

## Organization Science

Publication details, including instructions for authors and subscription information:  
<http://pubsonline.informs.org>

### Watchers, Watched, and Watching in the Digital Age: Reconceptualization of Information Technology Monitoring as Complex Action Nets

Aljona Zorina, France Bélanger, Nanda Kumar, Stewart Clegg

To cite this article:

Aljona Zorina, France Bélanger, Nanda Kumar, Stewart Clegg (2021) Watchers, Watched, and Watching in the Digital Age: Reconceptualization of Information Technology Monitoring as Complex Action Nets. *Organization Science* 32(6):1571-1596.  
<https://doi.org/10.1287/orsc.2021.1435>

Full terms and conditions of use: <https://pubsonline.informs.org/Publications/Librarians-Portal/PubsOnLine-Terms-and-Conditions>

This article may be used only for the purposes of research, teaching, and/or private study. Commercial use or systematic downloading (by robots or other automatic processes) is prohibited without explicit Publisher approval, unless otherwise noted. For more information, contact [permissions@informs.org](mailto:permissions@informs.org).

The Publisher does not warrant or guarantee the article's accuracy, completeness, merchantability, fitness for a particular purpose, or non-infringement. Descriptions of, or references to, products or publications, or inclusion of an advertisement in this article, neither constitutes nor implies a guarantee, endorsement, or support of claims made of that product, publication, or service.

Copyright © 2021, INFORMS

Please scroll down for article—it is on subsequent pages






With 12,500 members from nearly 90 countries, INFORMS is the largest international association of operations research (O.R.) and analytics professionals and students. INFORMS provides unique networking and learning opportunities for individual professionals, and organizations of all types and sizes, to better understand and use O.R. and analytics tools and methods to transform strategic visions and achieve better outcomes.

For more information on INFORMS, its publications, membership, or meetings visit <http://www.informs.org>

# Watchers, Watched, and Watching in the Digital Age: Reconceptualization of Information Technology Monitoring as Complex Action Nets

Aljona Zorina,<sup>a</sup> France Bélanger,<sup>b</sup> Nanda Kumar,<sup>c</sup> Stewart Clegg<sup>d,e</sup>

<sup>a</sup> Leeds University Business School, Leeds LS2 9JT, United Kingdom; <sup>b</sup> Virginia Tech, Blacksburg, Virginia 24061; <sup>c</sup> Zicklin School of Business, Baruch College, City University of New York, New York, New York 10010; <sup>d</sup> Nova School of Business and Economics Campus de Carcavelos, 2775-405 Carcavelos, Cascais, Portugal; <sup>e</sup> University of Stavanger Business School, 8600 Forus, Norway

Contact: a.zorina@leeds.ac.uk,  <https://orcid.org/0000-0001-9133-1478> (AZ); belanger@vt.edu,  <https://orcid.org/0000-0002-3213-2636> (FB); nanda.kumar@baruch.cuny.edu (NK); stewart.clegg@uts.edu.au,  <https://orcid.org/0000-0001-6083-4283> (SC)

Received: June 20, 2019

Revised: July 15, 2020; October 20, 2020; November 16, 2020

Accepted: November 21, 2020

Published Online in Articles in Advance: March 1, 2021

<https://doi.org/10.1287/orsc.2021.1435>

Copyright: © 2021 INFORMS

**Abstract.** Despite increasing studies of information technology (IT) monitoring, our understanding of how IT mediates relations between the watcher and watched remains limited in two areas. First, either traditional actor-centric frameworks assuming predefined watcher-watched relationships (e.g., panopticon or synopticon) are adopted or monitoring actors are removed to focus on data flows (e.g., dataveillance, assemblages, panspectron). Second, IT monitoring research predominantly assumes IT artifacts to be stable, bounded, designed objects, with prescribed uses which provides an oversimplified view of actor relationships. To redress these limitations, a conceptual framework of veillance applicable to a variety of possible IT or non-IT-mediated relationships between watcher and watched is developed. Using the framework, we conduct a conceptual review of the literature, identifying IT-enabled monitoring and transformations of actors, goals, mechanisms and foci and develop an action net model of IT veillance where IT artifacts are theorized as equivocal, distributable and open for diverse use, open to edits and contributions by unbounded sets of heterogeneous actors characterized by diverse goals and capabilities. The *action net of IT veillance* is defined as a flexible decentralized interconnected web shaped by multidirectional watcher-watched relationships, enabling multiple dynamic goals and foci. Cumulative contributions by heterogeneous participants organize and manipulate the net, having an impact through influencing dispositions, visibilities and the inclusion/exclusion of self and others. The model makes three important theoretical contributions to our understanding of IT monitoring of watchers and watched and their relationships. We discuss implications and avenues for future studies on IT veillance.

**Supplemental Material:** The online appendices are available at <https://doi.org/10.1287/orsc.2021.1435>.

**Keywords:** monitoring • veillance • information technology transformations • surveillance • panopticon • action net model • veillance foci • veillance apparatus • veillance goals • veillance actors • veillance web

## 1. Introduction

Advances in computing technologies, especially in the capture and manipulation of large quantities of data, have led to a rise in digital monitoring on a scale impossible just a decade earlier (e.g., Astor et al. 2013, Newell and Marabelli 2015). Digital monitoring involves heterogeneous participants engaging in diverse alliances and conflict that are able to challenge previously exclusive rights of watchers<sup>1</sup> to manipulate visibility and anonymity (Scott and Orlikowski 2014, Anteby and Chan 2018). During the 2020 COVID-19 pandemic, for example, contact tracing of citizens in various countries differed in significant ways, co-shaped by complex interactions among government, tech companies, citizens, businesses, and privacy advocates (Busvine and Rinke 2020, Haskins 2020, Servick

2020). Norway's data-protection regulators vetoed distribution of the health authority's contact-tracing app that used location data and processed proximity data centrally rather than on individual smartphones (Browne 2020), whereas, conversely, Taiwan and South Korea relied on individual smartphones and peer reporting for centralized collection of data, as well as intensive cooperation between the government, private health providers, and hacking communities (McCurry 2020, Silva 2020). Traditional conceptions of monitoring (e.g., Orwell's "Big Brother") project a sinister image of malevolent watchers, although these monitoring practices are premised on possibilities that may benefit the targets of monitoring.

Much recent work employs a frame popularized by Foucault's (1977) focus on Jeremy Bentham's

sponsorship of a panoptical architectural device, situated in a watchtower, to maximize the visibility of those being surveyed while minimizing the visibility of its practice. Foucault argued that panoptic observation trains those under surveillance to conduct themselves as if they are being watched, even though they may not be. Knowing that one and one's fellows are potentially under surveillance induces conformance with surveillance precepts. The panopticon model's popular influence on the monitoring/surveillance literature brought to the fore how disciplinary power operates through the few watching over the many (Haggerty 2006). Gaps remain, however; researchers focused largely on the disciplinary relationships between the watcher and watched and ignored attributes of contemporary monitoring practices not neatly fitting the panoptic frame (Haggerty 2006, Lyon 2006). Contemporary monitoring requires different framing (e.g., Haggerty 2006; Mann and Ferenbok 2013; Leclercq-Vandelannoitte et al. 2014; Zuboff 2015, 2016). Whereas some recent work on information technology (IT) monitoring either extends the panoptical model while still focusing on actors (e.g., portable panopticon, postpanopticon, superpanopticon, and synopticon) (e.g., Lyon 2006, De Saulles and Horner 2011), others remove actors from central focus by developing models based on data flows (e.g., data-veillance, assemblages, panspectron) (e.g., DeLanda 1991, Haggerty 2006). New gaps emerge in consequence, premised on the assumption that IT artifacts mediating monitoring between watchers and watched are stable, bounded, and designed objects. Recent studies in the management organization studies (MOS) and information systems (IS) fields challenge these assumptions, exploring IT artifacts as fundamentally editable, reprogrammable, and open for contributions from potentially unbounded heterogenous participants (Manovich 2001, Garud et al. 2008, Kallinikos et al. 2010, Yoo et al. 2010). For instance, the design and functioning of COVID-19 tracing apps can be (re) designed and (re)negotiated by diverse participants (Singer 2020). These newer perspectives on IT artifacts change our knowledge about relationships between watcher and watched and their possible implications for predictable social order and control<sup>2</sup> on which theorizing of non-IT monitoring has traditionally relied (Clegg et al. 2006). A veillance concept and a synthesizing veillance framework applicable to a variety of IT- or non-IT-mediated relationships between watchers and watched is proposed as a means of addressing these gaps in the literature.

We offer three important theoretical contributions. We do so by developing an action net model of IT veillance as a flexible, decentralized, and interconnected web shaped by watcher-watched relationships that are multidirectional, enabling multiple dynamic goals and

foci to be affected by cumulative contributions of heterogenous participants organizing, manipulating, and having an impact on the net, influencing the dispositions of the roles, visibilities, and inclusion/exclusion of others and self. First, our action net captures IT-enabled flexibility, complexity, unpredictability, and constant evolution of heterogenous actors and their relationships, addressing transformative IT impacts on monitoring (e.g., Mann and Ferenbok 2013, Leclercq-Vandelannoitte et al. 2014, Zuboff 2016). Second, the action net is built on neither particular predefined patterns of actor relationship as watcher/watched nor prior organizational boundaries (Czarniawska 2004). Participant relationships and IT enactments performative to actor roles, flexible system elements, and boundaries, enabling multiple dynamic foci, continuously reestablish these relations. Third, our findings reveal four new relational logics between the watcher and watched in contemporary IT veillance systems. These relational logics are constituted by (i) flexibility of veillance elements, (ii) diffused actor roles, (iii) cumulative extended manipulations, and (iv) emergent nonlinear actor relationships. IT monitoring aligned with IT artifacts as equivocal, distributed, and open for uses, edits, and contributions of unbounded sets of heterogenous actors with diverse logics and goals ground these relational logics.

The paper is structured as follows. First, we review monitoring terms, discuss their applicability in IT-mediated contexts and develop a veillance framework to theorize *what* factors and concepts characterize the relationships between the watcher and the watched in IT and non-IT monitoring. Second, the literature review is elaborated and the framework explained. Third, the findings, highlighting key transformations enabled by IT to actors, goals, mechanisms, and foci of monitoring are elaborated. Fourth, the theoretical contributions are presented, including the proposed action net model of monitoring and the new logics of IT veillance systems. We also present avenues for future research.

## 2. Conceptual Review and Veillance Web Framework

### 2.1. Monitoring Concepts

Most monitoring terms and frameworks conceptually emphasize either the watcher or the watched or monitoring as a scrutinized sets of data flows (see Table 1). We discuss these concepts in turn, as they apply to the watcher, watched, or act of watching.

The relationship implied between the watcher and the watched, from the watcher's perspective, is either top-down or bottom-up, conceptualized as *surveillance* or *sousveillance*. Surveillance is the most widely used approach, associated with centralized control

**Table 1.** Conceptual Review of Monitoring Terms

Term	Focus	Definition	Examples	Sample studies	Conceptual theorizing limitations
Surveillance	Watcher (who watches)	Monitoring designed and enacted by watcher who can observe from the position of either: <ul style="list-style-type: none"> <li>• Above (i.e. from French “sur” (“over”) and “veiller” (“see/watch”)),</li> <li>• Below (i.e., from French “sous” [“under”] and “veiller” [“see/watch”])</li> </ul>	Government watching citizens; managers watching employees; firms watching customers	Lyon 2001, 2006; Doolin 2004; Zuboff 2015, 2018	<ul style="list-style-type: none"> <li>• Offers contradictory insights on the nature of the watcher</li> <li>• Implies hierarchical top-down relationships between watchers and watched</li> <li>• Prioritizes actor on particular hierarchical side (e.g., from the sur- or the sous- type)</li> <li>• Assumes IT tools as stable objects</li> </ul>
Sousveillance			Protestors filming police; corporate; citizens watching government; CCTV; peer monitoring on social media	Brivot and Gendron 2011, Ferenbok 2013, Kubitschko 2015	
Panopticon	Watched (who is watched)	Monitoring where the many are watched by a few (from Greek “pan” [“all”] and “opticon” [“observed”])	Actors supervised in correctional organizations (prisons, clinics, camps); citizens monitored by government	Foucault 1977, Clegg et al. 2012,	<ul style="list-style-type: none"> <li>• Does not account for agency of watched, implies their consciousness</li> <li>• Fails to include flexible organizational spaces</li> <li>• Fails to include IT-enabled reciprocal interconnections of watcher and watched</li> <li>• Assumes IT tools as stable objects</li> <li>• Fails to include IT-enabled reciprocal interconnections of watcher and watched</li> <li>• Assumes IT tools as stable objects</li> <li>• Fails to incorporate IT-enabled reciprocal interconnections of watcher and watched</li> <li>• Implies consciousness of being tracked by watched</li> <li>• Assumes IT tools as stable objects</li> <li>• Fails to incorporate interconnections between the watcher and the watched</li> </ul>
<i>Electronic/information</i>		Monitoring with enhanced visibility of all IT-mediated actors and processes	Employees and customers monitored by corporations via IT systems	Orlikowski 1991, Lyon 1994, Jonsson 2006	
<i>Portable (free control)</i>		Monitoring of all IT-mediated spaces	Corporate monitoring of distanced work	De Saullles and Horner 2011, Leclercq-Vandelannoitte et al. 2014	
<i>Super</i>		IT-enhanced monitoring “without walls, windows, towers or guards” (Poster 1996, p. 93)	Electronic databases	Poster 1995, 1996	
<i>Post</i>		Monitoring enabling softer and more distributed forms of control	Participatory management; corporate transparency culture; total quality management	du Gay 2004; Sewell and Barker 2006; Baudrillard 2006, 2007; Iedema and Rhodes 2010	<ul style="list-style-type: none"> <li>• Assumes IT tools as stable objects</li> <li>• Fails to incorporate IT-enabled reciprocal interconnections between the watcher and the watched</li> <li>• Implies consciousness of being tracked by the watched</li> <li>• Assumes IT tools as stable objects</li> <li>• Fails to incorporate IT-enabled reciprocal interconnections of watcher and watched (does consider top-down &amp; centralized control)</li> </ul>
Synopticon		Monitoring where many watch the few (from Greek “syn” [“with/ together”] and “opticon” [“observed”])	Politicians scrutinized via the masses; celebrities or favorite organizations followed on social media	Mathiesen 1997; Boyne 2000; Lyon 2006	



Table 1. (Continued)

Term	Focus	Definition	Examples	Sample studies	Conceptual theorizing limitations
Dataveillance	Data flows	IT-enabled systematic monitoring of people or groups in order to regulate or govern their behavior	Customer loyalty cards; swipe corporate cards; monitoring of truck drivers; Google search engine; EyeSee Mannequins <sup>a</sup> ; Google Maps app <sup>b</sup>	Clarke 1988; Zimmer 2008; Van Dijk 2014; Degli Esposti 2014	<ul style="list-style-type: none"> <li>Does not include non-IT monitoring</li> <li>Assumes IT tools as stable objects</li> </ul>
Assemblages		Monitoring of multidirectional temporary data flows (i.e., rhizome-like structures without one center) created by multiple heterogeneous actors	Facebook app; data generated, searched, and collected from iPhone; contemporary policing collecting information from aggregated databases and multiple agents	Deleuze and Guattari 1987, Haggerty and Ericson 2000, Haggerty 2006,	<ul style="list-style-type: none"> <li>Analytically challenged for what to include/exclude: filtering of IT precludes heterogeneous and multidirectional connections</li> <li>Assumes IT tools as stable objects</li> <li>Focuses on IT-enabled monitoring only</li> </ul>
Panspectron		Monitoring that bypasses visible practices (e.g., base for panopticon) and shifts attention to nonvisible practices enabled by IT	Encryption techniques, wireless technologies, AI that offers new, invisible or hard to detect monitoring dimensions	DeLanda 1991	<ul style="list-style-type: none"> <li>Does not take the coexisting forms of hierarchical control into account</li> <li>Assumes IT tools as stable objects</li> </ul>

<sup>a</sup>EyeSee Mannequin, produced by the Italian company Almax, uses facial recognition technology to reveal customers' age range, gender, and race. Its voice recognition applications listen to what shoppers say about mannequins (Degli Esposti 2014).

