.e., "gamification"; Landers, 2015; Ryan & Ployhart, 2014) yield similar results. The findings are also potentially relevant for traditional employee selection methods such as face-to-face interviews: disclosure levels (and associated privacy concerns) could be higher in unstructured interviews versus structured interviews. Thus, in addition to the lower validity of unstructured interviews compared to structured interviews (e.g., Huffcutt & Arthur, 1994), unstructured interviews may also pose greater risks of invasiveness.

Privacy-Related Preferences, Attitudes, and Behaviors

Central to understanding how employees make privacy-related decisions is to learn more about their privacy preferences. Assessments of privacy preferences, however, are problematic: people's privacy preferences are often incongruent with their privacy-related behaviors. People may assert that they desire privacy, but this may not be borne out in their (disclosure) behaviors—a phenomenon labelled as the privacy paradox (Norberg, Horne, & Horne, 2007). Acquisti and colleagues (2015) note that it is thus unproductive to pinpoint exact values that people assign to privacy and that measures of privacy preferences are questionable.

In that vein, Hoofnagle and Urban (2014) have criticized Westin's classification of privacy preferences (i.e., fundamentalists, unconcerned, and pragmatists), contending that his assessment conflated the knowledge people (consumers, in Westin's studies) possessed about

protecting their privacy with their intent to do so. That is, people may not be sufficiently knowledgeable regarding the protections afforded to them, and rather than being unconcerned or pragmatists, they may simply be uninformed and mistaken about their preferences (Francis & Francis, 2017). In light of these arguments, a clearer understanding of employees' knowledge about the privacy protections to which they are legally entitled, particularly in light of notable regulatory changes such as the EU's GDPR, is essential.

Furthermore, notwithstanding the concerns voiced by Acquisti et al. (2015) regarding assessing privacy preferences, assessments of privacy values (a similar construct) have been fruitfully employed in organizational research (e.g., E. F. Stone et al., 1983). Organizational research has also navigated through other preferences of employees, such as their work values, where there are similar distinctions between espoused behavior and enacted behavior (Meglino & Ravlin, 1998). It is thus probable that within the context of the employment relationship, a clearer assessment of employees' privacy preferences is more feasible.

Related to this, privacy intrusions occur when people believe that social norms regarding the information collection and information use are violated; conversely, the upholding of these norms reflects "contextual integrity" (Nissenbaum, 2004). The notion of contextual integrity could be considered analogous to parallel constructs of "fit" and "congruence," on which there is ample organizational research (e.g., Kristof-Brown & Guay, 2011) and for which theoretical models (Edwards, 2008) and data-analytic approaches (Edwards, 2007) are relatively well-developed. Examining linkages between employees' privacy values and organizational norms related to workplace privacy could help identify employment settings when contextual integrity is upheld.

How do employees view organizational actions to elicit greater control over their information or their work environment? Are organizational actions to potentially elicit greater information disclosure viewed to be in accordance with contextual norms or an infringement

of those norms? Understanding employees' causal attributions of such organizational actions and whether they reflect contextual integrity would provide insight. This is relevant because the broader human resources literature has shown that employees' attributions of human resources practices influences downstream consequences such as employees' attitudes and work behaviors (Nishii, Lepak, & Schneider, 2008).

Conversely, how would organizations view employees' reticence to provide the information sought? Would organizations view employees' behaviors as tenable privacy-protection behaviors or as attempts to withhold information (i.e., counterproductive work behaviors; see Martinko, Gundlach, & Douglas, 2002)? Similar concerns could surface in a team setting. For instance, norms of "keeping information within the team" may conflict with requirements to disclose information and may be construed as knowledge hiding (Connelly, Zweig, Webster, & Trougakos, 2012). Thus, attribution theory could provide a useful lens to understand how the information interfaces between employees and their organization, and between employees and their team, play out (see Martinko, Harvey, & Dasborough, 2011).

Because of the increasing trend of alternate work arrangements, another interface that has emerged is the fusion of employees' information and their workspace. Increasingly, employees now work from locations different from their primary place of employment (i.e., telework), including their homes or coworking spaces, and communicate with their colleagues using technology (Bouncken & Reuschl, 2018; Spivack, Askay, & Rogelberg, 2009). Furthermore, because of location sensing technologies, employees' work environments themselves are sources of data that provide information on employees' productivity and counterproductivity (see Tomczak, Lanzo, & Aguinis, 2018). Put simply, employees' workspace itself represents a form of data now. This points to an emerging entanglement of privacy contexts: information privacy and work environment privacy are increasingly enmeshed. Assessing the implications of these trends—whether they increase

perceptions of invasiveness, exacerbate privacy fatigue, result in different coping strategies—and identifying the unique and additive effects of the privacy contexts on employees' work outcomes are areas for future research (see online supplement for related findings).

Finally, we note that the putative "outcomes" of the employee privacy calculus—employee behavioral and cognitive-affective "reactions"—may also serve as antecedents to the privacy calculus: in other words, the relationship may be reciprocal. For instance, perhaps employees find electronic performance monitoring more invasive if they are not performing well than if they are (see Stanton, 2000). Arguments that employees should not fear surveillance if they have nothing to hide may be fallacious (see, e.g., Solove, 2011), but they may also suggest that employees' performance and job attitudes can influence their privacy calculus in addition to being influenced by it. Future research should therefore use research designs aimed at teasing apart causal direction (e.g., cross-lagged panel designs and designs that include instrumental variables; Antonakis, Bendahan, Jacquart, & Lalive, 2010).

Implications for Employees, Employers, and Policy Makers

We examined two major developments that are likely to have significant privacy implications for organizations and the employment relationship: technological trends and data privacy laws. Now, more than ever, technological innovations are transforming the way that organizations are structured, how they operate, and how they relate to their stakeholders (Cascio & Montealegre, 2016). According to a 2018 Deloitte Global Survey of more than 11,000 business and human resources leaders, more than 70% of respondents were convinced that trends in artificial intelligence, robotics, and automation were important or very important (D. Agarwal, Bersin, Lahiri, Schwartz, & Volini, 2018). In Table 2, we identify nine major emerging technologies that are being adopted in the workplace. For each technology, we outline the privacy implications for both employers and employees.

--See Table 2--

Although details may differ for each technology, overall the implications can be grouped into three areas: *collection* of data, *processing* of data, and data and network *access*. In terms of collection of data, many of the technologies involve collecting data in massive quantities, often unobtrusively (e.g., sensors embedded in a robot coworker) and in a continuous fashion (e.g., via mobile devices carried by employees). Employers will need to establish policies on the consent procedures, the actual data collection processes (how much data to collect, and when—i.e., only at the workplace, or also outside the workplace and after work hours—and where to collect it), and potential information disclosure. Employees will need to decide whether they are comfortable with the high level of monitoring that comes with the collection of such data and whether they are comfortable with ceding such data—some of which could be highly personal (e.g., heart rate and physical movements through the building)—to their employers.

In terms of processing of data, many of the technologies, especially those in artificial intelligence, involve sophisticated algorithms that analyze the massive quantities of data collected to discover patterns in prior activities and predict future behaviors. Because insights from such algorithms may be obtained at the group or organizational level (e.g., turnover rates), they may provide some measure of privacy to individual employees who contributed, wittingly or unwittingly, to the collective data input. There are potential instances, however, where insights pertaining to individual employees may emerge unbeknownst to them (e.g., health profile of an employee pieced together from various tracking devices).

The third area of data and network access relates to security concerns about such data (e.g., protection against hacking into networks containing sensitive data). This involves issues of control and access restrictions for employees not only to internal networks but also to external networks (e.g., Internet access) that may compromise organizations' internal systems (e.g., exposure to malware and viruses).

The enactment of data privacy laws in recent years, chief among them the EU's GDPR, has far-reaching implications. The implementation of the GDPR in May 2018, for instance, has been described variously as a milestone for the "sovereignty" of people over their digital lives (Waters, 2018) as well as the "mindfulness" that organizations will need to maintain in the treatment of personal data (Economist, 2018). In the online supplement, we discuss the GDPR in greater depth and outline recent regulatory changes in other countries.

Given the specific privacy interests of employees and employers, it is inevitable that some of these interests may conflict (i.e., organizations' need for information for employment-related decisions vs. employees' desire for control over their personal information). Although privacy laws may stipulate the specific rights to which stakeholders are entitled, interpretations of these rights may differ. In such instances, a conflict resolution model would help stakeholders reach an agreement without escalating matters to the court. Budd and Colvin provide a framework for resolving workplace conflicts that draws on three criteria: efficiency ("effective use of scarce resources"), equity ("fairness and justice") and voice ("ability to participate and affect decision making"; 2008: 466). Using these three criteria, the framework identifies a number of options—mediation, arbitration, appeal procedures, among others—that employers across unionized and nonunionized settings could fruitfully utilize for mutually beneficial privacy-related conflict resolution.

Conclusion

> *"It's a dangerous business, Frodo, going out of your door," he used to say. "You step into the Road, and if you don't keep your feet, there is no knowing where you might be swept off to." (Tolkien, 1954: 83)*

Whether one steps onto the information superhighway or onto a neighborhood street, privacy perils await. Arguments about privacy are, at their heart, arguments about nothing less than what it means to be a modern citizen (Igo, 2018)—and therefore a modern

employee. Notwithstanding many recent proclamations to the effect that privacy is "dead," we (like other privacy scholars; see, e.g., Igo, 2018) do not actually expect concerns about privacy to diminish, although we do expect the surface manifestations of such concerns to change as a result of changes in technology, culture, law, and the like. Stated differently, we expect the employee's privacy calculus, which forms the psychological hub of our stakeholders' privacy calculus model, to persist even as its specific antecedents change over time. We therefore believe our review serves as a road map that (1) catalogs existing landmarks in workplace privacy research and (2) illuminates the road ahead, both for researchers looking to make sense of and contribute to this voluminous literature and for employees and employers looking for practical guidance from this literature regarding how to navigate privacy dilemmas and contests.

References

Acquisti, A. 2004. Privacy in electronic commerce and the economics of immediate gratification. In J. Breese, J. Feigenbaum, & M. Seltzer (Eds.), *Proceedings of the Fifth ACM Electronic Commerce Conference:* 21-29. New York: Association for Computing Machinery.

Acquisti, A. 2009. Nudging privacy: The behavioral economics of personal information. *IEEE Security & Privacy,* 6: 82-85.

Acquisti, A., Brandimarte, L., & Loewenstein, G. 2015. Privacy and human behavior in the age of information. *Science,* 347: 509-514.

Acquisti, A., John, L. K., & Loewenstein, G. 2013. What is privacy worth? *The Journal of Legal Studies,* 42: 249-274.

Adams, M. 2017. Big Data and individual privacy in the age of the Internet of Things. *Technology Innovation Management Review,* 7: 12-24.

Adjerid, I., Peer, E., & Acquisti, A. 2018. Beyond the privacy paradox: Objective versus relative risk in privacy decision making. *MIS Quarterly,* 42: 465-488.

Agarwal, A. K., Gans, J. S., & Goldfarb, A. 2017. What to expect from artificial intelligence. *MIT Sloan Management Review,* 58(3): 23-27.

Agarwal, D., Bersin, J., Lahiri, G., Schwartz, J., & Volini, E. 2018. AI, robotics, and automation: Put humans in the loop. *2018 Deloitte Global Human Capital Trends.* Retrieved from https://www2.deloitte.com/insights/us/en/focus/human-capital-trends/2018/ai-robotics-intelligent-machines.html.

Agresti, W. W. 2010. The four forces shaping cybersecurity. *Computer,* 43: 101-104.

Akhtar, P., & Moore, P. 2016. The psychosocial impacts of technological change in contemporary workplaces, and trade union responses. *International Journal of Labour Research,* 8: 101-131.

Alder, G. S., Schminke, M., & Noel, T. W. 2007. The impact of individual ethics on reactions to potentially invasive HR practices. *Journal of Business Ethics,* 75: 201-214.

Alder, G. S., Schminke, M., Noel, T. W., & Kuenzi, M. 2008. Employee reactions to Internet monitoring: The moderating role of ethical orientation. *Journal of Business Ethics,* 80: 481-498.

Alge, B. J. 2001. Effects of computer surveillance on perceptions of privacy and procedural justice. *Journal of Applied Psychology,* 86: 797-804.

Alge, B. J., Ballinger, G. A., Tangirala, S., & Oakley, J. L. 2006. Information privacy in organizations: Empowering creative and extrarole performance. *Journal of Applied Psychology*, 91: 221-232.

Alge, B. J., & Hansen, S. D. 2014. Workplace monitoring and surveillance research since "1984": A review and agenda. In M. D. Coovert & L. F. Thompson (Eds.), *Frontiers of industrial/organizational psychology: The psychology of workplace technology:* 209-236. New York: Routledge/Psychology Press.