<sup>b</sup>Google Maps reads the speed and position of millions of cars to construct the traffic pattern and select the best routes for those asking for driving directions.

(Foucault 1977) predicated on IT monitoring (Boyne 2000, Iedema and Rhodes 2010). *Sousveillance*, in which watchers are decentralized and flexible actors (Bogard 1996, Baudrillard 2006, Zuboff 2015), was originally proposed to account for relationships in which those that are objects of surveillance use IT to observe their supervisors and peers, such as protestors filming police (Mann and Ferenbok 2013). *Sousveillance* in the form of the video recording of Mr. George Floyd's death in 2020 sparked widespread civil unrest in the United States. Organizational members' digital devices can capture or report actions of other members (Silverman 2019). The leak of the U.K. National Security Council's decision to allow Huawei to provide noncore parts of the United Kingdom's 5G mobile network is a case in point (Loughran 2019).

From the perspective of the watched, it is terms from the second meta-group (*panopticon* in its multiple variations and *synopticon* in terms of the many watching the few) that define monitoring. Originally proposed by Bentham in 1843 as a design based on his brother Samuel's innovations at a Moscow factory, panopticism was developed in parallel in a diverse range of institutions. Foucault (1977) popularized the term, to describe a disciplinary society that sought to control and normalize the conduct of the watched in contemporary organizations, giving rise to a transdisciplinary "surveillance theory" (Brocklehurst 2001, Wood 2002). What the panopticon does not account for are diverse IT-enabled transformations (Haggerty and Ericson 2000, Marx 2002), including the agency and IT-enabled empowerment of the watched (Brocklehurst 2001, Leclercq-Vandelannoitte et al. 2014). Furthermore, it conceives of organizations as bounded, observable, and calculable spaces rather than as IT-enabled flexible spaces with emergent and reciprocal interconnections between watchers and watched (Martin et al. 2009). Several extensions of the term *panopticon* include *electronic panopticon*, *information panopticon*, *portable panopticon*, *postpanopticon*, and *superpanopticon* (Table 1). Radical IT transformations make extensions of these metaphors contradictory and possibly irrelevant (Haggerty 2006).

IT monitoring is increasingly discussed as emphasizing data flows more than the actors associated with them. Thus, *dataveillance* builds on employees' and customers' digital data traces to access, interpret, and monitor behaviors (Mayer-Schönberger and Cukier 2013, Van Dijk 2014). In surveillance *assemblages*, "there is no central force . . . no Big Brother, no panopticon, but a shifting, moving observation, presentation, and regulation of the self by countless measures in countless locations" (Gilliom and Monahan 2012, p. 22). Data collection flows exist prior to any particular assemblage's fixing of them temporarily and spatially, emergently and unstably through unique

IT capturing of flow (Haggerty and Ericson 2000). Likewise, DeLanda's (1991) *panspectron* focuses on new, previously unavailable, zones for monitoring enabled by decentralized, pervasive, and often-invisible or difficult-to-detect digital networks made up of sensors, satellites, digital antennae, and cable-traffic intercepts (DeLanda 1991, p. 2006). Similar to assemblages, the *panspectron* focuses only on IT-enabled monitoring, often ignoring coexisting systems of non-IT and/or top-down monitoring; for instance, it could not grasp the complexities of contact tracing of citizens within a community.

Two fundamental problems are highlighted by conceptually oversteering monitoring terms and associated frameworks. First, none either serve as a foundation for a comparative systematic analysis of transformations enabled by IT or offer mutually excluding models describing IT-mediated watcher-watched relationships. Some rely on extensions to traditional actor-centric terms (e.g., portable panopticon, postpanopticon, superpanopticon, and synopticon) (e.g., Poster 1996, De Saulles and Horner 2011), whereas others develop models of data flows specific and exceptional for IT contexts (e.g., data-veillance, assemblages, *panspectron*) (e.g., DeLanda 1991). Second, despite substantial differences, these studies assume that IT tools are stable objects. Recent studies question such assumptions with regard to IT artifacts. Table 2 shows diverse IT characteristics, definitions, and sample studies calling for rethinking fundamental assumptions and explanations of IT processes and outcomes (e.g., Zittrain 2008, Nambisan et al. 2017).

As Table 2 illustrates, IT artifacts are increasingly seen as possessing unique characteristics of being editable and reprogrammable during the process of IT use (Manovich 2001, Kallinikos et al. 2010, Yoo et al. 2010). What is enabled are potentially unbounded and heterogenous participant contributions guided by multiple logics of organizing (Majchrzak

and Malhotra 2013, Lyytinen et al. 2016). Emerging knowledge about IT artifacts has yet to be incorporated into theorizing the roles of the watcher, the watched, and the act of watching in the digital age. To address this, we propose a new conceptual *veillance* framework to guide analysis of IT-enabled monitoring.

## 2.2. Veillance Framework

A framework for analyzing contemporary monitoring should be simple but flexible enough to incorporate diverse and oftentimes complex and evolving relationships. Our proposed conceptual framework has three major elements: the *veillance* concept (VC), a typology of *veillance* foci (VF), and a *veillance* web (VW) framework. Together, these elements help guide, structure, and bound our analyses and theorization of *what* factors of the phenomenon change, as well as *how* and *why* (Whetten 1989).

**2.2.1. Veillance Concept.** We propose the concept of *veillance* (based on the French verb *veiller*, meaning “to watch”) as an elementary operation common to various monitoring practices, whether non-IT- or IT mediated. Building on Lyon's (2006) work, we define *veillance* as the social operation making a phenomenon visible. The focus is on *what is made visible* and *how*, emphasizing processual and practical aspects relating to a range of actors and relationships. The proposed concept is sufficiently universal in terms of Ockham's razor<sup>3</sup> to incorporate both IT and non-IT monitoring and avoids predefined a priori relationships between the watcher and the watched (as sur- and sousveillance do), as well as predefined subjects of monitoring (as panoptical or synoptical approaches do).

**2.2.2. Typology of Veillance Foci (VF).** The *focus of veillance*, that which is made visible and traceable, recognizes the diversity and evolution of monitoring practices. Clegg et al. (2006) discuss how organizational monitoring changed in focus from the body to

**Table 2.** Characteristics of IT Artifacts as Transformative Agents

Characteristic	Definition	Key studies
Editability	Ability of IT to be continuously and systematically modified and updated	Kallinikos et al. 2013, Lyytinen et al. 2016, Leonardi and Vaast 2017
Distributedness	Ability of IT to store and manage data from and to multiple sources, actors, and institutions	Kallinikos et al. 2013, Majchrzak and Malhotra 2013, Nambisan et al. 2017
Granularity (modularity)	Ability of IT to be decomposable and broken down into self-sufficient blocks (or modules) or elementary units	Manovich 2001, Zittrain 2008, Yoo et al. 2010, Kallinikos et al. 2013
Interactivity	Ability of IT to allow users to follow alternative pathways of information exploration by activating different functions embedded in the IT	Garud et al. 2008, Kallinikos et al. 2013, Lyytinen et al. 2016
Reprogrammability	Ability of IT to be accessible and modifiable by other digital objects	Zittrain 2008, Yoo et al. 2010, Kallinikos et al. 2013, Leonardi and Vaast 2017

soul, to commitment, and to productive resistance. We build on this classification by proposing three *foci* of veillance: *body*, *soul*, and *commitment*. We do not include Clegg et al.'s fourth political regime, power as productive resistance, because it can take place across each of the veillance types in the form of sousveillance and peer veillance when those being watched also constitute perceptions of the body, soul, and commitment of their watchers (Sewell 1998, Kenny 2019).<sup>4</sup> Table A1 in Online Appendix A provides examples of the VF typology for non-IT and IT veillance.

**2.2.2.1. Veillance of Body (VoB).** Veillance of body is the social operation making the bodies and behaviors of the watched visible. It is practiced, for example, when organizations associate their efficiency with physical control over the bodies of the watched and induce desirable behavior from them. Historically, VoB was used for particular institutionalized groups, such as soldiers, prisoners, or people with socially contagious diseases (Foucault 2003, Clegg et al. 2006). A shift in the paradigm of organizational monitoring was introduced with scientific management, which justified the scrutiny of “productive hands” (Clegg et al. 2006), surveying employees’ bodies and behaviors using simple productivity metrics. Although the approach became standard for work design, it also proved to be associated with high fatigue, turnover, and absenteeism (Yates 1993). The body as an object of political economy is extended by IT tools enabling biometric identification, monitoring of biohealth markers such as blood pressure and heart rate, as well as closed-circuit television (CCTV) operation. Such digital devices enable the body to be increasingly subject to self-surveillance as well as that of corporate training programs and the peer surveillance of other team members.

**2.2.2.2. Veillance of Soul (VoS).** The social operation of veillance of the soul makes the moral life of those watched visible and knowable. Organizations practicing VoS seek to become knowledgeable about the motivations of employees and their informal work lives and attitudes (Trahair 2001). VoS is practiced when organizations demand to know the contexts framing the social and emotional souls of employees, as in Ford’s Sociological Department<sup>5</sup> (Clegg et al. 2006) or when managers built on Mayo (1975)’s interpretation of the perplexing results from the Hawthorne experiments to turn the focus of their veillance of bodies to that of their interior lives, dispositions, and how these frame the informal work relations of the watched (Mayo 1975, Muldoon 2017). For the watched, transformations in veillance from VoB to VoS, moving from Taylorist to human relations thinking in management, might appear to offer minimal supervision,

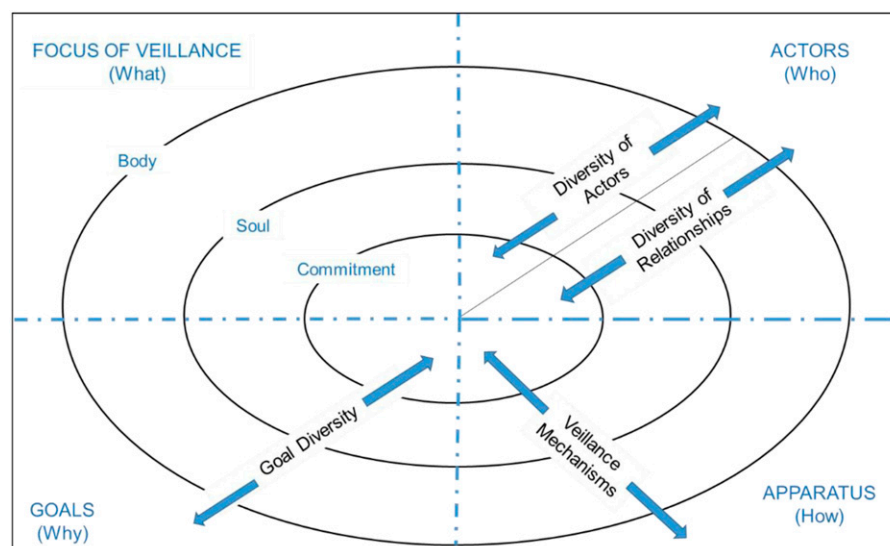
often taking the form of a “friendly chat” (Clegg et al. 2006, p. 81). However, as Mayo writes, “Their opinion is, of course, mistaken: in a sense they are getting closer supervision than ever before, the change is in the quality of the supervision” (Mayo 1975, p. 75). In this sense, VoS encompasses VoB, while also stressing interpretations of consciousness and unconsciousness (Mayo 1975) as a priority (Clegg et al. 2006). Examples of IT-mediated VoS include company monitoring of employees’ social media posts and the blogosphere. In the evaluation of performativity in UK and Australian universities, for example, social media displays by academics are taken as representational devices to be monitored for tallying signs of media appearances.

**2.2.2.3. Veillance of Commitment (VoC).** Veillance of commitment strives to make visible the commitment of those watched in nonstandardized situations, such as creative tasks, independent and spontaneous actions, or activities with high complexity or communication requirements. Here, control is sought through people freely expressing obeisance to a normative order, showing willing consent. Digitally performing HR tests devised to insure the organization against claims of sexual harassment, health and safety breaches, and other sources of litigation would be examples. Organization members have to consent to do these periodic tests; consent and completion ensures that the organization is protected against any misdemeanors, as it can be claimed that any deviance on the part of actors was a conscious violation of the digital protocols in play in membership tests that had been consented to and completed. In universities, using digital devices such as Publons for publicizing peer review for journals offers more voluntarist but still normatively framing examples. Other examples include peer monitoring in virtual teams and norms of continuous online accessibility and responsiveness, accelerated by the new home-working work practices established during the coronavirus pandemic. VoC implies a substantial internalization of (or at least high sensitivity toward) the watcher’s goals and values (Rhodes 2007, Levay and Waks 2009) and focuses on the subject’s commitment being realized as a part of team and peer scrutiny and (digital) self-monitoring.

**2.2.3. Veillance Web (VW) Framework.** Following our review and analysis of diverse monitoring concepts, we identified several key factors that characterize the relationships between the watcher and the watched in both IT and non-IT veillance. Contemporary veillance, we propose, is best represented as an action net conceived as a web of complexly interconnected elements that relate veillance actors and goals, apparatuses and foci. Figure 1 presents the conceptual VW framework.



**Figure 1.** (Color online) Conceptual Veillance Web Framework



Veillance *actors* refer to *who* is involved in the veillance and builds on the core idea that veillance could include various watchers and watched (conceptualized as *diversity of actors*) in a variety of top-down, bottom-up, and peer relationships (conceptualized as *diversity of relationships*). The veillance *goals* describe *why* veillance is being conducted (conceptualized as *goal diversity*). The veillance *apparatuses* focuses on *how* veillance is conducted, by specifying various ways in which the watched are made visible to the watchers (conceptualized as *veillance mechanisms*). Finally, veillance *foci* describe *what* is the main attention of the veillance operation (i.e., body, soul, or commitment), drawn from the typology in Table A1. The VW provides a simple but highly flexible framework to capture various veillance systems and watcher-watched relationships across non-IT and IT contexts. We apply the VW framework to guide our analysis of literature on IT and non-IT monitoring to understand how and in what ways IT mediation changes monitoring. As we will explain, the development of the framework emerged interactively with the process of coding papers in the literature review. The results of our analyses were then used to theorize key IT-enabled transformations of monitoring,

### 3. Methodology

We performed a review of the literature in the top eight MOS and IS journals using the VW framework as a basis for our analysis.<sup>6</sup> Although this approach does not result in a complete list of veillance articles, selecting these journals provides a representative sample of quality peer-reviewed veillance research. We used several keywords related to monitoring

practices: surveillance, panopticon, monitoring, privacy, and audit. To complement the articles in the leading journals, we also performed a search on the keyword “surveillance” in the EBSCO Business Source database. Finally, we conducted a citation analysis to ensure that we identified highly cited articles to include in our discussion. In total, we identified 629 articles. Two rounds of screening were used to identify the final sample of 132 coded papers. A summary of the literature review and screening processes, counts per journal, the resulting sample, and coding categories appears in Online Appendix B.

#### 3.1. Coding

An iterative in-depth coding process coded empirical papers identified (e.g., Shapira 2011, Bélanger et al. 2014), a process involving initially reading several articles, identifying initial codes, grouping codes into categories and recoding articles as new categories emerged. The coding resulted in the development of key attributes of the elements of the VW framework. Attributes for *veillance foci* are veillance of body (VoB), commitment (VoC), and soul (VoS); *diversity of actors* includes organizations, employees, customers, governments (i.e., governments, nations, states, or agencies), and other people (students, citizens, etc.); attributes for *diversity of relationships* include patterns of interplay of roles of watchers (“W”) and watched (“w”); attributes for *goal diversity* are documentation, verification, prevention/protection, discovery, influence/persuasion, profit, provision of benefits, self-improvement, and compliance; attributes for *veillance mechanisms* include hard and soft mechanisms. These refer to how veillance is conducted. For example, hard mechanisms could include coercion, physical markings, and inspections



to generate fear; examples of soft mechanisms include seduction, deception, rewarding, and internationalizing by the watched. Each category was examined across non-IT and IT veillance. The details of the coding process, categories, and attributes are shown in Online Appendix B, and the resulting codes for the 132 papers are shown in Online Appendix C.

### 3.2. Thematic Analysis

Once papers were coded, we conducted a thematic analysis to identify *how* the elements of the VF are transformed by IT. As detailed in Figure A1 in Online Appendix A, we analyzed the coded papers across each element of the VF and its related categories and attributes of non-IT and IT veillance, which enabled us to develop detailed insights into how each VF element was transformed by IT. Notably, the analysis of IT transformations to veillance actors resulted in identification of two groups of the watcher-watched (“Ww” hereafter) relationship patterns: (1) *shared patterns* that were identical in terms of participating actors and their roles across both non-IT and IT veillance, and (2) *distinctive patterns* where actors and their Ww roles are distinctively explored in either non-IT or IT settings. Examples of shared and distinctive patterns are presented in Table 4 in the next section. Comparative analysis of other VF elements (goals, mechanisms, and foci) across non-IT and IT veillance proceeded across the identified shared and distinctive patterns to identify detailed transformations enabled by IT mediation.

## 4. Findings: IT-Enabled Transformations to the Watcher-Watched Relationships

The thematic analysis identified IT-enabled transformations to VW framework elements and their relationships. We discuss here the IT-enabled transformations, and, in Section 5, we integrate these transformations into an ensemble and theorize how they affect the interplay of VF framework elements.

### 4.1. Actor Relationships and Roles

Our analysis identified that shared Ww patterns of actor relationships incorporated widely discussed patterns across non-IT and IT contexts of organizations watching employees (e.g., Bernstein 2012) and organizational peer veillance (Poppo and Zhou 2014, Anderson et al. 2017) (see Table 3). At the same time, an important distinctive pattern discussed only in non-IT veillance included relationships where organizations and employees are both watchers and watched (e.g., Riad 2005, Long et al. 2011). Other distinctive patterns of IT veillance were multiple, for example, relationships where organizations and customers are both watchers and watched (e.g., Orlikowski and

Scott 2014). As our analysis illustrates, IT makes relationships between veillance actors more complex and intensive, with the roles of the watcher and watched more interactional, facilitating the incorporation of a greater variety of actors.

#### 4.1.1. Increased Intensity and Complexity of Veillance.

Our analysis reveals the increased intensity and complexity introduced by IT in Ww relationships across *shared patterns*. For example, IT veillance of employees leads to their increased performance (Grant and Higgins 1991, Pierce et al. 2015) and responsible behavior (Gozman and Currie 2014) but is also associated with increased resistance (Ball and Wilson 2000), stress (Ayyagari 2011), and disciplinary control (Brocklehurst 2001). Other studies discuss new areas in IT monitoring (e.g., artificial intelligence [AI], online spaces) (e.g., D’Arcy et al. 2009, Leclercq-Vandelannoitte et al. 2014). Likewise, studies mention that IT enables or significantly intensifies previously unstudied peer organizational veillance, such as information sharing in healthcare (Anderson et al. 2017). Notably, organizations watching customers rely on IT-enabled new approaches to collecting and sharing customer data (e.g., Culnan 1993, Li and Qin 2017), as well as new ways of acting on collected data such as smart metering technology to monitor electricity usage and control or disable consumers’ appliances (Karwatzki et al. 2017a, b). Another shared pattern concerned transformations in work practices that IT veillance brings to traditional industries, such as healthcare (e.g., Doolin 2004, Stahl et al. 2012, Staats et al. 2017), universities (Alvarez 2008), trading and retailing (Wareham et al. 1998, Marsden and Tung 1999), transport (Shaw et al. 2000), and navy sites (Stanko and Beckman 2015).

In terms of *distinctive patterns*, the analysis reveals a significantly higher variety of actors involved in IT veillance, with more complex and intense Ww relationships. For example, governments use IT to collect data and regulate market traders (Tung and Marsden 2000) and monitor citizen tax activities (Williams 1996), online activism (Ameripour et al. 2010), and behaviors in special economic zones (Karanasios and Allen 2013). Other studies suggest that IT intensifies veillance by enabling multidirectional monitoring between buyers and sellers via online platforms (e.g., Dellarocas 2005, Kordzadeh and Warren 2017) and new IT-enabled tools and techniques of identifying, collecting, and managing data (Singh et al. 2011, Clemons and Wilson 2015). Summarizing our analysis, we propose the following.

**Proposition 1.** *IT increases the complexity and intensity of monitoring.*

**Table 3.** Summary of Shared and Distinctive Patterns for Actor Relationships

Actors							Ketopics
Organization	Employees	Customers	Other	Government	IT or Non-IT	Citation counts	
Shared patterns							
1	W	w			Non-IT	36	Diverse and complex effects of monitoring on employee behavior and productivity; monitoring in the corporate governance and board of directors
					IT	24	Diverse effects of monitoring on employee behavior and productivity driven by new technologies (e.g., RFID, ERP, AI, mobile IS); transformations of work practices
2		Ww			Non-IT	15	Impacts of employee self-awareness, self-regulation, and peer monitoring on job performance
3			Ww		IT	1	Third-party online and offline surveillance in teams
					Non-IT	2	Impacts of third-party limited monitoring or its avoidance on behavior outcomes
					IT	1	Neuro IS tool for monitoring and improving emotion regulation
4			W	W	Non-IT	1	Monitoring in total institution
					IT	1	Relationships between user privacy concerns and government surveillance
5	Ww				Non-IT	7	Interorganizational veillance in traditional industries (e.g., construction, sport)
					IT	3	Interorganizational veillance in industries that were transformed or enabled by IT
6	W	w			Non-IT	1	Customer secondary data collection via catalogs and magazine subscriptions
					IT	7	Customer data collection, disclosure, and sharing
Distinctive patterns							
1	Ww	Ww			Non-IT	3	Multidirectional monitoring between organization and employees
2	W	w		W		1	Veillance relationships in privatization of a state-owned enterprise
1	W	w	w	W	IT	1	Healthcare IS enabling multiple watchers and watched
2	W	w	w			2	IT-enabled systems and techniques of data collection and identification
3	W					8	IT-enhanced capability of making employees visible to their managers and peers
4	W	Ww	Ww			1	Predictions in crowd-generated data
5	Ww		Ww			4	Multidirectional monitoring on online platforms
6	w		W	W		1	Impact of customers' culture and state regulation on corporate information privacy
7	W		w	W		1	Monitoring of customer data in location-based services and its regulation by the state
8	Ww		w	W		1	Impacts of law on information collection and sharing of patient data
9	W	w	w	W	W	1	IT-enabled method of screening individuals for concealing information
10	Ww			W		1	Identity ecosystems
11	W		w			3	IT-enabled capabilities to collect and manage customer data
12	Ww			W	W	1	Market surveillance systems
13		Ww	Ww			1	IT-enabled multidirectional veillance of professional peers and their customers
14		w		W		1	Using IT to monitor traders' activities
15			Ww	W		1	Video surveillance enabling monitoring of citizen behavior by the state and by peers
16			Ww	Ww		1	Data collection in Iranian internet social networks
17			w	W		1	State regulation of individual tax agents

Note. ERP, enterprise resource planning.

**4.1.2. Increased Complexity of Ww Roles and Relationships.** Our analysis reveals that IT stimulates more complex and distributed roles of watchers and watched compared with non-IT settings. Table 4 summarizes the number of papers with three or more actors, two or more watchers or watched, and the number of papers with actors who are both watchers and watched. In the table, distinctive patterns of IT veillance suggest complex roles of being watchers and watched compared with non-IT veillance.

The watchers in IT veillance are often complex and distributed, with several watchers observing the same watched or where the watcher can be also the watched. Patients' data are collected by doctors that are monitored and regulated by governments (Rizq 2013). Complex and multiple roles of watchers tend to hold true for both veillance between organizations and employees (e.g. Mazmanian et al. 2013, Vance et al. 2015) and organizations and customers (e.g., Dellarocas 2005, Brynjolfsson et al. 2016, Kordzadeh and Warren 2017). For example, social media websites (e.g., TripAdvisor.com) enable complex Ww relationships: customers monitor and review hotels that monitor reviews by customers as well as reviews received by other hotels, while hotel accreditation services monitor and review hotels and customer feedback (Scott and Orlikowski 2014). Additional examples include the unintended disclosure of information or enhanced visibility of veillance actors to third parties via social networks (Kordzadeh and Warren 2017) or online communication (Zhang and Venkatesh 2013). Another trend is to study the government as a (co) watcher regulating the organizational collection of customer information via IT tools in a range of contexts, including location-based services, healthcare IS, and market surveillance systems (e.g., Li et al. 2015, Adjerid et al. 2016). Contact tracing during the 2020 pandemic is an example of the government as (co)watcher.

In IT veillance, the watched, traditionally subjects of veillance, become (co)watchers. Examples include citizen online social media activism (e.g., Ameripour et al. 2010), citizens using state-installed video surveillance systems in public places to observe other citizens and organizations (Allen et al. 2007), customers using IT tools to monitor eBay traders (Dellarocas 2005), and healthcare practitioners using surveillance IT to self-present to peers and clients (Visser et al. 2018). Hence, based on our analysis, we propose the following.

**Proposition 2.** *IT enhances the complexity of roles for the watcher and for the watched.*

**Proposition 3.** *IT enables highly interactional veillance watcher-watched relationships.*

## 4.2. IT Transformations of Veillance Goals

IT monitoring stimulates an increased variety of goals, as well as emergent and cocreated goals.

### 4.2.1. Increased Diversity of Goals and New Goals.

With some notable exceptions, our analysis indicates a greater diversity of goals in IT veillance. We provide detailed tables in Online Appendix D describing the coding results with respect to veillance goals. Table D1 shows the diversity of goals while the details on the important goals in non-IT and IT veillance are shown in Table D2 together with sample areas and illustrative studies for each goal. The one exception to increased goal diversity in IT veillance is profit, which is relatively more intensively studied in non-IT contexts. In non-IT veillance, the goals of profit and compliance are often cogoals to each other (e.g., Gentry and Shen 2013, Goranova et al. 2017). In contrast, in IT veillance, the goals of compliance and profit are increasingly interrelated with a greater diversity of other goals, such as provision of benefits (e.g., Kordzadeh and Warren 2017), discovery and documentation (Natividad 2014), influence (e.g.,

**Table 4.** Actor Involvement in IT and Non-IT Veillance

	Three or more actors	Two or more watchers (W)	Two or more watched (w)	Has both W and w (Ww relationships)	Total papers
Shared patterns					
Non-IT veillance	0	0	0	24	62
IT veillance	0	0	0	5	36
Distinctive patterns					
Non-IT veillance	1	1	0	3	4
IT veillance	8	22	12	18	30
Total in non-IT veillance	1	1	0	27	66
Total in IT veillance	8	22	12	23	66
Total (all papers)	9	23	12	50	132

Dellarocas 2005; Karwatzki et al. 2017a, b), and self-improvement (e.g., Astor et al. 2013).

Actors in IT veillance often pursue a wider diversity of goals across both shared and distinctive patterns of Ww relationships (see Table D3). The diversity is particularly evident in the shared patterns of *organizations watching customers* (Warkentin et al. 2017) and *organizations watching employees* (e.g., Marsden and Tung 1999, Anandarajan 2002). Furthermore, IT enables goals that are rare or too costly to pursue in non-IT veillance, such as discovery, documentation, provision of benefits, and prevention/protection. For example, the goal of *discovery* is rarely studied in non-IT veillance (see Riad 2005 for an exception) and is typically better facilitated with IT (Twyman et al. 2014), similar to the goal of *documentation* in the veillance of physician clinical activities (Rizq 2013) as well in the veillance enabled by algorithms (Scott and Orlikowski 2014). Likewise, the goal of *provision of benefits* is linked to IT-enabled decreased costs of data exchange between heterogenous participants (Kohli and Kettinger 2004, Anderson et al. 2017) and improved quality prediction of watched behaviors (Xu et al. 2009, Singh et al. 2011, Brynjolfsson et al. 2016). Several studies do admit that IT-enabled sharing of personal information among different parties can be beneficial (e.g., Kordzadeh and Warren 2017) and that provision of benefits is subjective among diverse watched (Dinev et al. 2008). Finally, IT stimulates the goals of *prevention/protection* in veillance within information management, economic efficiency, healthcare, and security (Vance et al. 2015, Adjerid et al. 2016). Therefore, we propose the following.

**Proposition 4.** *IT enables wide diversity of veillance goals across watcher-watched relationships.*

**4.2.2. Emergent and Cocreated Goals.** As the relationships between watcher and watched unfold, novel properties of goals emerge and evolve in IT veillance. For example, whereas an IS monitoring system was originally introduced to gain compliance, provide information, and influence clinical decisions by managers, some doctors being monitored used it for the provision of benefits (to negotiate more resources) (Doolin 2004). Similarly, a novel IS system designed to ensure employee compliance with respect to resources met resistance, leading to a new mutual goal of provision of benefits (access to resources) (Silva and Backhouse 2003). Alvarez (2008) discusses how an enterprise system was introduced for compliance in a large research university but led to loss of compliance, employee resistance, and the emergent goal of self-improvement, enabling employees' reskilling and system workaround. Mobile

technologies aimed at providing employees with more freedom have led to tighter control and compliance monitoring (Mazmanian et al. 2013, Leclercq-Vandelannoitte et al. 2014).

IT veillance affords opportunities for the watched to be involved in the (co)creation of veillance goals. In non-IT veillance, goals were traditionally a prerogative of the watchers; participation of the watched in goal creation was mainly limited to relationships of peer veillance. In contrast, the watched can participate in the cocreation of goals across a variety of IT veillance relationships, including developing new veillance goals beyond those deployed by watchers (e.g., Brocklehurst 2001, Iedema and Rhodes 2010). Wareham et al. (1998) discuss the introduction of an ineffective performance monitoring system in a large retail firm whose top managers originally designed it for control and compliance purposes. Instead, when the watched (technicians) were given authority to cocreate and improve the system with team self-improvement goals, the system became more effective and overcame resistance. Likewise, Iedema and Rhodes (2010) discuss how healthcare nurses codevelop goals, reflections, and interpretations of video-based surveillance in a hospital, enabling self-improvement and information provision to others to develop as emergent goals. Therefore, we propose the following.

**Proposition 5.** *IT enables emergent and cocreated veillance goals.*

### 4.3. IT Transformations of Veillance Apparatus

IT facilitates hard and mixed veillance mechanisms, enables diffusion of veillance mechanisms, and facilitates manipulative actions on the part of both the watchers and the watched.