Allen, D. G., Mahto, R. V., & Otondo, R. F. 2007. Web-based recruitment: Effects of information, organizational brand, and attitudes toward a website on applicant attraction. *Journal of Applied Psychology*, 92: 1696-1708.

Allen, M. W., Coopman, S. J., Hart, J. L., & Walker, K. L. 2007. Workplace surveillance and managing privacy boundaries. *Management Communication Quarterly*, 21: 172-200.

Alterman, A. 2003. "A piece of yourself'': Ethical issues in biometric identification. *Ethics and Information Technology,*5: 139-150.

Altman, I. 1975. *The environment and social behavior.* Monterey, CA: Brooks/Cole.

Angrave, D., Charlwood, A., Kirkpatrick, I., Lawrence, M., & Stuart, M. 2016. HR and analytics: Why HR is set to fail the Big Data challenge. *Human Resource Management Journal*, 26: 1-11.

Antonakis, J., Bendahan, S., Jacquart, P., & Lalive, R. 2010. On making causal claims: A review and recommendations. *The Leadership Quarterly*, 21: 1086-1120.

Appel-Meulenbroek, R., Groenen, P., & Janssen, I. 2011. An end-user's perspective on activity-based office concepts. *Journal of Corporate Real Estate*, 13: 122-135.

Arthur, W., Jr., & Doverspike, D. 1997. Employment-related drug testing: Idiosyncratic characteristics and issues. *Public Personnel Management,* 26: 77-87.

Ashkanasy, N. M., Ayoko, O. B., & Jehn, K. A. 2014. Understanding the physical environment of work and employee behavior: An affective events perspective. *Journal of Organizational Behavior*, 35: 1169-1184.

Awolusi, I., Marks, E., & Hallowell, M. 2018. Wearable technology for personalized construction safety monitoring and trending: Review of applicable devices. *Automation in Construction,* 85: 96-106.

Bagdasarov, Z., Martin, A. A., & Buckley, M. R. in press. Working with robots: Organizational considerations. *Organizational Dynamics*. doi:10.1016/j.orgdyn.2018.09.002.

Ball, K., Daniel, E. M., & Stride, C. 2012. Dimensions of employee privacy: An empirical study. *Information Technology & People,* 25: 376-394.

Bauer, T. N., Truxillo, D. M., Tucker, J. S., Weathers, V., Bertolino, M., Erdogan, B., & Campion, M. A. 2006. Selection in the information age: The impact of privacy concerns and computer experience on applicant reactions. *Journal of Management,* 32: 601-621.

Baumeister, R. F., Bratslavsky, E., Finkenauer, C., & Vohs, K. D. 2001. Bad is stronger than good. *Review of General Psychology,* 5: 323-370.

BBC News. 2017. Is privacy dead in an online world? October 6. Retrieved from https://www.bbc.com/news/technology-41483723.

Bernstein, E. S. 2017. Making transparency transparent: The evolution of observation in management theory. *The Academy of Management Annals,* 11: 217-266.

Beshears, J., Choi, J. J., Laibson, D., & Madrian, B. C. 2009. The importance of default options for retirement saving outcomes: Evidence from the United States. In J. R. Brown, J. Liebman, & D. A. Wise (Eds.), *Social security policy in a changing environment:* 167-195. Chicago: University of Chicago Press.

Bhave, D. P. 2014. The invisible eye? Electronic performance monitoring and employee job performance. *Personnel Psychology,* 67: 605-635.

Bilgiç, R., & Acarlar, G. 2010. Fairness perceptions of selection instruments used in Turkey. *International Journal of Selection and Assessment,* 18: 208-214.

Bloustein, E. J. 1964. Privacy as an aspect of human dignity: An answer to Dean Prosser. *New York University Law Review,* 39: 962-1007.

Bolderdijk, J. W., Steg, L., & Postmes, T. 2013. Fostering support for work floor energy conservation policies: Accounting for privacy concerns. *Journal of Organizational Behavior,* 34: 195-210.

Bonaccio, S., & Dalal, R. S. 2010. Evaluating advisors: A policy-capturing study under conditions of complete and missing information. *Journal of Behavioral Decision Making,* 23: 227-249.

Bouncken, R., & Reuschl, B. 2018. Coworking-spaces: How a phenomenon of the sharing economy builds a novel trend for the workplace and for entrepreneurship. *Review of Managerial Science,* 12: 317-334.

Bowcott, O., & Rawlinson, K. 2017. Romanian whose messages were read by employer "had privacy breached." *The Guardian,* September 5. Retrieved from

https://www.theguardian.com/law/2017/sep/05/romanian-chat-messages-read-by-employer-had-privacy-breached-court-rules.

Brett, J. F., Atwater, L. E., & Waldman, D. A. 2005. Effective delivery of workplace discipline: Do women have to be more participatory than men? *Group & Organization Management,* 30: 487-513.

Brunia, S., De Been, I., & van der Voordt, T. J. M. 2016. Accommodating new ways of working: Lessons from best practices and worst cases. *Journal of Corporate Real Estate,* 18: 30-47.

Budd, J. W., & Bhave, D. 2008. Values, ideologies, and frames of reference in employment relations. In N. Bacon, P. Blyton, J. Fiorito, & E. Heery (Eds.), *The Sage handbook of industrial relations:* 92-112. London: Sage.

Budd, J. W., & Bhave, D. P. 2010. The employment relationship. In A. Wilkinson, N. Bacon, T. Redman, & S. Snell (Eds.), *SAGE handbook of human resource management:* 51-70. Thousand Oaks, CA: Sage.

Budd, J. W., & Colvin, A. J. 2008. Improved metrics for workplace dispute resolution procedures: Efficiency, equity, and voice. *Industrial Relations: A Journal of Economy and Society,* 47: 460-479.

Butterfield, K. D., Trevino, L. K., & Ball, G. A. 1996. Punishment from the manager's perspective: A grounded investigation and inductive model. *Academy of Management Journal,* 39: 1479-1512.

Carlson, D. S., & Kacmar, K. M. 1994. Learned helplessness as a predictor of employee outcomes: An applied model. *Human Resource Management Review,* 4: 235-256.

Cascio, W. F., & Montealegre, R. 2016. How technology is changing work and organizations. *Annual Review of Organizational Psychology and Organizational Behavior,* 3: 349-375.

Chamorro-Premuzic, T., Akhtar, R., Winsborough, D., & Sherman, R. A. 2017. The datafication of talent: How technology is advancing the science of human potential at work. *Current Opinion in Behavioral Sciences,* 18: 13-16.

Comer, D. R., & Buda, R. 1996. Drug testers versus nontesters: Human resources managers' perceptions and organizational characteristics. *Employee Responsibilities and Rights Journal,* 9: 131-148.

Connelly, C. E., Zweig, D., Webster, J., & Trougakos, J. P. 2012. Knowledge hiding in organizations. *Journal of Organizational Behavior,* 33: 64-88.

Connerley, M. L., Mael, F. A., & Morath, R. A. 1999. “Don’t ask—please tell”: Selection privacy from two perspectives. *Journal of Occupational and Organizational Psychology*, 72: 405-422.

Conteh, N. Y., & Schmick, P. J. 2016. Cybersecurity: Risks, vulnerabilities and countermeasures to prevent social engineering attacks. *International Journal of Advanced Computer Research,* 6: 31-38.

Culnan, M. J., & Armstrong, P. K. 1999. Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science,* 10*:* 104-115.

Culnan, M. J., Smith, H. J., & Bies, R. J. 1994. Law, privacy, and organizations: The corporate obsession to know versus the individual right not to be known. In S. B. Sitkin & R. J. Bies (Eds.), *The legalistic organization:* 190-211. Thousand Oaks, CA: Sage.

Dahm, P. C., Kim, Y., & Glomb, T. M. 2019. Leaning in and out: Work–life tradeoffs, self-conscious emotions, and life role satisfaction. *The Journal of Psychology,* 153: 478-506.

Dalal, R. S., Bhave, D. P., & Fiset, J. 2014. Within-person variability in job performance: A theoretical review and research agenda. *Journal of Management,* 40: 1396-1436.

Davies, S. G. 1997. Re-engineering the right to privacy: How privacy has been transformed from a right to a commodity. In P. E. Agre & M. Rotenberg (Eds.), *Technology and privacy: The new landscape:* 143-165. Cambridge, MA: MIT Press.

Davison, H. K., Maraist, C. C., Hamilton, R. H., & Bing, M. N. 2012. To screen or not to screen? Using the Internet for selection decisions. *Employee Responsibilities and Rights Journal,* 24: 1-21.

De Been, I., & Beijer, M. 2014. The influence of office type on satisfaction and perceived productivity support. *Journal of Facilities Management,* 12: 142-157.

DeYoung, C. G., Quilty, L. C., & Peterson, J. B. 2007. Between facets and domains: 10 aspects of the Big Five. *Journal of Personality and Social Psychology*, 93: 880-896.

Dillon, T. W., Hamilton, A. J., Thomas, D. S., & Usry, M. L. 2008. The importance of communicating workplace privacy policies. *Employee Responsibilities Rights Journal,* 20: 119-139.

Dinev, T., & Hart, P. 2006. An extended privacy calculus model for e-commerce transactions. *Information Systems Research,* 17: 61-80.

Dul, J., Ceylan, C., & Jaspers, F. 2011. Knowledge workers’ creativity and the role of the physical work environment. *Human Resource Management,* 50: 715-734.

Dwight, S. A., & Alliger, G. M. 1997. Reactions to overt integrity test items. *Educational and Psychological Measurement,* 57: 937-948.

Economist. 2018. The jobs of data hygiene: Europe's tough new data-protection law. April 5. Retrieved from https://www.economist.com/business/2018/04/05/europes-tough-new-data-protection-law.

Eddy, E. R., Stone, D. L., & Stone-Romero, E. 1999. The effects of information management policies on reactions to human resource information systems: An integration of privacy and procedural justice perspectives. *Personnel Psychology,* 52: 335-358.

Edwards, J. R. 2007. Polynomial regression and response surface methodology. In C. Ostroff & T. A. Judge (Eds.), *Perspectives on organizational fit:* 361-372. San Francisco: Jossey-Bass.

Edwards, J. R. 2008. Person–environment fit in organizations: An assessment of theoretical progress. *The Academy of Management Annals,* 2: 167-230.

Eisenhardt, K. M. 1989. Agency theory: An assessment and review. *Academy of Management Review,* 14: 57-74.

Elsbach, K. D., & Pratt, M. G. 2007. The physical environment in organizations. *The Academy of Management Annals,* 1: 181-224.

European Commission. 2018. *2018 reform of EU data protection rules*. Retrieved from https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en

Farrall, K. N. 2008. Global privacy in flux: Illuminating privacy across cultures in China and the U.S. *International Journal of Communication,* 2: 993-1030.

Fiesta, J. 1993. Liability for drug testing. *Nursing Management,* 24: 22-23.

Foucault, M. 1995. *Discipline and punish* (2nd ed.). New York: Random House.

Francis, L. P., & Francis, J. G. 2017. *Privacy: What everyone needs to know.* New York: Oxford University Press.

Fusilier, M. R., & Hoyer, W. D. 1980. Variables affecting perceptions of invasion of privacy in a personnel selection situation. *Journal of Applied Psychology,* 65: 623-626.

Gagné, M., & Bhave, D. P. 2011. Autonomy in the workplace: An essential ingredient to employee engagement and well-being in every culture. In V. Chirkov, R. Ryan, & K. Sheldon (Eds.), *Personal autonomy in cross-cultural context: Global perspective on the psychology of freedom and people's well-being:* 163-187. New York: Springer.

Gagné, M., & Deci, E. L. 2005. Self-determination theory and work motivation. *Journal of Organizational Behavior,* 26: 331-362.

Garba, A., Armarego, J., Murray, D., & Kenworthy, W. 2015. Review of the information security and privacy challenges in bring your own device (BYOD) environments. *Journal of Information Privacy and Security,* 11: 38-54.

Gavison, R. 1980. Privacy and the limits of law. *The Yale Law Journal,* 89: 421-471.

Gelfand, M. J., Nishii, L. H., & Raver, J. L. 2006. On the nature and importance of cultural tightness-looseness. *Journal of Applied Psychology,* 91: 1225-1244.

George, G., Haas, M., & Pentland, A. 2014. Big Data and management. *Academy of Management Journal,* 57: 321-326.

Greenberg, C. I., & Firestone, I. J. 1977. Compensatory responses to crowding: Effects of personal space intrusion and privacy reduction. *Journal of Personality and Social Psychology,* 35: 637-644.