#### 4.3.1. Prevailing Hard and Mixed Veillance Mechanisms.

In non-IT contexts, organizations typically rely on hard coercive veillance mechanisms to conduct VoB and softer mechanisms of persuasion for VoS and VoC (e.g., Courpasson 2000, Rutherford et al. 2007, Bernstein 2012). Distribution of hard and soft mechanisms differs substantially for IT veillance, and with some nuances this holds true across shared and distinctive patterns. Table 5 shows that papers discussing soft mechanisms in IT veillance are relatively few compared with cases discussing hard mechanisms.

IT enables location-based tracking of customers (Xu et al. 2009) and remote workers (Brocklehurst 2001, Leclercq-Vandelannoitte et al. 2014, Mazmanian et al. 2013), monitoring of theft in restaurants (Pierce et al. 2015), hospital employees' hand hygiene (Staats et al. 2017), concealed information (Twyman et al. 2014), traders' information access (Tung and Marsden 2000), illegal market trading (Li et al. 2015), and remote



**Table 5.** Distribution of Papers and Cases Discussing Hard, Soft, or Both Veillance Mechanisms

	Number of occurrences			Occurrences per pattern	% of Papers		
	Only hard	Only soft	Both		Only hard %	Only soft %	Both %
Shared patterns							
Non-IT veillance	25	15	22	62	40.3%	24.2%	35.5%
IT veillance	24	3	9	36	66.7%	8.3%	25.0%
Distinctive patterns							
Non-IT veillance	0	1	3	4	0%	25.0%	75.0%
IT veillance	13	6	11	30	43.3%	20.0%	36.7%
<i>Total across papers</i>	62	25	45	132			

patient health data (Singh et al. 2011). The intensiveness of veillance increases both for predominantly IT-mediated jobs, such as exhaustive monitoring in call centers (Deery et al. 2002), as well as jobs where IT monitoring complements offline activities, for example, electronic individual monitoring that increases peer scrutiny in teams (Sewell 1998) and shifting physicians' behaviors closer to congruence with management's goals (Kohli and Kettinger 2004). Tracking capacities embedded in IT tools (e.g., radio-frequency identification (RFID) tags, mobile devices, sensors) enable the monitoring of bodies and behaviors of employees beyond formal workplaces (Allmer 2011, Pierce et al. 2015). The possibilities and spaces for hard veillance mechanisms (e.g., marking of the body, physical inscription) are thus extended beyond fixed spatial locations to capture employee behaviors and bodies, both within formal and informal organizational spaces (Stanko and Beckman 2015) and in private locations (Brocklehurst 2001).

IT-enabled monitoring leads to the emergence of more intensive group-level norms that act as coercive mechanisms, including "anytime anywhere" norms of responsiveness (Guillemette et al. 2009, Lee 2017), self-regulation (Short and Toffel 2010), and self-auditing (Levy and Waks 2009). Dissolving traditionally bounded organizational veillance spaces can transform traditional panopticon veillance into a portable panopticon (De Saullés and Horner 2011), also referred to as "free control" (Leclercq-Vandelannoitte et al. 2014, p. 543), and postpanopticon (Baudrillard 2006, 2007; Sewell and Barker 2006) that relies on subtle and relatively invisible (but intrusive) veillance. IT intensifies government veillance with variable effects on the subjectification of the watched (Williams 1996, Stahl et al. 2012). For example, the UK National Health Service requires professionals to collect and document data on their patients using computers and standardized software, serving rational aims of state-funded health provision rather than subjective needs of patients, while persuading

patients to accept new norms (Rizq 2013). Based on the our analysis, we propose the following.

**Proposition 6.** *IT intensifies veillance conducted with hard or mixed (hard and soft) mechanisms.*

**4.3.2. Diffused IT Veillance Mechanisms.** Typically, in non-IT veillance, the watcher owns, designs, and implements control systems. IT enables veillance mechanisms to become diffused, that is, owned, designed, and implemented by actors other than the watchers. IT allows different actors (hotels, customers, government, and citizens) to perform intensive monitoring without owning the tools, but knowing how these are designed, and without controlling the implementation of the veillance mechanisms (Ameripour et al. 2010, Scott and Orlikowski 2014).

An emerging stream of research specifically discusses the roles and impacts of diverse, intermediate actors influencing processes and results of monitoring. Examples include third-party intermediaries who authenticate users before granting participation to data repositories (Crossler and Posey 2017), companies mediating and moderating reviews and message exchanges between customers and hotels (Scott and Orlikowski 2014), healthcare providers sharing medical and healthcare data (Adjerid et al. 2016, Anderson et al. 2017, Li and Qin 2017), and governments whose tracking of consumer online transactions and citizen data is increasingly justified to detect and prevent security breaches, fraud, terrorist activities, and other crimes (Dinev et al. 2008). Diffused IT veillance mechanisms also enable the watched to increasingly participate in the cocreation of norms and implementation processes of monitoring (e.g., Visser et al. 2018) and claim ownership of collected data (Spiekermann and Korunovska 2017). Thus, we propose the following.

**Proposition 7.** *IT enables the mechanisms of veillance to be owned, designed, and implemented by multiple actors beyond the watchers.*

**4.3.3. Manipulative Actions of Veillance Actors.** Both watchers and watched in IT veillance engage in reciprocally manipulative behavior. First, in non-IT monitoring, the watcher needs to make the watched *aware* that they might be visible for the disciplining effect of the panopticon to take place (e.g., Foucault 1977). Recent studies increasingly discuss the manipulative effects of IT monitoring that are unknown or invisible to the watched (e.g., Ball 2009, Kubitschko 2015, Newell and Marabelli 2015). For example, remote diagnostics technology embedded in physical products is often invisible to employees but might be used by companies to analyze their behavior (Jonsson 2006). Contrary to the panoptical model, the informative capacity of IT enables “uninformed” veillance (e.g., Newell and Marabelli 2015). Ethical responsibilities become vested in organizations (e.g., Jonsson 2006, Buhl and Mueller 2010), requiring further research that watches how these responsibilities are framed and discharged (Adelstein and Clegg 2015). Further, watchers can manipulate the visibility of information via IT tools, such as altering or playing with different features of monitoring systems (Grant and Higgins 1991), campaigning to get customers to write online reviews, or writing fake or defamatory reviews (Scott and Orlikowski 2014).

IT enables watchers to manipulate the behavior of the watched based on highly tailored veillance mechanisms (Kosinski et al. 2013, Howard and Woolley 2016). For example, sensors in cars can be used to collect data in real time to modify driver behavior through punishments (real-time rate hikes, financial penalties, curfews, engine lockdowns) or rewards (rate discounts, coupons, gold stars to redeem for future benefits) (Zuboff 2016). IT allows for government attempts to influence public opinion with counter propaganda movements (Ameripour et al. 2010), but even more powerful is the facility to play to dispositions that require no implanting but are already there, merely awaiting recognition. The recognition is twofold: first, by veillance and its messages and, second, by the gaze of familiarity with which the messages are received by those who become their subjects. The use of Facebook data by Cambridge Analytica on social network “likes” was premised on such foundations (Clegg et al. 2019): bots projected messages to those who probabilistically estimated to be empathetically open to the messages sent. Empathetic tendencies, once known, can be curated and manipulated. Research provides increasing evidence of the application of this new model by organizations, such as when companies provide real-time situated and personalized feedback to selected employees via private chats (Stanko and Beckman 2015), evaluate employee behavior via appliances with embedded remote diagnostics technology (Jonsson

2006), or directly access consumer appliances in households (Warkentin et al. 2017).

IT veillance enables various manipulations by the *watched*. In non-IT settings, visibility is often imposed on the watched in VoB (e.g., factory floor worker uniforms, compulsory Jewish badges in Nazi Germany) that internalizes goals and complies with team or organizational norms in VoS and VoC (Clegg et al. 2006). In contrast, the watched can creatively use IT to manipulate their visibility in VoB. Thus, the watched in IT veillance can manipulate visibility of their behavior to get more resources from the watchers (Doolin 2004), maintain otherwise challenged access to resources (Alvarez 2008), diversify production reporting between team members and managers (Bernstein 2012), and remain unnoticed despite being constantly observed by video (Anteby and Chan 2018). The watched also use IT systems to manipulate their visibility in VoS and VoC to enable displays of professionalism to increase their status and appraisal in the eyes of the watcher (Vieira da Cunha 2013, Visser et al. 2018) and to present a false visibility to management providing an impression of compliance (e.g., Vieira da Cunha and Carugati 2009). IT users can exchange visibility/privacy aspects for some benefits (e.g., Dinev et al. 2006, Pavlou 2011, Bélanger and Crossler 2019, Crossler and Bélanger 2019). Under conditions of IT veillance, “subjects participate, to a significant extent, in the very construction and institutionalization of the virtual cells which are used to categorize them” (Brivot and Gendron 2011, p. 152). Thus, we propose the following.

**Proposition 8.** *IT facilitates manipulations of veillance by both the watchers and the watched.*

#### 4.4. Transformations to Veillance Foci

Our analysis illustrates that IT enables veillance of all three foci, but research privileges investigation of VoB. As Table 6 highlights, the relative percentage of papers studying VoB is higher in IT veillance across both shared and distinctive patterns of the watcher-watched relationships. Furthermore, IT dynamically shapes and dramatically transforms the epistemology of the focus of veillance. In non-IT veillance, the focus of veillance is known in advance and the interests of the watchers in the watched is preconceptualized as focusing on a particular aspect (body, soul, or commitment). Such veillance, structured around known a priori focus, aligns with other elements (e.g., the particular actors, apparatuses, and goals). Accordingly, mixed veillance foci (e.g., VoB and VoS) in non-IT veillance relies on two or more systems of veillance specifically designed to support each particular focus. For example, VoB relies on a system of veillance enabling the monitoring of employee bodies and

**Table 6.** Distribution of Veillance Foci Across Shared and Distinctive Patterns

	Occurrences per foci per pattern			Occurrences per veillance type	% of Occurrences of veillance foci per pattern		
	VoB	VoS	VoC		VoB	VoS	VoC
Shared patterns							
Non-IT veillance	39	29	3	71	55%	41%	4%
IT veillance	31	9	3	43	72%	21%	7%
Distinctive patterns							
Non-IT veillance	3	3	1	7	43%	43%	14%
IT veillance	25	7	5	37	68%	19%	13%
Total in non-IT veillance	42	32	4	78	54%	41%	5%
Total in IT veillance	56	16	8	80	70%	20%	10%
Total cases across all papers	98	48	12	158			

behaviors, whereas VoS focuses on specially planned and established organizational or team culture.

In contrast, IT enables the foci of veillance to be dynamically shaped and emerging during the process of veillance, as discussed in Table D4. The original focus of IT veillance on body and behavior (VoB) of the watched is often complemented with an emergent VoC and VoS focus. The original IT veillance of workers' location, time, and frequency of emails and online activities is often complemented by emerging norms for continuous responsiveness, availability, and engagement that display employee commitment and professionalism (e.g., Kohli and Kettinger 2004, Visser et al. 2018). Additionally, an emerging culture of individual addiction to devices enabling continuous peer visibility and collective monitoring of information flows can also occur (e.g., Mazmanian et al. 2013, Stanko and Beckman 2015).

The analysis of the literature also reveals a possible extension of veillance foci to a new dimension, namely, the *veillance of the future* being inscribed in the candidate's present through the veillance of traces of their past. IT automatically facilitates the cumulative aggregation of personal data from multiple databases to use for simulation of the future. For example, information aggregation and verification firms such as Choicepoint offer aggregation of data such as pre-employment screening of bankruptcy records, civil cases, liens, criminal records, education and employment histories, media coverage, judgment histories, credit reports, and address and driving histories (Allmer 2011). IT veillance then becomes increasingly used for predicting "the likelihood of this or that person turning out to be a responsible and hard-working employee" (Lyon 2001, p. 41), anticipating the patterns of future behavior of the watched (Stanko and Beckman 2015), and making visible "who the worker *will have been*, what the worker *will have produced*, what path his or her career *will have taken*"

(Bogard 1996, p. 117). Veillance of the future not only makes probabilistic bets on what will happen but also leads to the active formation, manipulation, and limitation of the "free" choices of those whose data traces are being watched (Zuboff 2015, 2016). The intensely media-debated case of Cambridge Analytica's massive use of IT-facilitated cumulative aggregation of personal data, including its use for veillance of future and related manipulations and its consequences for democracy, provides an illustrative example in this regard (Clegg et al. 2019, Metcalf 2018, Tas and Kimpen 2020). The current relatively small amount of research on this topic, particularly in terms of the ethical implications, requires extension.

To summarize, instead of a prefixed focus of interest (e.g., body, soul, commitment), the watched become dynamic and unique subjects for which IT-mediated veillance systems are crafted. Veillance can be dynamically adjusted, mixed, and/or extended in its focus. Therefore, we propose the following.

**Proposition 9.** *IT enables emergent and dynamically adjusted veillance foci.*

## 5. Theoretical Implications

What elements of the veillance system are transformed by IT and *how* they change has been theoretically analyzed (Whetten 1989). Our findings reveal significant IT-enabled transformations of all elements of the veillance system and the relationships between the watcher and the watched. Based on our findings and further reflection of how these transformations relate to each other, we develop an action net model of IT veillance in the digital age.

### 5.1. Action Net Model of IT Veillance in the Digital Age

An action net is a system of differentiated actors loosely or temporarily related by the constitutive

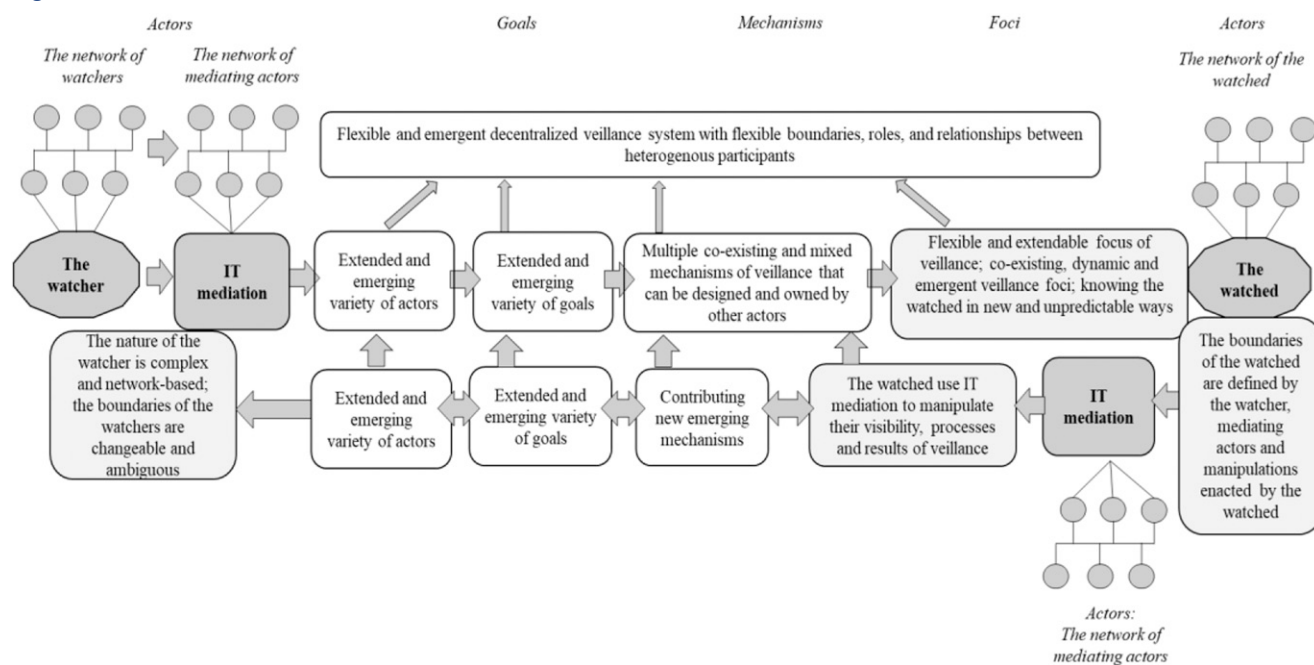
work of the system (Czarniawska 2004, Lindberg and Czarniawska 2006). The IT veilance action net model is produced by the actants and actions of heterogeneous veilance actors, their diverse goals, flexible roles and relationships, apparatuses, and boundaries, which together create dynamic and multiple foci.