Haans, A., Kaiser, F. G., & de Kort, Y. A. W. 2007. Privacy needs in office environments: Development of two behavior-based scales. *European Psychologist,* 12: 93-102.

Haapakangas, A., Hongisto, V., Varjo, J., & Lahtinen, M. 2018. Benefits of quiet workspaces in open-plan offices: Evidence from two office relocations. *Journal of Environmental Psychology,* 56: 63-75.

Hajli, N., & Lin, X. 2016. Exploring the security of information sharing on social networking sites: The role of perceived control of information. *Journal of Business Ethics,* 133: 111-123.

Hann, I. H., Hui, K. L., Lee, S. Y. T., & Png, I. P. 2007. Overcoming online information privacy concerns: An information-processing theory approach. *Journal of Management Information Systems,* 24: 13-42.

Hargittai, E., & Litt, E. 2013. New strategies for employment? Internet skills and online privacy practices during people's job search. *IEEE Security & Privacy,* 11: 38-45.

Hausknecht, J. P., Day, D. V., & Thomas, S. C. 2004. Applicant reactions to selection procedures: An updated model and meta-analysis. *Personnel Psychology,* 57: 639-683.

Helens-Hart, R. 2017. Females' (non)disclosure of minority sexual identities in the workplace from a communication privacy management perspective. *Communication Studies,* 68: 607-623.

Highhouse, S., Nye, C. D., Zhang, D. C., & Rada, T. B. 2017. Structure of the DOSPERT: Is there evidence for a general risk factor? *Journal of Behavioral Decision Making,* 30: 400-406.

Hofstede, G. 1980. Culture and organizations. *International Studies of Management & Organization,* 10(4): 15-41.

Hoofnagle, C. J., & Urban, J. M. 2014. Alan Westin's privacy homo economicus. *Wake Forest Law Review,* 49: 261-317.

The HR Specialist. 2018. How "private" email between managers can doom your organization in court. May: 3.

Hsu, C. L., & Lin, J. C. C. 2016. An empirical examination of consumer adoption of Internet of Things services: Network externalities and concern for information privacy perspectives. *Computers in Human Behavior,* 62: 516-527.

Huffcutt, A. I., & Arthur, W. 1994. Hunter and Hunter (1984) revisited: Interview validity for entry-level jobs. *Journal of Applied Psychology,* 79: 184-190.

Hui, K. L., Tan, B. C., & Goh, C. Y. 2006. Online information disclosure: Motivators and measurements. *ACM Transactions on Internet Technology (TOIT),* 6: 415-441.

Hulin, C. L. 1991. Adaptation, persistence, and commitment in organizations. In M. D. Dunnette & L. M. Hough (Eds.), *Handbook of industrial and organizational psychology* (2nd ed.), vol. 2: 445-505. Palo Alto, CA: Consulting Psychologists Press.

Hyman, J. 2017. A legal firing for fire chief's fiery posts. *Workforce*. Retrieved from https://www.workforce.com/2017/05/02/legal-firing-fire-chiefs-fiery-posts/.

Igo, S. E. 2018. *The known citizen.* Cambridge, MA: Harvard University Press.

Jain, A. K., Ross, A., & Pankanti, S. 2006. Biometrics: A tool for information security. *IEEE Transactions on Information Forensics and Security,* 1: 125-143.

John, L. K., Acquisti, A., & Loewenstein, G. 2010. Strangers on a plane: Context-dependent willingness to divulge sensitive information. *Journal of Consumer Research,* 37: 858-873.

Johns, G. 2006. The essential impact of context on organizational behavior. *Academy of Management Review,* 31*:* 386-408.

Jordan, M. I., & Mitchell, T. M. 2015. Machine learning: Trends, perspectives, and prospects. *Science,* 349: 255-260.

Kanfer, R., Frese, M., & Johnson, R. E. 2017. Motivation related to work: A century of progress. *Journal of Applied Psychology,* 102: 338-355.

Karren, R. J., & Zacharias, R. 2007. Integrity tests: Critical issues. *Human Resource Management Review,* 17: 221-234.

Kelly, K. D., & Hays, B. I. 2018. Biometric timeclocks may be a ticking time bomb for employers. *Employee Relations Law Journal,* 43: 39-42.

Khazanchi, S., Sprinkle, T. A., Masterson, S. S., & Tong, N. 2018. A spatial model of work relationships: The relationship-building and relationship-straining effects of workspace design. *Academy of Management Review,* 43: 590-609.

Kim, J., & de Dear, R. 2013. Workspace satisfaction: The privacy-communication trade-off in open-plan offices. *Journal of Environmental Psychology,* 36: 18-26.

Klein, K. J., & Zedeck, S. 2004. Introduction to the special section on theoretical models and conceptual analyses: Theory in applied psychology: Lessons (re) learned. *Journal of Applied Psychology,* 89: 931-933.

Klopfer, P. H., & Rubenstein, D. I. 1977. The concept privacy and its biological basis. *Journal of Social Issues,* 33: 52-65.

Krasnova, H., Spiekermann, S., Koroleva, K., & Hildebrand, T. 2010. Online social networks: Why we disclose. *Journal of Information Technology,* 25*:* 109-125.

Kristof-Brown, A. L., & Guay, R. P. 2011. Person-environment fit. In S. Zedeck (Ed.), *Handbook of industrial and organizational psychology:* 1-50. Washington, DC: American Psychological Association.

Kumaraguru, P., & Cranor, L. F. 2005. *Privacy indexes: A survey of Westin's studies*. ISRI Technical Report CMU-ISRI-05-138. Retrieved from http://reports-archive.adm.cs.cmu.edu/anon/isri2005/CMU-ISRI-05-138.pdf. Accessed July 3, 2006.

Kuo, F., Lin, C. S., & Hsu, M. 2007. Assessing gender differences in computer professionals' self-regulatory efficacy concerning information privacy practices. *Journal of Business Ethics,* 73: 145-160.

Landers, R. N. 2015. An introduction to game-based assessment: Frameworks for the measurement of knowledge, skills, abilities and other human characteristics using behaviors observed within videogames. *International Journal of Gaming and Computer-Mediated Simulations,* 7: iv-viii.

Langer, M., König, C. J., & Krause, K. 2017. Examining digital interviews for personnel selection: Applicant reactions and interviewer ratings. *International Journal of Selection and Assessment,* 25: 371-382.

Latham, G. P., & Pinder, C. C. 2005. Work motivation theory and research at the dawn of the twenty-first century. *Annual Review of Psychology,* 56: 485-516.

Laufer, R. S., & Wolfe, M. 1977. Privacy as a concept and a social issue: A multidimensional developmental theory. *Journal of Social Issues,* 33: 22-42.

Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. 2019. Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management,* 45: 13-24.

Linowes, D. F., & Spencer, R. C. 1997. Privacy in the workplace in perspective. *Human Resource Management Review,* 6: 165-181.

Lucas, G. M., Gratch, J., King, A., & Morency, L. P. 2014. It's only a computer: Virtual humans increase willingness to disclose. *Computers in Human Behavior,* 37: 94-100.

Mael, F. A., Connerley, M., & Morath, R. A. 1996. None of your business: Parameters of biodata invasiveness. *Personnel Psychology,* 49: 613-650.

Maltseva, K., & Lutz, C. 2018. A quantum of self: A study of self-quantification and self-disclosure. *Computers in Human Behavior,* 81: 102-114.

Margulis, S. T. 2003. Privacy as a social and behavioral concept. *Journal of Social Issues,* 59: 243-261.

Martinko, M. J., Gundlach, M. J., & Douglas, S. C. 2002. Toward an integrative theory of counterproductive workplace behavior: A causal reasoning perspective. *International Journal of Selection and Assessment,* 10: 36-50.

Martinko, M. J., Harvey, P., & Dasborough, M. T. 2011. Attribution theory in the organizational sciences: A case of unrealized potential. *Journal of Organizational Behavior,* 32: 144-149.

May, D. R., Oldham, G. R., & Rathert, C. 2005. Employee affective and behavioral reactions to the spatial density of physical work environments. *Human Resource Management,* 44: 21-33.

McAfee, A., & Brynjolfsson, E. 2012. Big Data: The management revolution. *Harvard Business Review,* 90(10): 60-68.

McCarrey, M. W., Peterson, L., Edwards, S., & von Kulmiz, P. 1974. Landscape office attitudes: Reflections of perceived degree of control over transactions with the environment. *Journal of Applied Psychology,* 59: 401-403.

McCarthy, J. M., Bauer, T. N., Truxillo, D. M., Anderson, N. R., Costa, A. C., & Ahmed, S. M. 2017. Applicant perspectives during selection: A review addressing "So what?," "What's new?," and "Where to next?" *Journal of Management,* 43: 1693-1725.

McDonald, P., Thompson, P., & O'Connor, P. 2016. Profiling employees online: Shifting public-private boundaries in organisational life. *Human Resource Management Journal,* 26: 541-556.

McNall, L. A., & Roch, S. G. 2007. Effects of electronic monitoring types on perceptions of procedural justice, interpersonal justice, and privacy. *Journal of Applied Social Psychology,* 37: 658-682.

McNall, L. A., & Stanton, J. M. 2011. Private eyes are watching you: Reactions to location sensing technologies. *Journal of Business and Psychology,* 26: 299-309.

Meglino, B. M., & Ravlin, E. C. 1998. Individual values in organizations: Concepts, controversies, and research. *Journal of Management,* 24: 351-389.

Milberg, S. J., Burke, S. J., Smith, H. J., & Kallman, E. A. 1995. Values, personal information privacy, and regulatory approaches. *Communications of the ACM,* 38*:* 65-75.

Mill, J. S. 1978. *On liberty.* Indianapolis, IN: Hackett.

Mims, C. 2018. Privacy is dead. Here's what comes next. *Wall Street Journal*. Retrieved from https://www.wsj.com/articles/privacy-is-dead-heres-what-comes-next-1525608001.

Mossholder, K. W., Giles, W. F., & Wesolowski, M. A. 1991. Information privacy and performance appraisal: An examination of employee perceptions and reactions. *Journal of Business Ethics,* 10: 151-156.

Nielsen, M. L., & Kuhn, K. M. 2009. Late payments and leery applicants: Credit checks as a selection test. *Employee Responsibilities and Rights Journal,* 21: 115-130.

Nishii, L. H., Lepak, D. P., & Schneider, B. 2008. Employee attributions of the "why" of HR practices: Their effects on employee attitudes and behaviors, and customer satisfaction. *Personnel Psychology,* 61: 503-545.

Nissenbaum, H. 2004. Privacy as contextual integrity. *Washington Law Review,* 79: 119-158.

Norberg, P. A., Horne, D. R., & Horne, D. A. 2007. The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs,* 41: 100-126.

Oldham, G. R. 1988. Effects of changes in workspace partitions and spatial density on employee reactions: A quasi-experiment. *Journal of Applied Psychology,* 73: 253-258.

Oldham, G. R., & Rotchford, N. L. 1983. Relationships between office characteristics and employee reactions: A study of the physical environment. *Administrative Science Quarterly*, 28: 542-556.

Orwell, G. 1949. *1984*. Planet eBook. Retrieved from https://www.planetebook.com/.

Paschal, J. L., Stone, D. L., & Stone-Romero, E. F. 2009. Effects of electronic mail policies on invasiveness and fairness. *Journal of Managerial Psychology*, 24: 502-525.

Pedersen, D. M. 1987. Sex differences in privacy preferences. *Perceptual and Motor Skills*, 64: 1239-1242.

Pedersen, D. M. 1999. Model for types of privacy by privacy functions. *Journal of Environmental Psychology,* 19: 397-405.

Pepper, A., & Gore, J. 2015. Behavioral agency theory: New foundations for theorizing about executive compensation. *Journal of Management,* 41: 1045-1068.

Petronio, S. 2000. The boundaries of privacy: The praxis of everyday life. In S. Petronio (Ed.), *Balancing the secrets of private disclosures:* 37-49. Mahwah, NJ: Erlbaum.

Petronio, S. 2002. *Boundaries of privacy: Dialectics of disclosure.* Albany: State University of New York Press.

Prosser, W. L. 1960. Privacy. *California Law Review,* 48: 383-423.

Rachels, J. 1975. Why privacy is important. *Philosophy and Public Affairs,* 4: 323-333.

Rosenbaum, B. L. 1973. Attitude toward invasion of privacy in the personnel selection process and job applicant demographic and personality correlates. *Journal of Applied Psychology,* 58: 333-338.

Rosenberg, K. 2010. Location surveillance by GPS: Balancing an employer's business interest with employee privacy. *Washington Journal of Law, Technology & Arts,* 6: 143-154.