In conventional (non-IT) monitoring systems, relationships between the watcher and the watched are typically unidirectional (e.g., top-down or bottom-up) or lateral (e.g., peer veilance), with goals being defined prior to veilance. The participating actors are known in advance and the apparatus of veilance is constructed before the act of monitoring to enable a particular focus for the veilance (body, soul, or commitment). Each conceptualization requires a different design in terms of actors, goals, and veilance mechanisms; they are not mutually exclusive and can be used additively. In the action net model of IT veilance, the relationships between the watcher and the watched are mediated by actant devices that are multidirectional and allow for diverse manipulations. Goals might emerge before and after the act of veilance, relating to participating actors who are multiple, heterogeneous, emergent, unbound, and often unpredictable. Relationships between the watcher and the watched may be mediated by a variety of intermediate actors and actants that can be involved in various complex and flexible roles with the watchers and the watched. For instance, during the 2020 pandemic, the role of phone manufacturers, such as Apple, in refusing to share location information forced governments to rethink tracing strategies (Fowler 2020). In consequence, rather than

relating users to central databases, several governments opted for more decentralized approaches supported by Apple and Google phones (Busvine and Rinke 2020). These strategic shifts underline the changeable boundaries of the veilance system and multiple veilance foci. Figure 2 illustrates the IT veilance action net model.

Existing models, such as the panopticon and synopticon (e.g., Foucault 1977, 1982) focus on a fixed set of actor relationships and roles or are based on data flows enabled by IT networks in which actors are no longer central, such as dataveillance, assemblages, and panspectron models (Deleuze and Guattari 1987, Haggerty and Ericson 2000, Haggerty 2006). The action net model of IT veilance differs significantly. It brings the relationships between actors to the center of the analysis and presents veilance as a flexible and emergent decentralized interconnected web with flexible boundaries, roles, and relationships between heterogeneous actors and actants involved in the system of veilance. It illustrates that the net is not defined by the structural/hierarchical position of the actors but by the relationships between heterogeneous veilance participants and their cumulative abilities to organize, impact, and otherwise manipulate the net, including influences on the dispositions of roles, visibilities, and inclusion/exclusion of other relevant actors and intermediates. In this regard, our model builds on and extends calls to rethink the role of the watched in IT monitoring as no longer passive (Scott and Orlikowski 2014, Anteby and Chan 2018, Visser et al. 2018).

**Figure 2.** Action Net Model of IT Veilance





The action net does not define a particular pre-defined actor relationship pattern or set of organizational boundaries (Czarniawska 2004) but is continuously reestablished by flexible system relationships, enabling multiple dynamic foci coshaped by inputs from flexible watchers, watched, and intermediate devices and actants. In the action net model, there are diverseveillance participants and roles; for instance, research can focus on intermediate participants, such as companies campaigning for customers to write reviews (Scott and Orlikowski 2014), watchers disabling consumer appliances or internet access (Stanko and Beckman 2015, Warkentin et al. 2017), as well as attempts to counter propaganda movements by governments (Ameripour et al. 2010). Additionally, research can focus on those that are watched who become self-aware and learn to cocreate and manage how they might be (in)visible and self-present and attract resources and attention to the watched (Doolin 2004, Brivot and Gendron 2011, Anteby and Chan 2018, Visser et al. 2018). By changing their visibility, actors can manipulate the action net, thus blurring boundaries between preestablished roles.

The action net model is particularly useful for describing complex and flexible Ww relationships in the digital age. For example, instead of explaining COVID-19 contact-tracing surveillance as based on predefined Ww relationships or data flows and assemblages, the action net model focuses on a flexible web of Ww relationships, roles, and boundaries that emerge out of unprompted interplay between heterogenous actors (governments, healthcare organizations, citizens, and diverse intermediators, such as computer, app and internet providers). For instance, the German government initially backed a centralized contact-tracing standard known as the Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT), which required Apple to change the settings on its iPhones, which it declined to do; hence, Germany opted for a decentralized approach that involved users opting to share their phone number and details of symptoms (Busvine and Rinke 2020). The action net model also allows considering multiple and dynamic foci ofveillance. For example, as debates on obligatory use of Covi-passes (<https://www.covipass.com/>) reveal, whereas COVID-19 contact tracing might start as VoB, it may soon evolve into VoS/VoC (McCurry 2020).

The action net model ofveillance offers two important theoretical advantages. First, it captures IT-enabled flexibility, complexity, unpredictability, and constant evolution of heterogenous actors and their relationships as transformative IT impacts in monitoring (e.g., Haggerty 2006; Mann and Ferenbok 2013; Leclercq-Vandelannoitte et al. 2014; Zuboff 2015, 2016). Second, the model suggests new logics underlying the relationships between the watcher and the watched.

## 5.2. New Logics of Action Net IT Veillance Systems

In action net ITveillance systems, new logics characterize the relationships between the watcher and the watched. The underlying logics of the action net functionalities are enabled by the unique characteristics of IT artifacts such as their editability, distributedness, granularity, interactivity, and reprogrammability (Manovich 2001, Garud et al. 2008, Kallinikos et al. 2010, Yoo et al. 2010) (see Table 2), which existing studies onveillance have yet to incorporate in knowledge and assumptions about IT artifacts. Such emerging understanding of IT artifacts is particularly useful for grasping how the functioning of ITveillance systems and the relationships between the watcher and the watched are affected by the transformations identified in the findings. We next discuss the proposed logics in contrast to the assumptions of extant monitoring theories, highlighting the underlying reasoning of the logics, as well as research questions and areas for future research. Table D5 in Online Appendix D summarizes our arguments.

**5.2.1. Flexibility of Veillance Elements.** The elements of the action net model of ITveillance are flexible and dynamically changing. In traditional theorizing, both the watchers and the watched constitute specific group(s) of actors who operate in a given context defined by the basic relations of power and authority that constitute the employment relations characterizing specific organizations. IT-mediatedveillance systems are, by contrast, unbounded in terms of the scope and nature of participating actors and diversity of their relationship patterns. Likewise, goals, mechanisms, and foci become flexible and dynamic in the ITveillance system.

Unique characteristics enable the functioning of ITveillance systems on this new logic. For example, *IT editability* (Constantiou and Kallinikos 2015) enables multiple actors (e.g., not only watchers but also watched and intermediate actors) to adjust diverse elements ofveillance, such as changingveillance goals, mechanisms (e.g., changing between OFF to ON settings for exposure notifications), or the focus during the process ofveillance or (re)discovering and (re)creating the actual focus based on the already collected data. The *distributedness of IT artifacts* creates a network environment that is borderless; that is, where, as a result of IT-enabled interconnectedness (Kallinikos et al. 2010), organizational boundaries do not exist. A heterogeneous and unbounded constellation of actors can participate, such as telephony carriers, mobile-phone operating systems (OSs) (Apple, Google), apps on top of OSs, as well as privacy advocates, miscellaneous technology vendors, and so on (Nambisan et al. 2017). Diffused agency ofveillance acts as another source of flexibility; diverseveillance

goals and mechanisms can be owned, designed, and used by multiple actors, facilitating cumulative aggregation of personal data from multiple databases that enable simulation of future behavior, preferences, and possible commitments of those being tracked through data traces (e.g., Marx 2002, Baudrillard 2006, O'Harrow 2006, Mayer-Schönberger and Cukier 2013, Marwick 2014, Van Dijck 2014). *IT granularity* enables multiple actors to introduce tailored changes to veilance goals, mechanisms, and foci, increasing the flexibility of the veilance process beyond the full control of the watchers. For example, employee knowledge about how different blocks of IT surveillance systems are connected and what their gaps and knowledge spots are enables their practices of invisibility (Anteby and Chan 2018). This is also one of the reasons why IT veilance over outsiders is easier than IT veilance over insiders, whose awareness of local knowledge and specificities creates more room for unexpected deviations in organizational information security (Vance et al. 2013). Likewise, *interactivity* of IT enables reinvention of veilance goals; for instance, when information collected by companies such as Choicepoint or Acxiom can be packaged and resold to interested actors (Turow 2011). An original veilance goal of profit might become associated with prevention of risky behavior and protection of resources (D'Arcy et al. 2009, Stahl et al. 2012, Vance et al. 2013). Location data can be used after the fact for contact-tracing purposes, and Clearview AI face recognition technology can use scraped images for completely different purposes. Clearview scraped images from sites such as Facebook and LinkedIn over their objections, which, while clearly unethical, is borderline legal. Finally, *IT reprogrammability* further extends veilance flexibility, enabling dynamic adjustments of veilance elements (goals, foci, mechanisms) as veilance proceeds (Jonsson 2006, Stanko and Beckman 2015, Warkentin et al. 2017).

These new logics create profound implications for the design of veilance systems. In particular, they imply a need for theorists and practitioners to design IT veilance systems for incompleteness (Garud et al. 2008) by focusing on pragmatic and emergent system design approaches that allow for the exploration of systems in which boundaries, system elements, and characteristics are not stable and where there might be multiple designers, with diverse visions of the veilance system boundaries and characteristics.

**5.2.2. Diffused Actor Roles.** The action net IT veilance system implies that various veilance participants might engage in multiple roles simultaneously on an emergent diffused basis. In contrast to non-IT veilance, where the watcher and the watched acquire their roles because of an a priori designated structural position, actors in the action net system acquire their

roles in the process of watching or being watched by other actors in the action net. The new logics challenge the conceptualization of the watchers as a central and coherent group of actors. They imply that the watcher(s) will be an emergent and distributed net of multiple actors whose heterogeneities might create important complementarities, extending joint capabilities but also creating unexpected tensions. As our analysis illustrates, multiple actors can participate in monitoring as watchers through associations and networks. Likewise, the new logics challenge conceptualizations of the watched as simply following or resisting their roles as defined by the watchers exercising veilance. Instead, the watched in the action net can be actively involved in the veilance process through IT-enabled manipulations and activation of various intermediators that shape the boundaries between the watcher and the watched as changeable, ambiguous, and subject to networked relationships.

The aforementioned logics are enabled in important ways by the IT characteristics discussed in Table 2. *IT editability* enables an easy alliance with new veilance actors as well as an exit from existing ones by bypassing the original watcher and various inclusive intermediated actors (e.g., monitoring system vendors, information aggregation firms, experts supporting and interpreting IT systems). For example, mobile carriers can sell location information to less-well-known data aggregation companies that sell the data to operators such as bounty hunters (Valentino-DeVries 2020). *IT distributedness* enables the watched to collect and store information with multiple IT devices, thus cocreating their veilance (Brivot and Gendron 2011, Leclercq-Vandelannoitte et al. 2014) and reversing the visibility of veilance actors, so that the watchers can be known to the watched, who can be concealed and anonymized. For example, in TripAdvisor, relevant hotel managers can be known to the anonymized public of online reviewers and platform users (Orlikowski and Scott 2014). Together, *IT editability* and *distributedness* enable multiple diffused monitoring actors and actants to generate much more detailed and diverse information about the watched, increasing the probability that they will be known in new ways (e.g., Kosinski et al. 2013, Vieira da Cunha and Carugati 2013, Pierce et al. 2015, Howard and Woolley 2016), while also unintentionally increasing their visibility to third parties (Leonardi 2014, Leonardi and Vaast 2017). Instead of being known through a predesigned veilance apparatus that has a specific focus for monitoring, those watched become known through the network of mobilized mediating actors and actants. Such mediation allows veilance to build simultaneously on multiple foci (body, soul, commitment) and to inscribe multiple actant boundaries to learn continuously about the watched in many

emergent ways (Barad 2007, Orlikowski and Scott 2014). Further, *IT granularity* enables data about those watched to be broken down into minute details (e.g., fitness devices that provide self-monitoring of water intake, heart rate, and sleep stages), which enables the engagement of the watched in the (co)-construction ofveillance mechanisms by deciding what to make visible within theveillance system. *IT granularity* also contributes to the diffusion of actor roles by enabling some devices of ITveillance to act as agents themselves, such as bots and algorithms, sometimes beyond the ways specified by the IT designers (Statt 2020). Likewise, *IT interactivity* enables the watched to modify the original uses of IT and become cocreators of ITveillance systems (Doolin 2004, Alvarez 2008, Brivot and Gendron 2011, Anteby and Chan 2018), thus blurring preassigned roles. Finally, *IT reprogrammability* enables a performative inclusion/exclusion of the intermediate actors to the conceptualizations of the watched and their real-time and future behavior modifications. For example, the new automotive telematics industry uses intrusive surveillance capabilities to combine the monitoring of locations and conditions of vehicles with impressive amounts of knowledge of personal data about the driver that can affect real-life driving behavioral modifications (Zuboff 2016).

The aforementioned logics condition areas for future research on the dynamics ofveillance systems, including the formation of diffused actor roles and their continuous change, (re)negotiation, interplay, and tensions. Table D5 in Online Appendix D details areas for future research in this area.

**5.2.3. Cumulative Extended Manipulations.** The action net ITveillance system operates on a logic of cumulative extended manipulations of diverseveillance participants. As discussed in Section 4, in ITveillance, both the watchers and the watched can engage in diverse manipulations previously impossible in non-ITveillance. Extended manipulative capabilities of the watchers include nonhuman oversight and action on the watched and possibilities to useveillance systems owned by other actors, as well as tailoredveillance mechanisms (e.g., predictive bets). The latter, in particular, enable the watchers to surpass significantly non-IT panoptical models derived from Foucault that are alert to the ever-present possibility of the experience of being under surveillance, leading to normalization of the watched. In contrast, ITveillance already takes patterning for granted, as it merely needs to work with that which is already constituted, for example, through the knowledge of Facebook likes and networks, which can be used to frame a message accordingly (Clegg et al. 2019). Likewise, extended manipulative capabilities of the watched significantly exceed those relatively limited manipulations

available to the watched in non-ITveillance, including “systematic soldering” (Clegg et al. 2006), “work-arounds” (Seaman and Erlen 2015), or “making out” games (Roy 1959, Burawoy 1979). In contrast, the watched in ITveillance can (co)create and manage their visibility and engage various intermediate actors to further manipulateveillance processes and results. Finally, intermediate actors can also engage inveillance manipulations. Such extended manipulative capabilities emphasize the importance of cumulative manipulations rather than manipulations of specific actors.