Roth, P. L., Bobko, P., Van Iddekinge, C. H., & Thatcher, J. B. 2016. Social media in employee-selection-related decisions: A research agenda for uncharted territory. *Journal of Management,* 42: 269-298.

Rothe, P., Lindholm, A., Hyvönen, A., & Nenonen, S. 2012. Work environment preferences—does age make a difference? *Facilities*, 30: 78-95.

Roulin, N. 2014. The influence of employers' use of social networking websites in selection, online self-promotion, and personality on the likelihood of faux pas postings. *International Journal of Selection and Assessment,* 22: 80-87.

Roy, J. 1999. "Polis" and "oikos" in classical Athens. *Greece & Rome,* 46: 1-18.

Ryan, A. M., & Lasek, M. 1991. Negligent hiring and defamation: Areas of liability related. *Personnel Psychology,* 44: 293-319.

Ryan, A. M., & Ployhart, R. E. 2014. A century of selection. *Annual Review of Psychology,* 65: 693-717.

Schatz, D., Bashroush, R., & Wall, J. 2017. Towards a more representative definition of cyber security. *Journal of Digital Forensics, Security and Law,* 12: 53-74.

Schoeman, F. 1984. Privacy: Philosophical dimensions. *American Philosophical Quarterly,* 21: 199-213.

Seijts, G. H., Skarlicki, D., & Gilliland, S. W. 2002. Reactions to managing counterproductive behavior through the implementation of a drug and alcohol testing program: Americans and Canadians are more different than you think. *International Journal of Selection and Assessment,* 10: 135-142.

Semple, J. 1993. *Bentham's prison: A study of the panopticon penitentiary.* Oxford, England: Clarendon Press.

Smith, A., & Pitt, M. 2009. Sustainable workplaces: Improving staff health and well-being using plants. *Journal of Corporate Real Estate,* 11: 52-63, 66-67.

Smith, A., Tucker, M., & Pitt, M. 2011. Healthy, productive workplaces: Towards a case for interior plantscaping. *Facilities,* 29: 209-223.

Smith, H. J., Dinev, T., & Xu, H. 2011. Information privacy research: An interdisciplinary review. *MIS Quarterly,* 35: 989-1016.

Smith, H. J., Milberg, S. J., & Burke, S. J. 1996. Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly,* 20: 167-196.

Snyder, J. L. 2010. E-mail privacy in the workplace: A boundary regulation perspective. *Journal of Business Communication,* 47: 266-294.

Solove, D. J. 2002. Conceptualizing privacy. *California Law Review,* 90: 1087-1155.

Solove, D. J. 2011. *Nothing to hide: The false tradeoff between privacy and security.* New Haven, CT: Yale University Press.

Spivack, J. A., Askay, A. D., & Rogelberg, G. S. 2009. Contemporary physical workspaces: A review of current research, trends, and implications for future environmental psychology inquiry. In J. Valentin & L. Gamez (Eds.), *Environmental psychology: New developments:* 37-62. Hauppauge, NY: Nova Science.

Stanton, J. M. 2000. Reactions to employee performance monitoring: Framework, review, and research directions. *Human Performance,* 13: 85-113.

Stergiou-Kita, M., Mansfield, E., Daiter, L., & Colantonio, A. 2015. Good intentions? Employer representative conceptualizations and, challenges to the workplace accommodation process: The case of electrical injuries. *Employee Responsibilities and Rights Journal,* 27: 1-25.

Stone, D. L. 1986. Relationship between introversion/extraversion, values regarding control over information, and perceptions of invasion of privacy. *Perceptual and Motor Skills,* 62: 371-376.

Stone, D. L., & Bowden, C. 1989. Effects of job applicant drug testing practices on reactions to drug testing. In F. Hoy (Ed.), *Academy of Management best papers proceedings:* 290-294. Briarcliff Manor, NY: Academy of Management.

Stone, D. L., & Kotch, D. A. 1989. Individuals' attitudes toward organizational drug testing policies and practices. *Journal of Applied Psychology,* 74: 518-521.

Stone, D. L., & Stone, E. F. 1987. Effects of missing application-blank information on personnel selection decisions: Do privacy protection strategies bias the outcome? *Journal of Applied Psychology,* 72: 452-456.

Stone, D. L., & Stone-Romero, E. F. 1998. A multiple stakeholder model of privacy in organizations. In M. Schminke (Ed.), *Managerial ethics: Moral management of people and processes:* 35-59. New York: Psychology Press.

Stone, E. F., Gueutal, H. G., Gardner, D. G., & McClure, S. 1983. A field experiment comparing information-privacy values, beliefs, and attitudes across several types of organizations. *Journal of Applied Psychology,* 68: 459-468.

Stone, E. F., & Stone, D. L. 1990. Privacy in organizations: Theoretical issues, research findings, and protection mechanisms. In K. M. Rowland & G. R. Ferris (Eds.), *Research in personnel and human resources management,* vol. 8: 349-411. Greenwich, CT: JAI Press.

Stone, P., Brooks, R., Brynjolfsson, E., Calo, R., Etzioni, O., Hager, G., Hirschberg, J., Kalyanakrishnan, S., Kamar, E., Kraus, S., Leyton-Brown, K., Parkes, D., Press, W., Saxenian, A., Shah, J., Tambe, M., & Teller. A. 2016. Artificial intelligence and life in 2030. *One hundred year study on artificial intelligence: Report of the 2015-2016 Study Panel, Stanford University, Stanford, CA.* Retrieved from https://ai100.stanford.edu/2016-report.

Stone-Romero, E. F., & Stone, D. L. 2007. Current perspectives on privacy in organizations. In S. W. Gilliland, D. D. Steiner, & D. P. Skarlicki (Eds.), *Managing social and ethical issues in organizations:* 325-362. Greenwich, CT: Information Age.

Stone-Romero, E. F., Stone, D. L., & Hyatt, D. 2003. Personnel selection procedures and invasion of privacy. *Journal of Social Issues,* 59: 343-368.

Stoughton, J. W., Thompson, L. F., & Meade, A. W. 2015. Examining applicant reactions to the use of social networking websites in pre-employment screening. *Journal of Business and Psychology,* 30: 73-88.

Suen, H. 2018. How passive job candidates respond to social networking site screening. *Computers in Human Behavior,* 85: 396-404.

Sundstrom, E. 1986. Privacy in the office. In J. Wineman (Ed.), *Behavioral issues in office design:* . New York: Van Nostrand Reinhold.[AQ4]

Sundstrom, E., Burt, R. E., & Kamp, D. 1980. Privacy at work: Architectural correlates of job satisfaction and job performance. *Academy of Management Journal,* 23: 101-117.

Thibodeaux, H. F., & Kudisch, J. D. 2003. The relationship between applicant reactions, the likelihood of complaints, and organization attractiveness. *Journal of Business and Psychology,* 18: 247-257.

Tifferet, S. 2019. Gender differences in privacy tendencies on social network sites: A meta-analysis. *Computers in Human Behavior,* 93: 1-12.

Tolchinsky, P. D., McCuddy, M. K., Adams, J., Ganster, D. C., Woodman, R. W., & Fromkin, H. L. 1981. Employee perceptions of invasion of privacy: A field simulation experiment. *Journal of Applied Psychology,* 66: 308-313.

Tolkien, J. R. R. 1954. *The lord of the rings*. Boston: Houghton Mifflin.

Tomczak, D. L., Lanzo, L. A., & Aguinis, H. 2018. Evidence-based recommendations for employee performance monitoring. *Business Horizons,* 61: 251-259.

Tonidandel, S., King, E., & Cortina, J. 2018. Big Data methods: Leveraging modern data analytic techniques to build organizational science. *Organizational Research Methods,* 21*:* 525-547.

van den Akker, O. B. A., Payne, N., & Lewis. S. 2017. Catch 22? Disclosing assisted conception treatment at work. *International Journal of Workplace Health Management,* 10: 364-375.

Van Eerde, W., & Thierry, H. 1996. Vroom's expectancy models and work-related criteria: A meta-analysis. *Journal of Applied Psychology,* 81: 575-586.

Wang, N., & Boubekri, M. 2010. Investigation of declared seating preference and measured cognitive performance in a sunlit room. *Journal of Environmental Psychology,* 30: 226-238.

Warren, S. D., & Brandeis, L. D. 1890. The right to privacy. *Harvard Law Review,* 4: 193-220.

Waters, R. 2018. Europe sets a high bar on privacy with GDPR. *Financial Times,* May 25. Retrieved from https://www.ft.com/content/bbbce328-5f64-11e8-9334-2218e7146b04.

Weber, E. U., Blais, A., & Betz, N. E. 2002. A domain-specific risk-attitude scale: Measuring risk perceptions and risk behaviors. *Journal of Behavioral Decision Making,* 15: 263-290.

Westin, A. F. 1967. *Privacy and freedom*. New York: Atheneum Press.

Westin, A. F. 2003. Social and political dimensions of privacy. *Journal of Social Issues,* 59: 431-453.

White, T. B. 2004. Consumer disclosure and disclosure avoidance: A motivational framework. *Journal of Consumer Psychology,* 14: 41-51.

Winter, S., Stylianou, J., & Giacalone, A. 2004. Individual differences in the acceptability of unethical information technology practices: The case of Machiavellianism and ethical ideology. *Journal of Business Ethics,* 54: 273-301.

Wittenberg-Lyles, E. M., & Villagran, M. M. 2006. Disclosure of a cancer diagnosis in organizational peer relationships. *Communication Research Reports,* 23: 251-257.

Woodman, R. W., Ganster, D. C., Adams, J., McCuddy, M. K., Tolchinsky, P. D., & Fromkin, H. 1982. A survey of employee perceptions of information privacy in organizations. *Academy of Management Journal,* 25: 647-663.

Woodruff, A., Pihur, V., Consolvo, S., Schmidt, L., Brandimarte, L., & Acquisiti, A. 2014. *Would a privacy fundamentalist sell their DNA for $1000 . . . if nothing bad happened as a result? The Westin categories, behavioural intentions, and consequences*. Paper presented at the Tenth Symposium on Usable Privacy and Security (SOUPS), Ottawa, Canada.

Woodward, J. D. 1997. Biometrics: Privacy's foe or privacy's friend? *Proceedings of the IEEE,* 85: 1480-1492.

Yang, H., Yu, J., Zo, H., & Choi, M. 2016. User acceptance of wearable devices: An extended perspective of perceived value. *Telematics and Informatics,* 33: 256-269.

Zalesny, M. D., & Farace, R. V. 1987. Traditional versus open offices: A comparison of sociotechnical, social relations, and symbolic meaning perspectives. *Academy of Management Journal,* 30: 240-259.

Zweig, D., & Webster, J. 2002. Where is the line between benign and invasive? An examination of psychological barriers to the acceptance of awareness monitoring systems. *Journal of Organizational Behavior,* 23: 605-633.

Zweig, D., & Webster, J. 2003. Personality as a moderator of monitoring acceptance. *Computers in Human Behavior,* 19: 479-493.

Table 1

Research Questions Related to the Stakeholders' Privacy Calculus Model

Domain	Questions for Future Research
Employees' Privacy Calculus and Employee Outcomes	• What are the meta-analytic estimates of the relationships between perceived invasion of privacy and employee cognitive-affective and behavioral outcomes? • How high are employees' privacy valuations (in currency units such as U.S. dollars) vis-à-vis protection against errors, improper access, and secondary use of personal information contained in organizations' personnel records? Are such privacy valuation judgments reliable (e.g., test-retest and interrater reliability)? • Can perceptions of the risks and benefits associated with multiple domains (e.g., employee selection vs. performance monitoring) be captured using the same set of items such that a single scale could assess employees' privacy calculus across domains? • Are perceived risks and benefits characterized more by differences across domains or by individual differences (cf. Highhouse, Nye, Zhang, & Rada, 2017)? • What is the interplay between perceived risks and perceived benefits? Does the impact of risks on employee outcomes depend on the level of benefits? When the levels of risks and benefits are in alignment, do employee outcomes differ as a function of whether the levels of risks and benefits are high versus low?
Macro Factors and the Organization's and Employees' Privacy Calculus	• How do macro factors at the organization level (e.g., organizational culture/climate, public- vs. private-sector nature of organization) influence employees' privacy calculus? • How do macro factors at the country/culture level (e.g., social norms, national culture, and legal environments) influence employers' and employees' privacy calculus? For example, adopting a multilevel perspective, do country/culture factors (both directly and via organizational level factors) exert effects on the individual employee's privacy calculus as well as moderate its relationships with various behavioral and cognitive-affective outcomes (cf. Gelfand, Nishii, & Raver, 2006)? • How do social norms related to ubiquitous information technologies influence employees' work-home trade-offs? • How do social norms related to privacy evolve with regulatory changes? How do such changes influence employers' and employees' privacy calculus? • How do regulatory changes (e.g., the EU's GDPR) influence dynamics in global teams? Does differential access to employees' personal data (based on location) influence supervisor-subordinate behaviors in a global team? • How do specific cultural dimensions of tightness-looseness influence privacy? How do these cultural dimensions influence employers' and employees' privacy calculus?
Privacy Contexts	• What are the meta-analytic estimates of the relationships of perceived invasiveness with putative privacy context antecedents? • Is there a hierarchy of information privacy concerns? Does this hierarchy differ based on individual differences, social norms, and national culture? • Are job applicants more accepting of employers accessing some social media platforms (e.g., LinkedIn) versus others (e.g., Facebook, Snapchat, Instagram)? Do perceptions of invasiveness vary based on the platform? • What is the impact of alternate work arrangements such as hot-desking and coworking spaces on employees' privacy perceptions? • If employees choose a nonresponse strategy for potentially invasive questions, does it actually decrease their perceptions of invasiveness? • Do employers consider applicants' who do not have a social media presence as choosing a nonresponse strategy? Do employers evaluate social media profiles of applicants with minimal (and non-objectionable) information more adversely than those who have more information, including some information that could be considered objectionable?