The logic of cumulative extended manipulations is enabled by specific IT, similar to previous logics. *IT editability* enables the watched to be continuously engaged in managing their visibility. For example, the watched who use virtual private network (VPN) applications to access region-restricted websites need to continuously upgrade their available applications as the watchers learn to block these. Likewise, those who seek to increase their visibility (e.g., marketing graduates promoting themselves on social media accounts to catch the attention of potential employers) need continuously to modify their IT choices to upgraded settings to stay competitive. *IT distributedness* enables intermediate actors to shape the action net of ITveillance beyond direct watchers and watched and beyond particular organizational boundaries (Czarniawska 2004). As remarked when discussing sousveillance, a murder by a policeman, captured on video, had significant effects for the now-global Black Lives Matter movement. The action net model provides a valuable framework demonstrating how a simple mobile phone video can have global effects as an intermediary device. *IT distributedness* also enables those watching to employ a system ofveillance owned by others instead of constructing their own. As illustrated by the case of Cambridge Analytica, such intermediate actors can use already-existing relationships (e.g., data collection of Facebook on its users) to build their own adjustedveillance system. *Granularity of IT* facilitates unique tailoring and adjustment ofveillance mechanisms for each subject of monitoring. *IT interactivity* enables users to activate different IT functions, thus enabling both watchers and watched to play with visibility and anonymity, exchange a part of their visibility/privacy for some benefits (Pavlou 2011, Bélanger and Xu 2015, Bélanger and Crossler 2019), or use IT for manipulative purposes in ways that empower them (Albrechtslund 2008, Ellerbrook 2010, Eslami et al. 2015). For example, online political content is often programmed to be commented on by bots in a radical way that attracts multiple responses and increases visibility (and thus importance) of the comment to a general public. Finally, *IT reprogrammability* enables newveillance mechanisms not



possible with non-IT tools, such as hyper-real simulation, data veillance, and real-time behavior modification capability by manipulating in process those being watched but unaware (Jonsson 2006, Ball 2009, Zuboff 2015, Howard and Woolley 2016). For example, Facebook users are largely unaware that the Facebook Newsfeed algorithm influences which stories and posts are visible from the pool of all stories and posts (Eslami et al. 2015). *IT reprogrammability* also enables the watched, as much as the watchers, to engage a variety of mediating actants to manipulate the processes, results, and visibilities of monitoring. For example, participants in TV game shows (or any other ranking-based system) could use bots and algorithms trained on profiled data to persuade others to vote for them or to bury unfavorable news or reviews deep in Google's lists. Furthermore, *IT reprogrammability* enables replacing human oversight with algorithms, bots, and the internet of things that not only collect, store, and analyze data but also trigger responses to humans and other actants (Jonsson 2006, Newell and Marabelli 2015). For instance, bots are widely used on Twitter (with approximately 30 million active accounts being bot driven) to mimic human actors so as to boost follower numbers and retweet content. Bots are also utilized on Wikipedia to track government employees' edits to Wikipedia or on Facebook to attack opponent conversations (Woolley and Howard 2016), but they have limits: they cannot recognize fluid and subtle phenomena, such as irony, which cannot be described in simple, machine-readable rules. Nonetheless, these developments allow veillance systems to function without the need of supervisors to approve work, removing from the existing system established mechanisms of checks and balances, while also allowing manipulations in new ways on a massive scale.

The aforementioned logics trigger important implications that require further analysis. The key implications and areas for future research relate to the functioning of IT veillance systems as relying on cumulative extended manipulations by multiple actors as well as to power construction and enactments. Thus, those being watched that are neither aware nor skillful in IT and in managing their action nets, or who lack resources to be able to do so, can become subject to manipulations by multiple watchers with the power to shape their experiences and curate goal internalization. In IT-mediated veillance, visibility becomes both a tool of control and of presentation of self in which it becomes important to be visible to the right person in the right ways. One can use visibility as part of the appraisal of one's own and peers' work and commitment (Brocklehurst 2001, Leclercq-Vandelannoitte et al. 2014); this can encourage the use of socially accepted behavior and expectations of being visible (Mathiesen 1997, Pecora 2002) in order to avoid

exclusion from benefits and resources. These changes have an important potential to affect employee accountability, responsibility, and knowledge sharing (Denyer et al. 2011, Aral et al. 2013, Miller and Tucker 2013, Leonardi 2014, Dong and Wu 2015, Huang et al. 2015, Leonardi and Vaast 2017). The system of embodied dispositions and tendencies that organize the ways in which individuals perceive the social world around them and react to it, the *habitus*, is affected. The ability to manage visibility and opt out of being monitored becomes an aspect of power in modern organizations.

**5.2.4. Emergent Nonlinear Actor Relationships.** Classically, organization was founded on labor processes in which communication, coordination, and control based on preplanned actor behavior and focus of veillance were central to efficient exploitation of resources (Clegg and Dunkerley 2013). Monitoring provided a critical practice in this regard, enabling the watcher to plan and predict the behavior of the watched (Clegg et al. 2006). Compared with extant theories that consider IT as an enabling tool for enhanced control and predictability, the action net model of IT veillance builds on a new logic that favors unpredictability and emergence of the participating actors and their relationships (e.g., Nambisan et al. 2017).

Specific IT properties guarantee the emergence of actor roles and relationships and limited or temporary control over monitoring systems. *IT editability* motivates diverse veillance actors to continuously update and refine their roles, participation, and dynamics in IT veillance. Instead of traditional conceptualization of watchers as active and powerful actors and the watched as passive recipients (e.g., Anteby and Chan 2018), the action net model of IT veillance conceptualizes roles and relationships between diverse actors as emergent, nonlinear, and subject to potential changes and modifications. *IT distributedness* allows the watchers and the watched to be expanded to unplanned "others," a process that will inevitably disturb previously delineated roles, dynamics, and modes framing watcher-watched relationships. Consider, for example, social media influencers allowing visitors to watch, while at the same time the visitors are being watched by YouTube/Google as well as, to a limited extent, the influencers. IT distributedness further contributes to emergent and nonlinear actor relationships by enabling an unbounded variety of actors who might participate in the veillance system in various ways, following diverse goals, constructing their own, or using other actors' mechanisms of veillance, dynamically changing veillance foci, as we have seen with the development of contact-tracing apps during the COVID-19 pandemic. *IT granularity* enables increased knowledge about the watched in a



diversity of areas, often in unpredictable and emergent ways (Zuboff 2015, 2019). *IT interactivity* contributes to emergent actor relationships in IT veillance nets through the interplay of compatibilities (or lack of these) across diverse actors, goals, mechanisms, and foci. For example, those developing algorithms for data collection might inscribe different assumptions in the code compared with how the watchers use the technology (Newell and Marabelli 2015), enabling the development of less predictable and stable IT veillance systems. Emergent veillance action nets can deviate significantly from those originally designed and may not be fully controlled by those watching the functioning of IT monitoring systems, suggesting important changes to the design and functioning of an effective veillance system. *IT reprogrammability* contributes dynamic and emergent changes in the IT veillance system by enabling mobilizations of both human and nonhuman actants as networks of mediating agencies. In non-IT veillance, the mediating agencies are usually specialized personnel, such as frontline supervisors (Dunkerly 2013). The more distributed IT is in terms of supporting agents, the more complex and branched will be the system of mediating agencies that might influence monitoring. Communication, coordination, and control switches from being relayed and mediated through actors to being embedded in actants as the passage points in circuits of power (Clegg 1989).

The aforementioned logics of emergent nonlinear actor relationships imply a need to rethink the effectiveness, design, and power enactment in IT veillance systems as no longer apparatuses attuned to a particular type of veillance system. Instead, their effectiveness depends on incorporating multiple related and networked actors within action nets, the ability to influence the inclusion/exclusion of actors or to manipulate others, as well as the ability to defend themselves from others' manipulations. The power of the watched and intermediate actors who can use IT to manipulate gaze and visibility, and thus coshape the veillance system in emergent ways, needs to be taken into account. In particular, future research is needed to rethink the criteria of effectiveness and key sources and agents of power in IT veillance systems, possibilities of systematic patterns in the emergent dynamics of actor relationships, and impacts of inclusion/exclusion of certain actors on the disposition of other actors in the action net (see Table D5).

### 5.3. Future Research

In addition to the aforementioned recommendations for future research, our findings suggest the need for studies in two major areas. First, we identified several gaps in knowledge of veillance elements. With regard to *veillance actors*, some relationship patterns, such as

employee peer veillance and organizational peer veillance, have received less attention in IT veillance as compared with studies of non-IT veillance. Second, with some rare exceptions (e.g., Ameripour et al. 2010), our analysis of veillance actors indicates that the government is almost never the watched in either IT or non-IT veillance. With an ever-increasing role of government in data collection in many critical domains of healthcare, security, and education, more research is required in this area. Third, some topics are exclusively studied in non-IT settings, such as monitoring of corporate governance and boards of directors (e.g., Benaroch and Chernobai 2017, Goranova et al. 2017) and might benefit from studies of veillance enabled by IT. Further research on the practices and implications of the manipulative aspects of *veillance mechanisms*, as well as dynamically shaped *veillance foci* and veillance of the future, are required. In particular, further research is needed on the ethical implications of veillance of the future, which involves the formation, manipulation, and limitation of the “free” choices of those whose data traces are being watched.

The new logics of the action net model suggest important questions and areas for future research. Thus, following the logics of *editability of veillance elements*, research is needed to shed light on the design of unbounded systems. In particular, future studies need to develop methods for designing deliberately incomplete and emergent IT veillance systems (Garud et al. 2006, 2008) with flexible boundaries and elements, examining whether and how the primary patterns of the watcher-watched relationships influence how veillance systems evolve, and exploring the problem of compatibility when multiple designers' visions of the veillance system boundaries and characteristics do not cohere. Following the logics of *distributed and interactive actor roles*, further studies are needed on the complex and nonlinear relationships between heterogenous watchers who might compete in circuits of power to manipulate each other. The complex multiactor and distributed nature of the watchers' impacts on the design of monitoring systems enabled by the specific properties of IT artifacts has yet to be incorporated by theories of monitoring and requires further studies.

The logics of *cumulative actor manipulations* imply that the functioning of the veillance system and its boundaries, visibility design, and power dispositions are cocreated by a multitude of actors. Further research is needed regarding the functioning of veillance systems: How do the interplays of various actor manipulations impact elements of the veillance system and actor boundaries and roles? How do veillance actors in different roles manipulate veillance systems? The logics also underline a need to reconceptualize

power relations in IT veillance. In particular, what is the relational role of IT expertise and mastering for manipulation? What relationships allow veillance systems to be manipulated without ownership? How can some actors involved in social or organizational relations opt out of monitoring? Future research needs to understand the formation of new monitoring modes of power that enable some watcher(s) to engage, orchestrate, and manage other heterogenous watchers, for example, the construction of the Social Credit System with which the Chinese government collects massive information about citizens from multiple heterogenous watchers (Liang et al. 2018). In this regard, more research on understanding the IT expertise of the watchers (e.g., in designing and using algorithms and bots) and their capacity to interpret and manipulate the network of related actors is needed. Skills need to be honed not only in IT but also in network effects on extant action nets of these actants: How do the strategic contingencies change, for example, when the obligatory passage points flow through actants that transform the relations of actors? Likewise, theories of organizational monitoring need to explore and develop insights into IT-enabled power of the watched to manipulate and influence monitoring. An important area of research in this direction would be to understand how activation of diverse action nets of watchers with diverse goals and mechanisms of veillance might generate diverse conceptualizations of the watched.

Finally, following the logics of *emergent and nonlinear actor relationships*, studies need to further elaborate and explore a variety of situated impacts of the unpredictability and emergent nature of monitoring systems in terms of effectiveness, design, and power relations. What particular criteria and sources of effectiveness might be applied to IT veillance systems with emergent and nonlinear actor relationships? Do any systematic patterns exist in the emergent dynamics of actor relationships? How does the inclusion/exclusion of certain actors change conceptualizations of the watched and the dispositions of other actors and roles? What are the key sources and agents of power in the action net model of IT veillance?

## 6. Limitations and Conclusion

Whereas an in-depth review allowed us to identify fundamental transformations enabled by IT, we cannot claim to have conducted an exhaustive review, although we have provided a foundation for exploring contemporary complex and multifaceted IT veillance on which further research might build. Our findings reconceive contemporary monitoring, aligning with various authors who note the necessity of doing so (e.g., Sewell 1998; Haggerty 2006; Mann and Ferenbok 2013; Leclercq-Vandelannoitte et al. 2014; Zuboff 2015, 2016). We have not had space to discuss the numerous

ethical issues and concerns associated with the IT transformations identified. Nonetheless, in line with other research in this area (e.g., Newell and Marabelli 2015; Zuboff 2015, 2019), we agree that such a discussion is fundamentally important. The proposed model provides a frame for much needed research in IT monitoring, including its ethical implications. We only reviewed papers from leading journals in two fields, which influenced our total counts and may not reveal all that is known about veillance. Finally, whereas this study focused on contrasting IT and non-IT monitoring to explore IT-enabled transformations, it paid limited attention to the possible effects generated by the interplay between non-IT and IT monitoring (e.g., Ajunwa et al. 2017).

To conclude, the paper pioneers the exploration of organizational transformations enabled by IT devices, artifacts, and capabilities. Based on the proposed veillance concept, typology, and framework, we analyzed the literature and identified key IT-enabled transformations in organizational monitoring, developed an action net model of IT monitoring, and proposed key logics on which IT veillance in the digital age operate. We also highlighted important implications of our findings for the design and functioning of systems of IT monitoring, as well as issues and relations of power and control within these.

## Acknowledgments

The authors thank two anonymous reviewers and Senior Editor Ann Majchrzak for valuable comments and helpful suggestions on ideas presented in this paper.

## Endnotes

<sup>1</sup> Formal definitions of *watchers*, *watched*, and other monitoring terms are provided in Table 1.

<sup>2</sup> We conceptualize organizational control as attempts to align individual behaviors with organizational objectives “based on monitoring and evaluation of behavior and outputs” (Ouchi, 1977, p. 95) and thus incorporate a broader set of organizational practices compared with monitoring.

<sup>3</sup> A principle attributed to William of Ockham that in explaining something one should make no more assumptions than are necessary.

<sup>4</sup> For example, power as productive resistance to veillance of body may be digitally constituted by counter-veillance that marks the subject as deviant. For example, resistance to normative femininity in terms of biometric normalization has been studied by focusing on “fashionistas” resisting subjectification to the biopower of fashion by embracing a lack of body discipline as a positive that they digitally project in videos and blogs (Harju and Huovinen 2015). Resistance to veillance of soul, such as resisting mandatory online courses (e.g., “Health and Safety”), is difficult but not impossible. These programs are oriented to the moral demeanor of the soul; they entail correctly identifying policy-approved options in online quizzes. No discretion is allowed; answers are either right or wrong. To resist such programs, a case may be made on ethical grounds of conscientious objection to the intrusiveness of some of the questions dealing with issues of sexuality, for instance, if one does not mind being noted as deviant. Resistance to commitment is another way of being noted

as deviant. Noncompliant commitment to organizational culture is a mark of being a whistleblower with notable effects within organizational interaction orders, local group cultures, and institutional structures, including media (Kenny 2019), for example, the cases of Chelsea Manning and Julian Assange (Munro 2019).

<sup>5</sup> An example comes from the Ford Sociological Department, which was one of the first and most striking extensions of VoB to VoS. To make sure that only deserving workers received high wages (e.g., the famous “five-dollars a day”), the department collected information on workers from the government, churches, civic organizations, and banks and regularly visited workers’ homes to ensure compliance with company standards for better morals, sanitary conditions, and habits of saving (Clegg et al. 2006).

<sup>6</sup> MOS journals were determined from the *Financial Times*’s list of the top 50 business journals, available at <https://www.ft.com/content/3405a512-5cbb-11e1-8f1f-00144feabdc0>. The leading IS journals were identified from the Association for Information Systems’ Senior Scholars’ list, available at <https://aisnet.org/?SeniorScholarBasket>.