Individual Factors and Employees' Privacy Calculus	• Similar to Westin's (2003; see also Kumaraguru & Cranor, 2005) classification of consumers (as "privacy fundamentalists," "privacy unconcerned," and "privacy pragmatists"), can employees also be categorized in segments based on their privacy preferences? Are there other possible segments, such as "information sellers," "convenience seekers" (Hann, Hui, Lee, & Png, 2007), and "disclosure fundamentalists"? • What is the impact of the Big 5 personality traits (conscientiousness, extraversion, neuroticism, agreeableness, and openness to experience) on workplace privacy? • What is the role of other traits such as dispositional paranoia and propensity to trust on workplace privacy? • Are there differences in privacy perceptions based on demographic differences (sex, race, age, and other characteristics)? If differences exist, what are their underlying causes? • Do personality traits mediate the relationships between demographic characteristics and privacy perceptions?
Privacy Contexts and Employee Outcomes	• Our model suggests that the impact of privacy contexts on employee outcomes is mediated by the employee privacy calculus. But could this impact also be moderated by the employee privacy calculus, as would be suggested by a person-environment fit approach (Edwards, 2008)? If so, are excessively privacy-protective organizational contexts viewed by the employee as being as harmful as privacy-invasive contexts? • What actions do employees take if they perceive privacy violations? What might a taxonomy of such employee actions look like, and how might these different actions be related to each other over time (e.g., temporally independent actions vs. temporally compensatory actions vs. a temporal progression from minor to serious actions; cf. Hulin, 1991)? What are organizational responses to such employee actions? • What is the impact of perceptions of invasiveness on relevant work behaviors such as task performance, citizenship behavior, counterproductive behavior, creativity, and voice (Dalal, Bhave, & Fiset, 2014)? • Are employees exhausted by repeated organizational announcements and initiatives related to privacy? Is the impact of subsequent events attenuated (privacy fatigue) or enhanced by previous events? • What are effective ways for employees to cope with potential privacy fatigue? Do coping strategies differ for information privacy compared to work environment privacy? Can privacy fatigue be explained by theoretical models analogous to organizational models of learned helplessness (e.g., Carlson & Kacmar, 1994) or more generally effort-performance expectancies (e.g., Van Eerde & Thierry, 1996)?

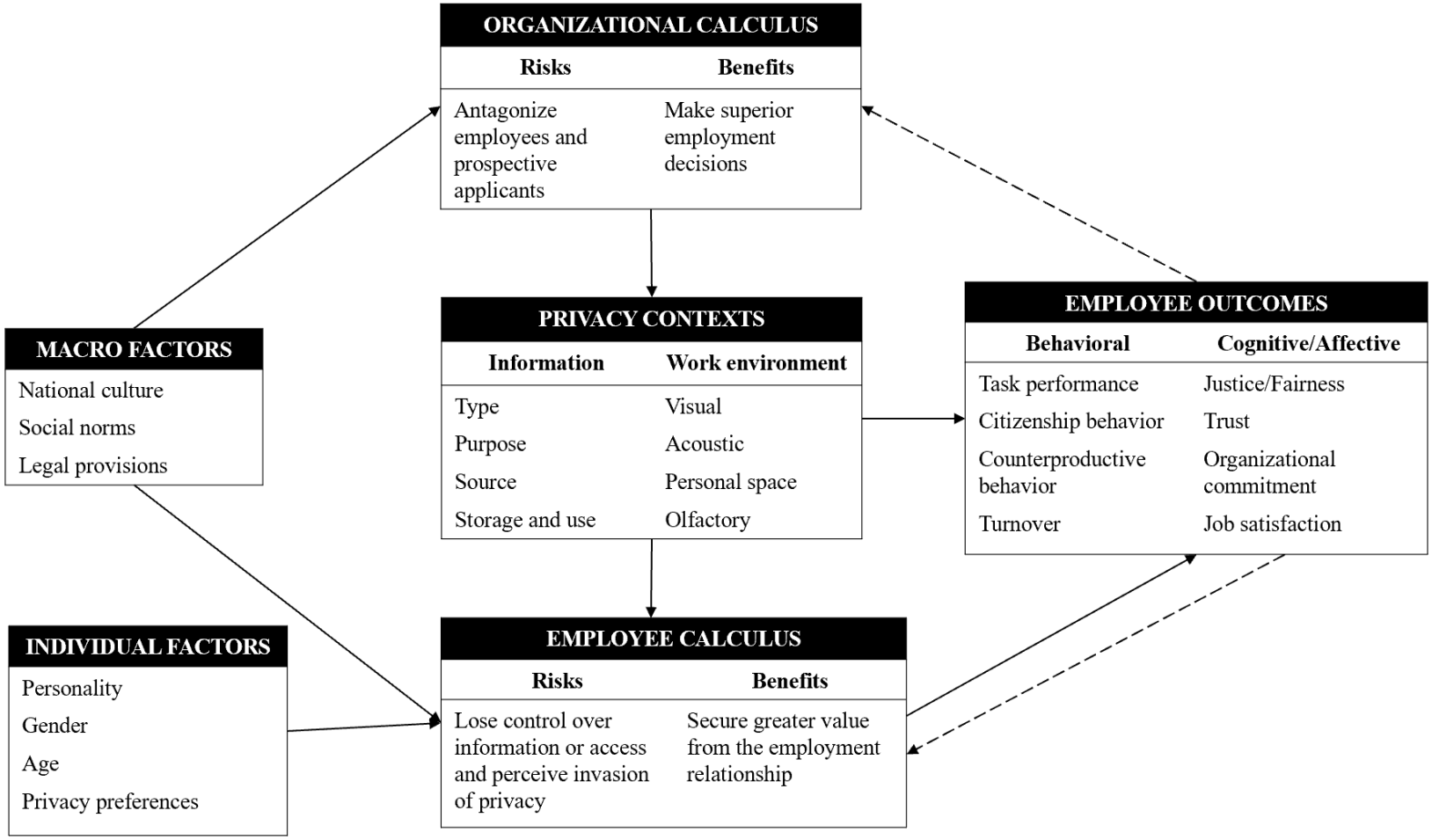
Table 2

Implications of Future Technological Trends for Privacy at Work

Technology	What is it?	Example in a Workplace Context	Employer Implications	Employee Implications
1. Cybersecurity	Often equated with "information assurance" or "information security" (Agresti, 2010). A comprehensive definition is provided by Schatz, Bashroush, and Wall: "The approach and actions associated with security risk management processes followed by organizations and states to protect confidentiality, integrity and availability of data and assets used in cyber space"; such actions include guidelines, policies, safeguards, tools, and training (2017: 66).	Security policies and measures that raise employee awareness of cyber threats or crimes (e.g., phishing and malware attacks, data leakage), improve their security practices (e.g., password management, attending security training), and control and/or restrict network access by personal mobile devices (Conteh & Schmick, 2016; Garba, Armarego, Murry, & Kenworthy, 2015; Li, He, Xu, Ash, Anwar, & Yuan, 2019).	Increase monitoring of employees' cyber behavior and activities while on the organization's system or using organizational resources.	Access to the organization's system via personal devices may be limited or even disallowed. Limited autonomy in accessing external systems and the Internet, especially for personal use, while on the organizational information technology (IT) system.
2. Wearable devices, smartphone applications and other personal monitoring devices	Devices worn as accessories or implanted in clothing, and fitted with sensors, Internet connections, processors, and operating systems (Yang, Yu, Zo, & Choi, 2016). Three main functions: Gather data (e.g., user health status and activities); enhance senses or physical ability (e.g., prosthetics and exoskeletons); facilitate virtual reality (headsets and telepresence systems that allow users to feel as if they are at meetings without physically being there; Cascio & Montealegre, 2016).	Sensors that track the heart rate, stress, fatigue levels of employees such as equipment operators whose work duties have critical safety implications; this could help reduce or prevent accidents caused by physical and/or emotional exhaustion (Awolusi, Marks, & Hallowell, 2018). Also, sensors that alert employees to safety threats and that track employees' movements and activities throughout the work day (Awolusi et al., 2018). Virtual reality devices and systems that enhance remote meeting experience (Cascio & Montealegre, 2016).	Increase productivity, safety and health of employees. But employers need to be transparent and upfront with employees about collection, usage and storage of such data, and ensure the procedures comply with privacy laws.	Significant potential for privacy invasion. Fitness and health records may be combined to present an overall medical profile of the employee which the employee may not be aware of or be willing to disclose to the employer. Possibility that data captured on non-work-related activities is incorporated in employee evaluations.
3. Global Positioning Systems (GPS) devices	Devices using satellite-based systems that display where objects or people are located in real time. Location information can be transmitted live to a receiver or stored in the device for use later (Rosenberg, 2010).	Used to track real-time locations and movements of couriers, delivery drivers, traveling or remote employees, and even movements and working speeds in warehouses, as well as to assist employees in getting directions and coordinating workflow (Akhtar & Moore, 2016; Rosenberg, 2010).	Employers need to decide on when and how GPS information is collected, and from whom. They also need to consider disclosure measures in accordance with relevant local privacy regulations.	Privacy considerations for employees: Is GPS tracking conducted via company-issued equipment, or the employee's personal device? Is the employee tracked only during work hours, or even at other times?
4. Biometrics	Technologies that measure or capture a physical trait or behavioral characteristic of a person (e.g., fingerprints, voice, facial features, keystroke or typing cadence, way of walking, etc.) and compare those data against measures of the same part previously recorded and stored in the database to achieve a match (Alterman, 2003; Jain, Ross, & Pankanti, 2006; Woodward, 1997). Biometric data are considered to be more authentic and harder to fake, compared to photo IDs and signatures (Alterman, 2003; Jain et al., 2006).	Organizations use fingerprints or facial recognition technology to establish employees' identity and control their access to physical facilities (entering buildings, rooms) or IT infrastructure (logging into systems) and for timekeeping records (Woodward, 1997). It increases security by doing away with scan cards that can easily be lost or stolen (Woordward, 1997).	Data of high-profile employees may attract hackers. Given the high-stakes and sensitive nature of such data, security concerns are significant.	The greater authenticity of biometric data also means that any theft of such data has severe consequences for employees whose identity has been stolen. Would employees have the right to opt out of providing such data?