## References

- Adelstein J, Clegg S (2015) Code of ethics: A stratified vehicle for compliance. *J. Bus. Ethics* 138:53–66.
- Adjerid I, Acquisti A, Telang R, Padman R, Adler-Milstein J (2016) The impact of privacy regulation and technology incentives: The case of health information exchanges. *Management Sci.* 62(4):1042–1063.
- Ajunwa I, Crawford K, Schultz J (2017) Limitless worker surveillance. *California Law Rev.* 105:735–776.
- Albrechtslund A (2008) Online social networking as participatory surveillance. *First Monday* 13(3):Article 7.
- Allen MW, Coopman SJ, Hart JL, Walker KL (2007) Workplace surveillance and managing privacy boundaries. *Management Comm. Quart.* 21(2):172–200.
- Allmer T (2011) Critical surveillance studies in the information society. *Comm. Capitalism Critique* 9(2):566–592.
- Alvarez R (2008) Examining technology, structure and identity during an enterprise system implementation. *Inform. Systems J.* 18(2):203–224.
- Ameripour A, Nicholson B, Newman M (2010) Conviviality of internet social networks: An exploratory study of internet campaigns in Iran. *J. Inform. Tech.* 25(2):244–257.
- Anandarajan M (2002) Profiling web usage in the workplace: A behavior-based artificial intelligence approach. *J. Management Inform. Systems* 19(1):243–266.
- Anderson C, Baskerville RL, Kaul M (2017) Information security control theory: Achieving a sustainable reconciliation between sharing and protecting the privacy of information. *J. Management Inform. Systems* 34(4):1082–1112.
- Anteby M, Chan CK (2018) A self-fulfilling cycle of coercive surveillance: Workers’ invisibility practices and managerial justification. *Organ. Sci.* 29(2):247–263.
- Aral S, Dellarocas C, Godes D (2013) Introduction to the special issue—Social media and business transformation: A framework for research. *Inform. Systems Res.* 24(1):3–13.
- Astor PJ, Adam MTP, Jerčić P, Schaaff K, Weinhardt C (2013) Integrating biosignals into information systems: A neuroIS tool for improving emotion regulation. *J. Management Inform. Systems* 30(3):247–278.
- Ayyagari R (2011) Technostress: Technological antecedents and implications. *MIS Quart.* 35(4):831–858.
- Ball K (2009) Exposure: Exploring the subject of surveillance. *Inform. Comm. Soc.* 12(5):639–665.
- Ball K, Wilson DC (2000) Power, control and computer-based performance monitoring: Repertoires, resistance and subjectivities. *Organ. Stud.* 21(3):539–565.
- Barad K (2007) *Meeting the Universe Halfway: Quantum Physics and the Entanglement of Matter and Meaning* (Duke University Press, Durham, NC).
- Baudrillard J (2006) *Simulacra and Simulation* (University of Michigan Press, Ann Arbor, MI).
- Baudrillard J (2007) *Forget Foucault* (Semiotext(e), Los Angeles).
- Bélanger F, Crossler RE (2019) Dealing with digital traces: Understanding protective behaviors on mobile devices. *J. Strategic Inform. Systems* 28(1):34–49.
- Bélanger F, Xu H (2015) The role of information systems research in shaping the future of information privacy. *Inform. Systems J.* 25(6):573–578.
- Belot M, Schröder M (2016) The spillover effects of monitoring: A field experiment. *Management Sci.* 62(1):37–45.
- Benaroch M, Chernobai A (2017) Operational IT failures, IT value destruction, and board-level IT governance changes. *MIS Quart.* 41(3):729–762.
- Bernstein E (2012) The transparency paradox: A role for privacy in organizational learning and operational control. *Admin. Sci. Quart.* 57(2):181–216.
- Bogard W (1996) *The Simulation of Surveillance: Hypercontrol in Tele-matic Societies* (Cambridge University Press, Cambridge, UK).
- Boyne R (2000) Post-panopticism. *Econom. Soc.* 29(2):285–307.
- Brivot M, Gendron Y (2011) Beyond panopticism: on the ramifications of surveillance in a contemporary professional setting. *Account. Organ. Soc.* 36(3):135–155.
- Brocklehurst M (2001) Power, identity and new technology homework: Implications for ‘new forms’ of organizing. *Organ. Stud.* 22(3):445–466.
- Browne R (2020) Why coronavirus contact-tracing apps aren’t yet the ‘game changer’ authorities hoped they’d be. *CNBC News* (July 3), <https://www.cnbc.com/2020/07/03/why-coronavirus-contact-tracing-apps-havent-been-a-game-changer.html>.
- Brynjolfsson E, Geva T, Reichman S (2016) Crowd-squared: Amplifying the predictive power of search trend data. *MIS Quart.* 40(4):941–961.
- Buhl HU, Mueller G (2010) The “transparent citizen” in web 2.0. *Bus. Inform. Systems Engrg.* 2(4):203–206.
- Burawoy M (1979) *Manufacturing Consent: Changes in the Labor Process under Monopoly Capitalism* (University of Chicago Press, Chicago).
- Busvine D, Rinke A (2020) Germany flips to Apple-Google approach on smartphone contact tracing. *Reuters* (April 26), <https://www.reuters.com/article/us-health-coronavirus-europe-tech/germany-flips-to-apple-google-approach-on-smartphone-contact-tracing-idUSKCN22807>.
- Clegg SR (1989) *Frameworks of Power* (Sage, London).
- Clegg S, Dunkerley D (2013) *Organization, Class and Control* (Routledge, London).
- Clegg SR, Courpasson D, Phillips N (2006) *Power and Organizations* (Sage, Thousand Oaks, CA).
- Clegg S, Cunha MP, Rego A (2012) The theory and practice of utopia in a total institution: The pineapple panopticon. *Organ. Stud.* 33(12):1735–1757.
- Clegg SR, Schweitzer J, van Rijmen M (2019) The politics of openness. Seidl D, von Krogh G, Whittington R, eds. *The Cambridge Handbook of Open Strategy* (Cambridge University Press, Cambridge, UK), 307–325.
- Clemons EK, Wilson JS (2015) Family preferences concerning online privacy, data mining, and targeted ads: Regulatory implications. *J. Management Inform. Systems* 32(2):40–70.
- Constantiou ID, Kallinikos J (2015) New games, new rules: Big data and the changing context of strategy. *J. Inform. Tech.* 30(1):44–57.
- Courpasson D (2000) Managerial strategies of domination. Power in soft bureaucracies. *Organ. Stud.* 21(1):141–161.
- Crossler RE, Bélanger F (2019) Why would I use location-protective settings on my smartphone? Motivating protective behaviors



- and the existence of the privacy knowledge–belief gap. *Inform. Systems Res.* 30(3):995–1006.
- Crossler RE, Posey C (2017) Robbing Peter to pay Paul: Surrendering privacy for security's sake in an identity ecosystem. *J. Assoc. Inform. Systems* 18(7):487–515.
- Culnan MJ (1993) "How did they get my name?": An exploratory investigation of consumer attitudes toward secondary information use. *MIS Quart.* 17(3):341–363.
- Czarniawska B (2004) On time, space, and action nets. *Organ.* 11(6):773–791.
- D'Arcy J, Hovav A, Galletta D (2009) User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Inform. Systems Res.* 20(1):79–98.
- De Saulles M, Horner DS (2011) The portable panopticon: Morality and mobile technologies. *J. Inform. Comm. Ethics Soc.* 9(3):206–216.
- Deery S, Iverson R, Walsh J (2002) Work relationships in telephone call centres: Understanding emotional exhaustion and employee withdrawal. *J. Management Stud.* 39(4):471–496.
- Degli Esposti S (2014) When big data meets dataveillance: The hidden side of analytics. *Surveillance Soc.* 12(2):209–225.
- DeLanda M (1991) *War in the Age of Intelligent Machines* (Zone Books, New York).
- Deleuze G, Guattari F (1987) Introduction: Rhizome. *A Thousand Plateaus: Capitalism and Schizophrenia* (University of Minnesota Press, Minneapolis), 3–25.
- Dellarocas C (2005) Reputation mechanism design in online trading environments with pure moral hazard. *Inform. Systems Res.* 16(2):209–230.
- Denyer D, Parry E, Flowers P (2011) "Social", "Open" and "Participative"? Exploring personal experiences and organisational effects of Enterprise 2.0 use. *Long Range Planning* 44(5–6):375–396.
- Dinev T, Hart P, Mullen MR (2008) Internet privacy concerns and beliefs about government surveillance—an empirical investigation. *J. Strategic Inform. Systems* 17(3):214–233.
- Dinev T, Bellotto M, Hart P, Russo V, Serra I, Colautti C (2006) Privacy calculus model in e-commerce—a study of Italy and the United States. *Eur. J. Inform. Systems* 15(4):389–402.
- Dong JQ, Wu W (2015) Business value of social media technologies: Evidence from online user innovation communities. *J. Strategic Inform. Systems* 24(2):113–127.
- Doolin B (2004) Power and resistance in the implementation of a medical management information system. *Inform. Systems J.* 14(4):343–362.
- du Gay P (2004) Against 'enterprise' (but not against 'enterprise', for that would make no sense). *Organ.* 11(1):37–57.
- Dunkerly D (2013) *The Foreman: Aspects of Task and Structure* (Routledge, London).
- Ellerbrook A (2010) Empowerment: Analysing technologies of multiple variable visibility. *Surveillance Soc.* 8(2):200–220.
- Eslami M, Rickman A, Vaccaro K, Aleyasen A, Vuong A, Karahalios K, Sandvig C (2015) "I always assumed that I wasn't really that close to [her]": Reasoning about invisible algorithms in news feeds. *Proc. 33rd Annual ACM Conf. Human Factors Comput. Systems*. (ACM, New York), 153–162.
- Foucault M (1977) *Discipline and Punish: The Birth of the Prison* (Penguin, Harmondsworth, UK).
- Foucault M (1982) The subject and power. *Critical Inquiry* 8(4):777–795.
- Foucault M (2003) *Society Must Be Defended: Lectures at the Collège de France, 1975–76*. (Picador, New York).
- Fowler GA (2020) One of the first contact-tracing apps violates its own privacy policy. *Washington Post* (May 21), <https://www.washingtonpost.com/technology/2020/05/21/care19-dakota-privacy-coronavirus/>.
- Garud R, Jain S, Tuertscher P (2008) Incomplete by design and designing for incompleteness. *Organ. Stud.* 29(3):351–371.
- Garud R, Kumaraswamy A, Sambamurthy V (2006) Emergent by design: Performance and transformation at Infosys Technologies. *Organ. Sci.* 17(2):277–286.
- Gentry RJ, Shen W (2013) The impacts of performance relative to analyst forecasts and analyst coverage on firm R&D intensity. *Strategic Management J.* 34(1):121–130.
- Gilliom J, Monahan T (2012) *SuperVision: An Introduction to the Surveillance Society* (University of Chicago Press, Chicago).
- Goranova ML, Priem RL, Ndofo HA, Trahms CA (2017) Is there a "dark side" to monitoring? Board and shareholder monitoring effects on M&A performance extremeness. *Strategic Management J.* 38(11):2285–2297.
- Gozman D, Currie W (2014) The role of investment management systems in regulatory compliance: A post-financial crisis study of displacement mechanisms. *J. Inform. Tech.* 29(1):44–58.
- Grant RA, Higgins CA (1991) The impact of computerized performance monitoring on service work: Testing a causal model. *Inform. Systems Res.* 2(2):116–142.
- Guillemette MG, Fontaine I, Caron C (2009) A hybrid tracking system of human resources: A case study in a Canadian university. *Comm. Assoc. Inform. Systems* 24(15):255–268.
- Haggerty KD (2006) Tear down the walls: on demolishing the panopticon. Lyon D, ed. *Theorizing Surveillance: The Panopticon and Beyond* (Willan Publishing, Cullompton, UK), 23–45.
- Haggerty K, Ericson R (2000) The surveillant assemblage. *British J. Sociol.* 51(4):605–622.
- Harju AA, Huovinen A (2015) Fashionably voluptuous: Normative femininity and resistant performative tactics in fat fashion blogs. *J. Marketing Management* 31(15–16):1602–1625.
- Haskins C (2020) Apple and Google's coronavirus tech won't actually do contact tracing. Here's why exposure notification is different. *BuzzFeed News* (May 20), <https://www.buzzfeednews.com/article/carolinehaskins1/what-are-exposure-notifications-contact-tracing-how-are>.
- Howard P, Woolley SC (2016) Political communication, computational propaganda, and autonomous agents—introduction. *Internat. J. Comm.* 10:4882–4890.
- Huang J, Baptista J, Newell S (2015) Communicational ambidexterity as a new capability to manage social media communication within organizations. *J. Strategic Inform. Systems* 24(2):49–64.
- Iedema R, Rhodes C (2010) The undecided space of ethics in organizational surveillance. *Organ. Stud.* 31(2):199–217.
- Jonsson K (2006) The embedded panopticon: Visibility issues of remote diagnostics surveillance. *Scandinavian J. Inform. Systems* 18(2):1–22.
- Kallinikos J, Aaltonen A, Marton A (2010) A theory of digital objects. *First Monday* 15(6):Article 2.
- Kallinikos J, Aaltonen A, Marton A (2013) The ambivalent ontology of digital artifacts. *MIS Quart.* 37(2):357–370.
- Karanasios S, Allen D (2013) ICT for development in the context of the closure of Chernobyl nuclear power plant: An activity theory perspective. *Inform. Systems J.* 23(4):287–306.
- Karwatzki S, Dytyanko O, Trenz M, Veit D (2017a) Beyond the personalization–privacy paradox: Privacy valuation, transparency features, and service personalization. *J. Management Inform. Systems* 34(2):369–400.
- Karwatzki S, Trenz M, Tuunainen V, Veit D (2017b) Adverse consequences of access to individuals' information: An analysis of perceptions and the scope of organisational influence. *Eur. J. Inform. Systems* 26(6):688–715.
- Kenny K (2019) *Whistleblowing: Toward a New Theory* (Harvard University Press, Cambridge, MA).
- Kohli R, Kettinger WJ (2004) Informing the clan: Controlling physicians' costs and outcomes. *MIS Quart.* 28(3):363–394.
- Kordzadeh N, Warren J (2017) Communicating personal health information in virtual health communities: An integration of