5. Big Data	Mass digitization and datafication of information has fueled the Big Data phenomenon. Historically defined by the three Vs of volume (sheer size), velocity (constantly being added), and variety (multiple and distinct data sources), practitioners are increasingly moving away from these parameters towards the smartness of the data (i.e., the insights that analyses of such data provide and the extent to which such insights can change mindsets and spur new thinking (George, Haas, & Pentland, 2014; Tonidandel, King, & Cortina, 2018).	Commonly used in marketing and retailing to analyze customers' browsing and purchasing habits and to generate personalized recommendations and promotions (McAfee & Brynjolfsson, 2012). Organizations have also begun using Big Data to study interactions between staff demographics, management behaviors, and employee attitudes and outcomes (Angrave, Charlwood, Kirkpatrick, Lawrence, & Stuart, 2016).	With the development of privacy laws such as the EU's GDPR, potential concerns could include the need to seek prior consent before analyzing massive amounts of employees' personal data as well as portability of data from another country with different privacy laws.	Can anonymity of employees be ensured in the collection and processing of Big Data? Will predictive powers of Big Data on potential (but not undertaken) behaviors of employees represent an invasion of privacy?
6. Artificial Intelligence (AI)	Computing technologies that simulate or imitate intelligent behavior, inspired by – but usually operating differently from – how humans use their nervous systems and bodies to "sense, learn, reason, and take action" (P. Stone et al., 2016: 4). Many AI technologies are dependent on Big Data as inputs for their algorithms. Major AI research areas and applications with workplace implications are set out below.			
a. Robotics	The design, manufacturing, operation and application of robots is now a major part of AI. The field has moved beyond automation to getting robots to interact with their environment - and humans – "in generalizable and predictable ways" (P. Stone et al., 2016: 9).	Partnered with humans, robots are deployed in a growing variety of work situations, ranging from military operations (collecting intelligence, conducting attacks) and assignments in extreme environments to disaster relief and care provision in hospitals and nursing homes; they act as coworkers rather than technological tools (Bagdasarov, Martin & Buckley, 2018).	Using robots would allow employers to monitor and track these machines' activities to a high degree of precision, including their interactions with human coworkers.	Would employees be aware that their interactions with robot coworkers may be recorded as part of the process of tracking and controlling these machines? Would this constitute monitoring in a different form, and would employees consider this an invasion of privacy?
b. Internet of Things (IoT)	The concept of interconnecting many different kinds of devices, ranging from appliances (e.g., coffee makers, washing machines, headphones, lights) to vehicles, buildings, and cameras such that they can be monitored and controlled remotely and so that the sensory information from such devices can be collected, shared, and interpreted intelligently by smart devices (Hsu & Lin, 2016; P. Stone et al., 2016).	Employees, machinery, and infrastructure can be fitted with networked sensors that monitor and report their status, take instructions, and act on the information received; this allows companies to better control workflow and resource allocation (Cascio & Montealegre, 2016).	Need to ensure that data collection and interpretation involving individual behaviors and activities are compliant with relevant privacy laws. This is likely to involve disclosure to employees.	Issues similar to those with Big Data. Also, concerns about data captured on work-related vs. non-work-related activities. Do employees agree with employers on what constitutes work-related data? Will data captured on non-work-related activities influence evaluations of employees?
c. Machine learning	Techniques used to analyze Big Data. Rooted in pattern recognition and the idea that algorithms learn from captured data to make predictions and improve behavior, rather than being programmed directly to do so (Jordan & Mitchell, 2015).).	Direct applications in the employment and human resources context are still emerging. Potential uses include collecting and analyzing digital records (e.g., gleaned from social media) to supplement traditional psychometric tests in evaluating talent and predicting work-related outcomes (Chamorro-Premuzic, Akhtar, Winsborough, & Sherman, 2017).	Machine learning and its subfields (including deep learning) use Big Data as input for analysis. Implications are thus similar to those for Big Data.	
d. Deep learning	More advanced sub-field of machine learning based on algorithms inspired by artificial neural networks; aids recognition of objects and activities, and is increasingly applied in other areas of perceptions such as audio, speech, and natural language processing (P. Stone et al., 2016).	Using image and video recognition in digital interviews to capture verbal and nonverbal interpersonal behaviors and translate them into a psychological profile and predict potential fit. (Chamorrow-Premuzic et al., 2017).		

Figure 1
The Stakeholders' Privacy Calculus Model



Note. Privacy contexts are the discrete contexts of information and work environment privacy. Employees experience these privacy contexts through explicit or implicit organizational practices and policies. The dashed arrow from employee outcomes to organizational calculus refers to a bottom-up effect (involving aggregation across employees) that occurs over time. The dashed arrow from employee outcomes to employee calculus refers to potential reverse causality.

APPENDIX 1: *ONLINE SUPPLEMENT* TO PRIVACY AT WORK: A REVIEW AND A RESEARCH AGENDA FOR A CONTESTED TERRAIN

In this *Online Supplement*, we provide additional details (beyond those in the main manuscript) in three areas: defining privacy (Section 1), review of empirical findings in organizational privacy research for two relationships that we identify in the stakeholders' privacy calculus model (Section 2), and discussion of legal issues in organizational privacy (Section 3). Table numbers below refer to those in this *Online Supplement.*

SECTION 1

PRIVACY: CONCEPTUALIZATIONS AND CONTEXTS

Privacy: Broader *Conceptualizations* from Law and Philosophy

What is privacy? Embedded in answering that question is a second one: why does privacy matter? Answers to this latter question reflect fundamentally different ways in which privacy is conceptualized. Conceptualizations reflect "an abstract mental picture" of privacy (Solove, 2002: 1095). We first consider conceptualizations from philosophy and law, which have influenced the prevailing *definitions in organizational research* that we delineate in the main manuscript.

Privacy can be considered as a person's moral or legal claim (right), or a person's physical or psychological state (condition), or a person's degree of control (control; Parker, 1974; Schoeman, 1984). When privacy is conceptualized as a right, it emphasizes people's claim to choose what information they wish to communicate to others, how that information will be obtained, and how it will be used (Westin, 1967; 2003). Claims that receive legitimacy, either through the law or through social norms, constitute a "right to privacy" (Westin, 2003). When privacy is conceptualized as a physical or psychological state, it reflects the perception of "being-apart-from-others" (Weinstein, 1971). It is the "voluntary and temporary withdrawal of a person from the general society through physical or psychological means…" Westin, 1967: 5). When privacy is conceptualized as control, it is

concerned with "control over who can sense us"; Parker, 1974: 281). It reflects the power people possess to oversee what information is collected or disseminated about themselves (Fried, 1970; Miller 1971). There are also other privacy conceptualizations. Solove (2002) summarized the legal and philosophical discourse on privacy by identifying six conceptions: a) the right to be let alone, b) limited access to the self, c) secrecy, d) control over personal information, e) personhood, and f) intimacy (for related discussions on the functions of privacy, see Westin, 1967; Marshall, 1974; and Pedersen, 1997). The merits of each of these conceptualizations of privacy, among others, remain a source of scholarly discontent across disciplines (for related discussions, see Bernstein, 2017; Parker, 1974; Gavison, 1980; Schoeman, 1984).

In the main manuscript, we discuss how defining privacy is relatively clearer when considering contextual norms (Nissenbaum, 2004), such as those that exist in the employment relationship. As such, we rely on the definition of organizational privacy offered by E. F. Stone and Stone (1990), which adheres to such contextual considerations. There are two notable aspects of the E. F. Stone and Stone (1990) definition of privacy. First, in terms of the conceptualizations of privacy discussed earlier, their definition considers privacy as a state and as control. E. F. Stone and Stone (1990) intentionally excluded privacy as a right from their definition: they viewed the issue of rights to fall within the legal domain. Second, the definition is pragmatic. That is, their definition aligns with Solove's (2002: 1128) view by eschewing "seeking to illuminate an abstract concept of privacy" and by "focus[ing] instead on understanding privacy in specific contexts." Doing so helps wade through legal and philosophical debates on privacy. In particular, E. F. Stone and Stone's (1990) definition identifies three specific privacy contexts pertaining to employees: their information, their work environment, and their autonomy. We now draw on other disciplines to elaborate upon and to clarify the definitions for each of these three *privacy contexts*.

Related Definitions from Other Disciplines for the Privacy *Contexts*

In economics, *information privacy* is "the concealment of [personal] information" (Posner, 1981: 405). That is, informational privacy focuses on the deliberate and rational processes that underlie the

protection and disclosure of personal data (Acquisti, Brandimarte, & Loewenstein, 2015). This simplifying viewpoint links the economics of privacy to the economics of information (Posner, 1978, 1981). In so doing, it explicitly conceptualizes privacy as a commodity that can be monetized and exchanged (Bennett, 1995). This conceptualization is also congruent with the spirit of Stone-Romero and Stone's (2007: 327) subsequent simplified definition of information privacy: "the ability of data subjects [employees and employers] to control information".

In environmental psychology, *work environment privacy* (also sometimes referred to as space privacy or architectural privacy) is "the visual and acoustic isolation supplied by an environment" (Sundstrom, Burt, & Kamp, 1980: 102), although, as we discuss in the main manuscript, isolation associated with other senses (e.g., olfaction) is also sometimes invoked. That is, work environment privacy focuses on the actual physical environment of the office or the work space (Davis, Leach, & Clegg, 2011). More specifically, it reflects "employees' ability to control or regulate the boundary between self and others and, hence, others' access to self, and vice-versa" (Khazanchi, Sprinkle, Masterson, & Tong, 2018: 594).

In legal scholarship, *autonomy privacy* is "an individual's ability to make certain significant decisions without interference" (Kang, 1998: 1202); the "[protection of] a realm for expressing one's self-identity or personhood through speech or activity" (DeCew, 1997: 77; also see Reiman, 1976, for a related philosophical view). In organizational research, such notions of autonomy privacy align with motivation research (e.g., self-determination theory, Gagné & Deci, 2005; job characteristics theory, Hackman & Oldham, 1980; demand-control-support model, Karasek, 1979). For instance, self-determination theory's consideration of autonomy ("Autonomy involves acting with a sense of volition and having the experience of choice"; Gagné & Deci, 2005: 333) reflects the legal and philosophical notions of autonomy privacy. In light of this voluminous existing literature, in both the main manuscript and this online supplement we consider autonomy privacy only to the extent that it directly informs information privacy and work environment privacy.

We include an illustrative set of definitions employed across primary studies in organizational

research (see Table OS1 in this Online Supplement). We primarily include distinct definitions of information privacy and work environment privacy, but we also include a couple of definitions that encompass different privacy contexts in broader terms. In addition, we identify the primary privacy conceptualization reflected in the focal definition.

A quick glance at this table reveals that there are some common elements reflected across the different definitions. First, a majority of the definitions draw on the original ones put forth by a small set of scholars such as Westin (1967), Altman (1975), and E. F. Stone and Stone (1990). For this reason, and guided by Nissenbaum's (2004) and Solove's (2002) advice to focus on the context (here, the organizational context), we define information privacy and work environment privacy based on E. F. Stone and Stone's (1990) work. Second, the privacy definitions in organizational research primarily lean on the conceptualization of "privacy as control". This is not surprising. Conceptualizing privacy as control is relevant from an organizational standpoint. For instance, considering privacy as control enables the introduction of appropriate governance mechanisms—a key responsibility for managers (Mintzberg, 1973)—to regulate privacy. In contrast, the conceptualization of "privacy as a state" primarily focuses on employees and their privacy perceptions. Thus, for instance, although Alge, Ballinger, Tangirala, and Oakley (2006) define information privacy primarily using the conceptualization of privacy as control (see Table OS1), their operationalization (through assessing employees' perceptions of information gathering control, information handling control, and perceived legitimacy) reflects the conceptualization of privacy as a state (Alge et al., 2006). This is consistent with Altman's (1975) view that even if employees provide a great deal of information (or permit its collection), they could still wish to experience a state of privacy.

SECTION 2

REVIEW OF EMPIRICAL FINDINGS IN ORGANIZATIONAL PRIVACY RESEARCH

As we discuss in the main manuscript, we first utilize the stakeholders' privacy calculus to review findings based on organizational research. We then evaluate this body of work by drawing on organizational research as well as research from other disciplines. In this Online Supplement, we

discuss two sets of findings: the relationship between macrofactors and the organization's and employees' privacy calculus, and the relationship between the privacy contexts and employee cognitive-affective and behavioral outcomes. Findings related to the other relationships outlined in the stakeholders' privacy calculus model are outlined in the main manuscript.

Findings Related to Macrofactors, the Organization's Calculus, and Employees' Calculus

Summary of findings. We identified three macrofactors that will influence both the organization's and employees' privacy calculus: national culture, social norms, and the legal environment. National culture is "the collective programming of the human mind that distinguishes the members of one [country or culture] from those of another" (Hofstede, 1980: 24). Social norms are social patterns that govern behavior of members of a particular group or society (Morris, Hong, Chiu, & Liu, 2015). The legal environment is the set of laws, regulations, statutes, and judicial decisions within a specific jurisdiction that pertain to privacy rights in the employment relationship (Budd, 2009; Edelman & Suchman, 1997).

When considering privacy from a macro standpoint, the factors of national culture, social norms and a country's regulatory environment are intertwined. For instance, the enactment of the General Data Protection Regulation (GDRP) in the European Union (EU) provides employees with rights to be informed about how organizations process their personal data, to access their personal data, to ask for inaccuracies in their data to be corrected and for their data to be erased when no longer needed (i.e., the "right to be forgotten"), to restrict or block processing of personal data in specific cases, and to retrieve the data and send it to another organization ("data portability"; European Commission, 2018). In the United States, employees' data do not receive similar protections—there is no single comprehensive federal data-protection law (O'Connor, 2018). Employees' information privacy rights are diffused across several laws and statutes (Determann & Sprague, 2011; Thoren-Peden & Meyer, 2018). Furthermore, employees in organizations in the private sector do not possess privacy rights and levels of protection comparable to those employees working in organizations in the public sector (Wilborn, 1998). Overall, though, the body of work in organizational research that identifies the

linkages between these macrofactors and the organization's or employee's privacy calculus is sparse. As such, the primary factor we consider below is national culture.

An information systems study (Milberg, Smith, & Burke, 2000) drew on a sample of internal auditors across 19 countries, and reported that Hofstede's (1980) cultural dimensions were related to personal privacy concerns. Specifically, participants from cultures higher on individualism, power distance and masculinity, as well as those from cultures lower on uncertainty avoidance, had greater privacy concerns. However, organizational research on applicant reactions toward selection methods reports some differing findings for power distance. Power distance reflects the degree to which cultures are tolerant of unequal power structures (or status differences) within an organization (Hofstede, 1980), and so employees in high power distance cultures (compared to those in low power distance cultures) are likely to be less sensitive to requests for personal information during employee selection (see Daniels & Greguras, 2014). In accordance, Phillips and Gully (2002) observed that Singaporean (high power distance) participants did not weigh privacy considerations as highly as American (low power distance) participants did. Similarly, Snyder and Shahani (2012) reported that privacy considerations vis-à-vis selection methods were not at the forefront for Indian (high power distance) participants.

Comparisons across American and Belgian participants, however, revealed few differences (and more commonalities) regarding privacy concerns related to using internet-based selection systems or providing employment-related information via the internet (Harris, Van Hoye, & Lievens, 2003). Anderson and Witvliet (2008) observed similar trends in a six-country (France, Portugal, Singapore, Spain, The Netherlands and the United States) study: participants were uniformly concerned about privacy associated with different selection methods although there were a few (negligible) differences across countries. Overall, although there exist some cross-cultural differences in information privacy concerns, there is also evidence of commonalities across cultures—an aspect consistent with Westin's (1967) observations that people across cultures value privacy (see also, Newell, 1998; Francis & Francis, 2017).

As regards work environment privacy, in a qualitative study of American interns working in

Japanese organizations, Masumoto (2004) observed that, in the open layout of the Japanese workplaces (where cubicles or partitions are less common compared to workplaces in the U.S.), the American interns perceived a lack of privacy. Kaya and Weber (2003) report a similar finding from a non-work setting: space privacy concerns of American students living in dorms were greater than those of their Turkish counterparts. Overall, though, we identified few cross-cultural differences for both information and work environment privacy, and no clear pattern of findings. For instance, in the Masumoto (2004) study discussed above, American interns' privacy concerns dissipated after six months, and they appreciated the opportunity to establish supportive relationships with coworkers in the open office layout.

Assessment of empirical findings and connections to related work in other disciplines. In general, social norms, national culture, and legal environments appear to have some impact on employees' privacy but the evidence is limited. Furthermore, most studies in this area have focused more on how these macrofactors have influenced employees' privacy concerns than on employers' actions that are proximal triggers for such concerns. To that end, in a recent qualitative study, Leclerq-Vandelannoitte (2017: 147) observed that ubiquitous information technologies (e.g., smartphones and wifi-enabled laptops), which were meant to increase autonomy, flexibility and responsiveness, also created a norm of "continuous availability" such that French employees perceived "an obligation to remain reachable" even outside the office and official work hours. Thus, the introduction of technologies and policies by the employer resulted in subtle privacy intrusions that extended beyond the workplace. More broadly, the role of distributed work practices (e.g., telecommuting) and the blurring of boundaries between the professional and home domains, with the concomitant evolution of social norms that could influence privacy, is an area that warrants further investigation. Future research could therefore adopt a multilevel perspective that includes the societal (or country) level, the organizational level, and the individual employee level, with societal level factors (both directly and via organizational level factors) exerting effects on the individual employee's privacy calculus as well as moderating its relationships with various behavioral and cognitive-affective outcomes (cf. Gelfand,

Nishii, & Raver, 2006).

Another approach could involve a more nuanced way to study the influence of national culture. Rather than examining direct effects of culture on privacy, Ayoko and Härtel (2003) studied dynamics of cultural interactions within two large Australian organizations. They found that members of culturally heterogenous workgroups (based on country of origin or cultural backgrounds of group members) had different values and norms of interaction, which led to different interpretations of personal space and privacy invasion. Culture could thus elicit tensions between coworkers and between work groups (i.e., not just between employers and employees). Global teams, multicultural teams, and culturally diverse workforces are some settings where such tensions could potentially manifest.

Findings Related to Privacy Contexts and Employee Outcomes

Information privacy and employee outcomes: Summary of findings. In terms of cognitive-affective outcomes, a key correlate of perceptions of invasion of privacy is procedural justice (i.e., employees' perceptions regarding the fairness of how employment-related decisions are made; Colquitt, Greenberg, & Zapata-Phelan, 2005). Although these two constructs are moderately negatively correlated, they are distinct (Alge, 2001; Eddy, Stone, & Stone-Romero, 1999). When employees (or applicants) perceive the selection (e.g., Bauer et al., 2006; Stoughton, Thompson, & Meade, 2015) or monitoring (McNall & Stanton, 2011; Posey, Bennett, Roberts, & Lowry, 2011; Zweig & Webster, 2002) process to be invasive, they consider it to be procedurally unfair. Other cognitive-affective outcomes that are negatively related to perceptions of invasion of privacy are job satisfaction (Mossholder, Giles, & Wesolowski, 1991), organizational trust and organizational commitment (Chory, Vela, & Avtgis, 2016), and satisfaction with the organization's human resources system (Lukaszewski, Stone, & Stone-Romero, 2008). In terms of performance outcomes, Alge and colleagues (2006) observed that information privacy (with three subdimensions of perceived legitimacy, information gathering control, and information handling control) was positively related to citizenship behavior directed at individuals within the organization (OCB-I) as well as the organization itself (OCB-O).

Information privacy and employee outcomes: Assessment of empirical findings and connections to related work in other disciplines. Overall, there is limited research that considers the effects of information privacy on employee outcomes. In this domain, most studies have focused on justice perceptions, and to some extent on other cognitive-affective outcomes. Few studies have examined the relationship between information privacy and performance or other work behaviors. Beyond the organizational literature, communications research has identified specific behaviors that employees enact if they perceive privacy invasion: specifically, employees with lower status (subordinates) are more likely to initiate actions (i.e., change the topic, or directly confront the violator by communicating their dislike of the invasive behavior) compared to those with higher status (supervisors; Le Poire, Burgoon & Parrott, 1992). Furthermore, information systems research suggests that perceptions beyond invasiveness are rising to the fore. For instance, Choi, Park and Jung (2018) introduced the notion of "privacy fatigue" (i.e., repeated consumer data breaches result in people feeling drained when considering online privacy) and observed that, compared to privacy concerns, privacy fatigue was associated with greater disclosure of personal information and disengagement from coping behaviors toward data breaches. This finding suggests that perceptions of too much invasiveness over too long a period of time could result in a reaction similar to "learned helplessness" (Carlson & Kacmar, 1994), which manifests as privacy fatigue. On that note, identifying functional ways to equip employees to cope with perceptions of invasiveness would be helpful.

Work environment privacy and employee outcomes: Summary of findings. In terms of cognitive-affective outcomes, a generally consistent finding is that employees report higher satisfaction with their workspace if it is a private one (Fischer, Tarquinio, and Vischer, 2004; Oldham and Rotchford, 1983; Sundstrom et al., 1980). This is especially so for employees higher in the organization's hierarchy (e.g., managers compared to clerical workers; Carlopio & Gardner, 1995; Sundstrom, Herbert, & Brown, 1982). Furthermore, if employees' work environment affords greater privacy (personal space, acoustic), they also report higher overall job satisfaction (Lee & Brand, 2005; Zalesny & Farace, 1987; Varjo, Hongisto, Haapakangas, Maula, Koskela, & Hyönä, 2015), lower

emotional exhaustion (Laurence, Fried & Slowik, 2013), and lower fatigue (Aries, Veitch, & Newsham, 2010).

In terms of performance outcomes, lower work environment privacy results in distractions in one's work environment and is associated with lower job performance (McElroy & Morrow, 2010; Varjo et al., 2015). Establishing zones of privacy could result in higher performance (Bernstein, 2012). In that vein, in a study of Korean employees' privacy beliefs, Keem (2017) observed that those employees who believed that they controlled others' access to them had higher psychological empowerment, and, in turn, creative performance. In a related finding, Dutch employees reported that the quality of their physical work environment (which included aspects of whether employees perceived personal space, acoustic, and olfactory privacy) was associated positively with creative performance (Dul, Ceylan, & Jaspers, 2011).

Work environment privacy and employee outcomes: Assessment of empirical findings and connections to related work in other disciplines. In contrast to the paucity of research on information privacy and employee outcomes, there is a larger body of research on work environment privacy and employee outcomes. The pattern of findings indicates that perceptions of lower work environment privacy lead to adverse cognitive-affective and performance outcomes. However, more research is essential to understand the reasons underlying such adverse reactions. Some potential mechanisms could be perceptions of crowding (Oldham & Rotchford, 1983) and psychological ownership (i.e., perceptions of possession of, and being deeply connected with, their workspace; Pierce, Kostova, & Dirks, 2001). Furthermore, as noted in the main manuscript, the broader literature on office layouts is more equivocal regarding their effects on employees' outcomes (see Elsbach & Pratt, 2007). For this reason, understanding boundary conditions of the work environment privacy – employee outcomes relationship will be helpful. In that vein, Laurence and colleagues (2013) found that personalization (a type of territorial behavior where employees intentionally decorate or modify their workspace as an affirmation of their identity; Brown, Lawrence, & Robinson, 2005) buffered the effects of work environment privacy on employees' emotional exhaustion. Other types of territorial behavior,

particularly control-oriented marking (e.g., creating borders around one's workspace; Brown, 2009), can also be examined as potential moderators.

Finally, understanding the ways employees cope with the lack of privacy is a relatively unexplored area that requires further understanding. To assess whether interventions during the lunch break decreased work-related strain, call center agents were assigned to two conditions: a) a muscle relaxation exercise in a "silent room" that provided visual, acoustic, and personal space privacy, and, b) spending time in the organization's staff room and interacting with "self-chosen colleagues" that provided affiliation benefits (Krajewski, Wieland & Sauerland, 2010). Following a six-month trial, only the relaxation exercise in the silent room significantly reduced post-lunchtime and afternoon strain. In a similar vein, in a qualitative study of four technology and telecommunications organizations, Cameron and Webster (2005) observed that employees were using Instant Messaging (IM) to have private conversations with colleagues and managers, especially in open-office environments where they felt face-to-face or telephone interactions could be easily overheard by coworkers. A newer study by Bernstein and Turban (2018) found much the same: a transition to open-plan offices led to a decline of about 70% in face-to-face interaction with an accompanying increase in electronic communication (IM and email). Identifying other coping strategies that employees adopt along with specific coping-facilitative organizational interventions (e.g., mindfulness; Glomb, Duffy, Bono, & Yang, 2011) could provide helpful guidance.

SECTION 3

LEGAL ISSUES IN ORGANIZATIONAL PRIVACY

As we discuss in the main manuscript, employees and employers have notable contests in the legal arena. For a set of contemporary legal cases in several illustrative countries, please see *Austin v. Honeywell Ltd.* (2013; Australia), *Communications, Energy and Paperworkers Union of Canada, Local 30 v. Irving Pulp & Paper Ltd.* (2013; Canada), *Toh See Wei v Teddric Jon Mohr & Anor* (2017; Malaysia), *National Union of Metalworkers of South Africa and other v Rafee NO and others* (2017; South Africa), *WM Morrison Supermarkers plc v. Various Claimants* (2018; United

Kingdom), *Barbulescu v. Romania* (2017; Council of Europe), and *City of Ontario, California, et al. v. Quon et al.* (2010; United States).

Concomitantly, privacy-related regulation is evolving. The EU's GDPR is an important development that has notable implications for employers and employees. The European Commission (2018) highlights that employers within the EU need to set up clear procedures around collection, processing, use, storage and transfer of personal data, and establish appropriate consent for doing so; "blanket consent" clauses are no longer allowed (Sanders, 2018).

In terms of employees, the European Commission (2018) highlights the GDPR applies to employees working in the EU at the time of processing of their personal data; employees have the right to know how their data are processed (right to be informed), to access the data, to ask for errors to be corrected and data to be removed when no longer needed or when processing is illegal (right to be forgotten), to curb processing of data in specific instances, to retrieve data and send to another organization (data portability), and to request that decisions made via computers or automated data processing be made by "natural persons" instead, and to dispute such decisions. With the enactment of the GDPR, multinationals with EU operations may need to consider aligning privacy policies globally, especially with the stringent limitations to cross-border data transfer. In turn, this may impact the implementation of Big Data analytics and other Artificial Intelligence functions that rely on massive data collection and usage.