- privacy calculus model and affective commitment. *J. Assoc. Inform. Systems* 18(1):45–81.
- Kosinski M, Stillwell D, Graepel T (2013) Private traits and attributes are predictable from digital records of human behavior. *Proc. Natl. Acad. Sci. USA* 110(15):5802–5805.
- Kubitschko S (2015) The role of hackers in countering surveillance and promoting democracy. *Media Comm.* 3(2):77–87.
- Leclercq-Vandelannoitte A, Isaac H, Kalika M (2014) Mobile information systems and organisational control: Beyond the panopticon metaphor? *Eur. J. Inform. Systems* 23(5):543–557.
- Lee D (2017) Facebook team working on brain-powered technology. *BBC News* (April 19), <https://www.bbc.com/news/technology-39648788>.
- Leonardi PM (2014) Social media, knowledge sharing, and innovation: Toward a theory of communication visibility. *Inform. Systems Res.* 25(4):796–816.
- Leonardi PM, Vaast E (2017) Social media and their affordances for organizing: A review and agenda for research. *Acad. Management Ann.* 11(1):150–188.
- Levy C, Waks C (2009) Professions and the pursuit of transparency in healthcare: Two cases of soft autonomy. *Organ. Stud.* 30(5):509–527.
- Li X-B, Qin J (2017) Anonymizing and sharing medical text records. *Inform. Systems Res.* 28(2):332–352.
- Li X, Sun SX, Chen K, Fung T, Wang H (2015) Design theory for market surveillance systems. *J. Management Inform. Systems* 32(2):278–313.
- Liang F, Das V, Kostyuk N, Hussain MM (2018) Constructing a data-driven society: China's social credit system as a state surveillance infrastructure. *Policy Internet* 10(4):415–453.
- Lindberg K, Czarniawska B (2006) Knotting the action net, or organizing between organizations. *Scandinavian J. Management* 22(4):292–306.
- Long CP, Bendersky C, Morrill C (2011) Fairness monitoring: Linking managerial controls and fairness judgments in organizations. *Acad. Management J.* 54(5):1045–1068.
- Loughran J (2019) Ministers could be prosecuted under the Official Secrets Act over Huawei 5G leak. *Engrg. Tech.* (April 26), <https://eandt.theiet.org/content/articles/2019/04/ministers-could-be-prosecuted-under-the-official-secrets-act-over-huawei-5g-leak/>.
- Lyon D (1994) *The Electronic Eye: The Rise of Surveillance Society* (Polity Press, Cambridge, UK).
- Lyon D (2001) *Surveillance Society: Monitoring Everyday Life* (Open University Press, Buckingham, UK).
- Lyon D (2006) 9/11, synopticon, and scopophilia: Watching and being watched. Haggerty KD, Ericson RV, eds. *The New Politics of Surveillance and Visibility* (University of Toronto Press, Toronto), 35–54.
- Lyytinen K, Yoo Y, Boland R (2016) Digital product innovation within four classes of innovation networks. *Inform. Systems J.* 26(1):47–75.
- Majchrzak A, Malhotra A (2013) Toward an information systems perspective and research agenda on crowdsourcing for innovation. *J. Strategic Inform. Systems* 22(4):257–268.
- Mann S, Ferenbok J (2013) New media and the power politics of sousveillance in a surveillance-dominated world. *Surveillance Soc.* 11(1/2):18–34.
- Manovich L (2001) *The Language of New Media* (MIT Press, Cambridge, MA).
- Marsden JR, Tung YA (1999) The use of information system technology to develop tests on insider trading and asymmetric information. *Management Sci.* 45(8):1025–1040.
- Martin AK, Van Brakel RE, Bernhard DJ (2009) Understanding resistance to digital surveillance: Toward a multi-disciplinary, multi-actor framework. *Surveillance Soc.* 6(3):213–232.
- Marwick AE (2014) How your data are being deeply mined. *New York Review of Books* (January 9), <https://www.nybooks.com/articles/2014/01/09/how-your-data-are-being-deeply-mined/>.
- Marx GT (2002) What's new about the “new surveillance”? Classifying for change and continuity. *Surveillance Soc.* 1(1):9–29.
- Mathiesen T (1997) The viewer society: Michel Foucault's ‘panopticon’ revisited. *Theoret. Criminology* 1(2):215–234.
- Mayer-Schönberger V, Cukier K (2013) *Big Data: A Revolution That Will Transform How We Live, Work, and Think* (Houghton Mifflin Harcourt, Boston).
- Mayo E (1975) *The Social Problems of an Industrial Civilization* (Routledge and Kegan Paul, London).
- Mazmanian M, Orlikowski WJ, Yates J (2013) The autonomy paradox: The implications of mobile email devices for knowledge professionals. *Organ. Sci.* 24(5):1337–1357.
- McCurry J (2020) Test, trace, contain: how South Korea flattened its coronavirus curve. *The Guardian* (April 22), <https://www.theguardian.com/world/2020/apr/23/test-trace-contain-how-south-korea-flattened-its-coronavirus-curve>.
- Metcalfe J (2018) Facebook may stop the data leaks, but it's too late: Cambridge Analytica's models live on. *MIT Technology Review* (April 9), <https://www.technologyreview.com/2018/04/09/104516/facebook-may-stop-the-data-leaks-but-its-too-late-cambridge-analyticas-models-live-on/>.
- Miller AR, Tucker C (2013) Active social media management: The case of healthcare. *Inform. Systems Res.* 24(1):52–70.
- Muldoon J (2017) The Hawthorne studies: an analysis of critical perspectives, 1936–1958. *J. Management Hist.* 23(1):74–94.
- Munro I (2019) An interview with Chelsea Manning's lawyer: Nancy Hollander on human rights and the protection of whistleblowers. *Organ.* 26(2):276–290.
- Nambisan S, Lyytinen K, Majchrzak A, Song M (2017) Digital innovation management: Reinventing innovation management research in a digital world. *MIS Quart.* 41(1):223–238.
- Natividad G (2014) Integration and productivity: Satellite-tracked evidence. *Management Sci.* 60(7):1698–1718.
- Newell S, Marabelli M (2015) Strategic opportunities (and challenges) of algorithmic decision-making: A call for action on the long-term societal effects of ‘datification’. *J. Strategic Inform. Systems* 24(1):3–14.
- O'Harrow R (2006) *No Place to Hide* (Free Press, New York).
- Orlikowski WJ (1991) Integrated information environment or matrix of control? The contradictory implications of information technology. *Accounting Management Information Tech.* 1(1):9–42.
- Orlikowski WJ, Scott SV (2014) What happens when evaluation goes online? Exploring apparatuses of valuation in the travel sector. *Organ. Sci.* 25(3):868–891.
- Ouchi WG (1977) The relationship between organizational structure and organizational control. *Admin. Sci. Quart.* 22(1):95–113.
- Pavlou PA (2011) State of the information privacy literature: Where are we now and where should we go? *MIS Quart.* 35(4):977–988.
- Pecora VP (2002) The culture of surveillance. *Qualitative Sociol.* 25(3):345–358.
- Pierce L, Snow DC, McAfee A (2015) Cleaning house: The impact of information technology monitoring on employee theft and productivity. *Management Sci.* 61(10):2299–2319.
- Poppo L, Zhou KZ (2014) Managing contracts for fairness in buyer-supplier exchanges. *Strategic Management J.* 35(10):1508–1527.
- Poster M (1993) *Politics, Theory, and Contemporary Culture* (Columbia University Press, New York).
- Poster M (1996) Databases as discourse; or, electronic interpellations. Lyon D, Zureik E, eds. *Computers, Surveillance, and Privacy* (University of Minnesota Press, Minneapolis), 175–192.
- Rhodes RA (2007) Understanding governance: Ten years on. *Organ. Stud.* 28(8):1243–1264.
- Riad S (2005) The power of ‘organizational culture’ as a discursive formation in merger integration. *Organ. Stud.* 26(10):1529–1554.

- Rizq R (2013) States of abjection. *Organ. Stud.* 34(9):1277–1297.
- Roy D (1959) “Banana time”: Job satisfaction and informal interaction. *Human Organ.* 18(4):158–168.
- Rutherford MA, Buchholtz AK, Brown JA (2007) Examining the relationships between monitoring and incentives in corporate governance. *J. Management Stud.* 44(3):414–430.
- Scott SV, Orlikowski WJ (2014) Entanglements in practice: Performing anonymity through social media. *MIS Quart.* 38(3):873–893.
- Seaman JB, Erlen JA (2015) Workarounds in the workplace: A second look. *Orthopaedic Nursing* 34(4):235–240.
- Servick K (2020) COVID-19 contact tracing apps are coming to a phone near you. How will we know whether they work? *Science* (May 21), <https://www.sciencemag.org/news/2020/05/countries-around-world-are-rolling-out-contact-tracing-apps-contain-coronavirus-how>.
- Sewell G (1998) The discipline of teams: The control of team-based industrial work through electronic and peer surveillance. *Admin. Sci. Quart.* 43(2):397–428.
- Sewell G, Barker J (2006) Coercion vs. care: Using irony to make sense of organizational surveillance. *Acad. Management Rev.* 31(4):934–961.
- Shapira Z (2011) I’ve got a theory paper—do you? Conceptual, empirical, and theoretical contributions to knowledge in the organizational sciences. *Organ. Sci.* 22(5):1312–1321.
- Shaw JD, Gupta N, Delery JE (2000) Empirical organizational-level examinations of agency and collaborative predictions of performance-contingent compensation. *Strategic Management J.* 21(5):611–623.
- Short JL, Toffel MW (2010) Making self-regulation more than merely symbolic: The critical role of the legal environment. *Admin. Sci. Quart.* 55(3):361–369.
- Silva S (2020) Coronavirus: How map hacks and buttocks helped Taiwan fight Covid-19. *BBC News* (June 6), <https://www.bbc.com/news/technology-52883838>.
- Silva L, Backhouse J (2003) The circuits-of-power framework for studying power in institutionalization of information system. *J. Assoc. Inform. Systems* 4(6):294–336.
- Silverman D (2019) *Interpreting Qualitative Data* (Sage, London).
- Singer N (2020) Virus-tracing apps are rife with problems. Governments are rushing to fix them. *New York Times* (July 8), <https://www.nytimes.com/2020/07/08/technology/virus-tracing-apps-privacy.html>.
- Singh R, Mathiassen L, Stachura ME, Astapova EV (2011) Dynamic capabilities in home health: IT-enabled transformation of post-acute care. *J. Assoc. Inform. Systems* 12(2):163–188.
- Spiekermann S, Korunovska J (2017) Toward a value theory for personal data. *J. Inform. Tech.* 32(1):62–84 (Palgrave Macmillan).
- Staats BR, Dai H, Hofmann D, Milkman KL (2017) Motivating process compliance through individual electronic monitoring: An empirical examination of hand hygiene in healthcare. *Management Sci.* 63(5):1663–1685.
- Stahl BC, Doherty NF, Shaw M (2012) Information security policies in the UK healthcare sector: A critical evaluation. *Inform. Systems J.* 22(1):77–94.
- Stanko TL, Beckman CM (2015) Watching you watching me: Boundary control and capturing attention in the context of ubiquitous technology use. *Acad. Management J.* 58(3):712–738.
- Statt N (2020) ACLU sues facial recognition firm Clearview AI, calling it a ‘nightmare scenario’ for privacy. *The Verge* (May 28), <https://www.theverge.com/2020/5/28/21273388/acu-clearview-ai-lawsuit-facial-recognition-database-illinois-biometric-laws>.
- Tas J, Kimpen J (2020) Health systems are in need of radical change; virtual care will lead the way. *MIT Technology Review* (April 30), <https://www.technologyreview.com/2020/04/30/1000818/health-systems-are-in-need-of-radical-change-virtual-care-will-lead-the-way/>.
- Trahair R (2001) George Elton Mayo. Witzel M, ed. *Biographical Dictionary of Management* (Thoemmes, Bristol, UK), 326.
- Tung A, Marsden JR (2000) Trading volumes with and without private information: A study using computerized market experiments. *J. Management Inform. Systems* 17(1):31–57.
- Turow J (2011) *The Daily You: How the New Advertising Industry Is Defining Your Identity and Your Worth* (Yale University Press, New Haven, CT).
- Twyman NW, Lowry PB, Burgoon JK, Nunamaker JF (2014) Autonomous scientifically controlled screening systems for detecting information purposely concealed by individuals. *J. Management Inform. Systems* 31(3):106–137.
- Valentino-DeVries J (2020) F.C.C. to fine cellphone carriers for selling customers’ locations. *New York Times* (February 27), <https://www.nytimes.com/2020/02/27/technology/fcc-location-data.html>.
- Van Dijk J (2014) Datafication, dataism and dataveillance: Big data between scientific paradigm and ideology. *Surveillance Soc.* 12(2):197–208.
- Vance A, Lowry PB, Eggett D (2013) Using accountability to reduce access policy violations in information systems. *J. Management Inform. Systems* 29(4):263–290.
- Vance A, Lowry PB, Eggett D (2015) Increasing accountability through user interface design artifacts: A new approach to addressing the problem of access-policy violations. *MIS Quart.* 39(2):345–366.
- Vieira da Cunha J (2013) A dramaturgical model of the production of performance data. *MIS Quart.* 37(3):723–748.
- Vieira da Cunha J, Carugati A (2009) Information technology and the first-line manager’s dilemma: Lessons from an ethnographic study. Newell S, Whitley EA, Pouloudi N, Wareham J, Mathiassen L, eds. *Proc. 17th Eur. Conf. Inform. Systems, ECIS 2009, Verona, Italy*, 2834–2845.
- Visser LM, Bleijenbergh IL, Benschop YWM, van Riel ACR (2018) Prying eyes: A dramaturgical approach to professional surveillance. *J. Management Stud.* 55(4):703–727.
- Walin M (2020) Traffic data, route planning, and ETA: How Google Maps predicts travel time. Accessed February 17, 2021, <https://www.verizonconnect.com/resources/article/google-maps-travel-time/>.
- Wareham J, Bjørn-Andersen N, Neergaard P (1998) Reinterpreting the demise of hierarchy: A case study in information technology, empowerment and incomplete contracts. *Inform. Systems J.* 8(4):257–272.
- Warkentin M, Goel S, Menard P (2017) Shared benefits and information privacy: What determines smart meter technology adoption? *J. Assoc. Inform. Systems* 18(11):758–786.
- Weber M (1949) *The Methodology of the Social Sciences* (Free Press, New York).
- Williams T (1996) Government regulation through voluntary cooperation: A follow-up study of the strategic impact of information technology. *J. Strategic Inform. Systems* 5(2):149–156.
- Wood D (2002) Foucault and panopticism revisited. *Surveillance Soc.* 1(3):234–239.
- Woolley SC, Howard PN (2016) Automation, algorithms, and politics: Political communication, computational propaganda, and autonomous agents—introduction. *Internat. J. Comm.* 10:4882–4890.
- Xu H, Teo H-H, Tan BCY, Agarwal R (2009) The role of push–pull technology in privacy calculus: The case of location-based services. *J. Management Inform. Systems* 26(3):135–174.
- Yates J (1993) *Control Through Communication: The Rise of System in American Management* (Johns Hopkins University Press, Baltimore).

- Yoo Y, Henfridsson O, Lyytinen K (2010) Research commentary—the new organizing logic of digital innovation: an agenda for information systems research. *Inform. Systems Res.* 21(4):724–735.
- Zhang X, Venkatesh V (2013) Explaining employee job performance: The role of online and offline workplace communication networks. *MIS Quart.* 37(3):695–722.
- Zimmer M (2008) The gaze of the perfect search engine: Google as an infrastructure of dataveillance. Spink A, Zimmer M, eds. *Web Search: Multidisciplinary Perspectives* (Springer, Berlin), 77–99.
- Zittrain J (2008) *The Future of the Internet—and How to Stop It* (Yale University Press, New Haven, CT).
- Zuboff S (2015) Big other: Surveillance capitalism and the prospects of an information civilization. *J. Inform. Tech.* 30(1):75–89.
- Zuboff S (2016) The secrets of surveillance capitalism. *Frankfurter Allgemeine* (March 5), <https://www.faz.net/aktuell/feuilleton/debatten/the-digital-debate/shoshana-zuboff-secrets-of-surveillance-capitalism-14103616.html>.
- Zuboff S (2019) *The Age of Surveillance Capitalism: The Fight for the Future at the New Frontier of Power* (PublicAffairs, New York).

**Aljona Zorina** is University Academic Fellow in Innovation Management at the Strategy and Organization Group of Leeds University Business School (LUBS). Her research interests include digital innovation, digital transformation, and peer production contexts.

**France Bélanger** is R. B. Pamplin Professor and Tom & Daisy Byrd Senior Faculty Fellow in Pamplin College of Business, as well as affiliate faculty in Hume Center for National Security and Technology and Center for Gerontology at Virginia Tech. Her research focuses on digital interactions between individuals, businesses, and governments and the related information security and privacy issues.

**Nanda Kumar** is an associate professor of information systems at Baruch College, City University of New York. He received his PhD in management information systems from University of British Columbia in 2003. His current research interests include human-computer interaction, privacy/security issues, workflow standardization, and technology policy.

**Stewart Clegg** is an emeritus professor of management at University of Technology Sydney Business School. His research is wide, with a central focus on power relations, situating them in many aspects of everyday and organizational life, with discussion of substantive topics such as spatial relations, ethics, project management, governance, as well as making major contributions to organization studies in general.