Other than the GDPR, there are several notable regulatory changes across the world. These include Brazil's General Data Privacy Law (approved in 2018, expected to be effective in 2020), Canada's Personal Information Protection and Electronic Documents Act (2000), China's Social Credit System (expected to be fully operational in 2020) and Personal Information Security Specification (2018), India's Personal Data Protection Bill (2018), and Singapore's Personal Data Protection Act (2012). These legal trends suggest that privacy challenges will continue to echo in the legal arena.

REFERENCES (*ONLINE SUPPPLEMENT*)

Anderson, N., & Witvliet, C. 2008. Fairness reactions to personnel selection methods: An international comparison between the Netherlands, the United States, France, Spain, Portugal, and Singapore. *International Journal of Selection and Assessment*, 16: 1-13.

Aries, M. B., Veitch, J. A., & Newsham, G. R. 2010. Windows, view, and office characteristics predict physical and psychological discomfort. *Journal of Environmental Psychology*, 30: 533-541.

Austin v. Honeywell Ltd [2013] FCCA 662

Ayoko, O. B., & Härtel, C. 2003. The role of space as both a conflict trigger and a conflict control mechanism in culturally heterogeneous workgroups. *Applied Psychology*, 52: 383-412.

Barbulescu v. Romania App. No. 61496/08 ECtHR (ECtHR, 5 September 2017)

Bennett, C. J. 1995. *The Political Economy of Privacy: A Review of the Literature.* Hackensack, NJ: Center for Social and Legal Research.

Bernstein, E. S. 2012. The transparency paradox: A role for privacy in organizational learning and operational control. *Administrative Science Quarterly*, 57: 181-216.

Bernstein, E. S., & Turban, S. 2018. The impact of the 'open' workspace on human collaboration. In press at *Philosophical Transactions of the Royal Society B: Biological Sciences*, 373(1753): 20170239.

Brown, G. 2009. Claiming a corner at work: Measuring employee territoriality in their workspaces. *Journal of Environmental Psychology*, 29: 44-52.

Brown, G., Lawrence, T. B., & Robinson, S. L. 2005. Territoriality in organizations. *Academy of Management Review*, 30: 577-594.

Budd, J. W. 2009. *Labor relations: Striking a balance:* 71-73. Boston: McGraw-Hill/Irwin.

Cameron, A. F., & Webster, J. 2005. Unintended consequences of emerging communication technologies: Instant Messaging in the workplace. *Computers in Human Behavior*, 21: 85-103.

Carlopio, J., & Gardner, D. 1995. Perceptions of work and workplace: Mediators of the relationship between job level and employee reactions. *Journal of Occupational and Organizational Psychology*, 68: 321-326.

Choi, H., Park, J., & Jung, Y. 2018. The role of privacy fatigue in online privacy behavior. *Computers in Human Behavior*, 81: 42-51.

Chory, R. M., Vela, L. E., & Avtgis, T. A. 2016. Organizational surveillance of computer-mediated workplace communication: Employee privacy concerns and responses. *Employee Responsibilities and Rights Journal*, 28: 23-43.

City of Ontario, California et al. v. Quon et al. 130 S. Ct. 2619 (2010)

Colquitt, J. A., Greenberg, J., & Zapata-Phelan, C. P. (2005). What is organizational justice? An historical overview of the field. In J. Greenberg, J., & J. A. Colquitt (Eds.), (2013). Handbook of organizational justice (pp. 3-56). Mahwah, NJ: Lawrence Erlbaum Associates.

Daniels, M. A., & Greguras, G. J. 2014. Exploring the nature of power distance: Implications for micro-and macro-level theories, processes, and outcomes. *Journal of Management*, 40: 1202-1229.

Davis, M. C., Leach, D. J., & Clegg, C. W. 2011. The physical environment of the office: Contemporary and emerging issues. In G.P. Hodgkinson & J.K. Ford (Eds.), *International Review of Industrial and Organizational Psychology:* 193-235. Chichester, UK: Wiley.

DeCew, J. W. 1997. *In pursuit of privacy: Law, ethics, and the rise of technology.* Ithaca, NY: Cornell University Press.

Determann, L., & Sprague, R. 2011. Intrusive monitoring: Employee privacy expectations are reasonable in Europe, destroyed in the United States. *Berkeley Technology Law Journal*, 26: 979-1036.

Edelman, L. B., & Suchman, M. C. 1997. The legal environments of organizations. *Annual Review of Sociology*, 23: 479-515.

Fried, C. 1970. *An anatomy of values.* Cambridge, MA: Harvard University Press.

Glomb, T. M., Duffy, M. K., Bono, J. E., & Yang, T. 2011. Mindfulness at work. In A. Joshi, H. Liao, & J. J. Martocchio (Eds.), *Research in personnel and human resources management*, 30: 115-157. Emerald Group Publishing Limited.

Hackman, J. R., & Oldham, G. R. 1980. *Work redesign.* Reading, MA: Addison-Wesley.

Harris, M. M., Van Hoye, G., & Lievens, F. 2003. Privacy and attitudes towards Internet-based selection systems: A cross-cultural comparison. *International Journal of Selection & Assessment*, 11: 230-236.

Communications, Energy and Paperworkers Union of Canada, Local 30 v. Irving Pulp & Paper Ltd. (2013), 2 SCR 458

Johnson, C. A. 1974. Privacy as personal control. In D. H. Carson (Ed.), *Man-environment interactions: evaluations and applications:* 83-100. Washington D.C.: Environmental Design Research.

Kang, J. 1998. Information privacy in cyberspace transactions. *Stanford Law Review*, 50: 1193-1294.

Karasek, R. A. 1979. Job demands, job decision latitude, and mental strain: Implications for job design. *Administrative Science Quarterly*, 24: 285-308.

Kaya, N., & Weber, M. J. 2003. Cross-cultural differences in the perception of crowding and privacy regulation: American and Turkish students. *Journal of Environmental Psychology*, 23: 301-309.

Keem, S. J. 2017. *Controlling my boundaries: Explaining how and when workplace privacy promotes creative performance.* Unpublished doctoral dissertation, Georgia Institute of Technology.

Krajewski, J., Wieland, R., & Sauerland, M. 2010. Regulating strain states by using the recovery potential of lunch breaks. *Journal of Occupational Health Psychology*, 15: 131-139.

Kupritz, V. W. 1998. Privacy in the work place: The impact of building design. *Journal of Environmental Psychology*, 18: 341-356.

Laurence, G. A., Fried, Y., & Slowik, L. H. 2013. My space: A moderated mediation model of the effect of architectural and experienced privacy and workspace personalization on emotional exhaustion at work. *Journal of Environmental Psychology*, 36: 144-152.

Le Poire, B. A., Burgoon, J. K., & Parrott, R. 1992. Status and privacy restoring communication in the workplace. *Journal of Applied Communication Research*, 20: 419-436.

Leclercq-Vandelannoitte, A. 2017. An ethical perspective on emerging forms of ubiquitous IT-based control. *Journal of Business Ethics,* 142: 139-154.

Lee, S. Y., & Brand, J. L. 2005. Effects of control over office workspace on perceptions of the work environment and work outcomes. *Journal of Environmental Psychology*, 25: 323-333.

Lukaszewski, K. M., Stone, D. L., & Stone-Romero, E. F. 2008. The effects of the ability to choose the type of human resources system on perceptions of invasion of privacy and system satisfaction. *Journal of Business and Psychology*, 23: 73-86.

Margulis, S. T. 1977. Conceptions of privacy: Current status and next steps. *Journal of Social Issues*, 33: 5-21.

Marshall, N. J. 1974. Dimensions of privacy preferences. *Multivariate Behavioral Research*, 9: 255-271.

Masumoto, T. 2004. Learning to 'DoTime' in Japan: A study of US interns in Japanese organizations. *International Journal of Cross Cultural Management*, 4: 19-37.

McElroy, J. C., & Morrow, P. C. 2010. Employee reactions to office redesign: A naturally occurring quasi-field experiment in a multi-generational setting. *Human Relations*, 63: 609-636.

McNall, L. A., & Stanton, J. M. 2011. Private eyes are watching you: Reactions to location sensing technologies. *Journal of Business and Psychology*, 26: 299-309.

Milberg, S. J., Smith, H. J., & Burke, S. J. 2000. Information privacy: Corporate management and national regulation. *Organization Science*, 11: 35-57.

Miller, A. R. 1971. *The assault on privacy: Computers, data banks, and dossiers.* Ann Arbor, MI: The University of Michigan Press.

Mintzberg, H. 1973. *The nature of managerial work*. New York: Harper and Row.

Morris, M. W., Hong, Y. Y., Chiu, C. Y., & Liu, Z. 2015. Normology: Integrating insights about social norms to understand cultural dynamics. *Organizational Behavior and Human Decision Processes*, 129: 1-13.

National Union of Metalworkers of South Africa and other v Rafee NO and others (2017) JOL 37705 (LC).

Newell, P. B. 1998. A cross-cultural comparison of privacy definitions and functions: A systems approach. *Journal of Environmental Psychology*, 18: 357-371.

O'Connor, N. 2018. Reforming the U.S. approach to data protection and privacy. *Council on Foreign Relations, January 30.* Retrieved from https://www.cfr.org/report/reforming-us-approach-data-protection

Parker, R. B. 1974. A definition of privacy. *Rutgers Law Review*, 27: 275-296.

Pedersen, D. M. 1997. Psychological functions of privacy. *Journal Of Environmental Psychology*, 17: 147-156.

Persson, A.J. & Hansson, S.O. 2003. Privacy at work – Ethical criteria. *Journal of Business Ethics*, 42: 59-70.

Phillips, J. M., & Gully, S. M. 2002. Fairness reactions to personnel selection techniques in Singapore and the United States. *International Journal of Human Resource Management*, 13: 1186-1205.

Pierce, J. L., Kostova, T., & Dirks, K. T. 2001. Toward a theory of psychological ownership in organizations. *Academy of Management Review*, 26: 298-310.

Posey, C., Bennett, B., Roberts, T., & Lowry, P. B. 2011. When computer monitoring backfires: Invasion of privacy and organizational injustice as precursors to computer abuse. *Journal of Information System Security*, 7: 24-47.

Posner, R. A. 1978. The right of privacy. *Georgia Law Review*, 12: 393-422.

Posner, R. A. 1981. The economics of privacy. *American Economic Review*, 71: 405-409.

Rapoport, A. 1972. *Some perspectives on human use and organization of space.* Paper presented at the Australian Association of Social Anthropologists, Melbourne, Australia.

Reiman, J.H. 1976. Privacy, intimacy, and personhood. *Philosophy and Public Affairs,* 6: 26-44.

Sanders, A. 2018. The GDPR – What does it mean for employers?. *Global Workplace Insider, May 25.* Retrieved from https://www.globalworkplaceinsider.com/2018/05/the-gdpr-what-does-it-mean-for-employers/

Shils, E. B. 1966. Privacy: Its constitution and vicissitudes. *Law and Contemporary Problems,* 31: 281-306.

Smith, H. J. 1993. Privacy policies and practices: Inside the organizational maze. *Communications of the ACM,* 36(12): 104-122.

Snyder, J. L., & Shahani, D. C. 2012. Fairness reactions to personnel selection methods: A look at professionals in Mumbai, India. *International Journal of Selection and Assessment,* 20: 297-307.

Sundstrom, E., Herbert, R. K., & Brown, D. W. 1982. Privacy and communication in an open-plan office: A case study. *Environment and Behavior,* 14: 379-392.

Thoren-Peden, D. & Meyer, C. 2018. USA: Data protection 2018. *International Comparative Legal Guides, June 12.* Retrieved from https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa

Toh See Wei v Teddric Jon Mohr & Anor [2017] 11 MLJ 67.

Varjo, J., Hongisto, V., Haapakangas, A., Maula, H., Koskela, H., & Hyönä, J. 2015. Simultaneous effects of irrelevant speech, temperature and ventilation rate on performance and satisfaction in open-plan offices. *Journal of Environmental Psychology,* 44: 16-33.

Weinstein, M. A. 1971. The uses of privacy in the good life. In J. R. Pennock & J.W. Chapman (Eds.), *Privacy and Personality:* 88-104. New York: Routledge.

Westin, A. F. 2003. Social and political dimensions of privacy. *Journal of Social Issues,* 59: 431-453.

Wilborn, S. 1998. Revisiting the public/private distinction: Employee monitoring in the workplace. *Georgia Law Review,* 32: 825 – 888.

WM Morrison Supermarkets plc v. Various Claimants [2018] EWCA Civ 2339.