# WATCHERS, WATCHED, AND WATCHING IN THE DIGITAL AGE:

# RECONCEPTUALIZATION OF IT MONITORING AS COMPLEX ACTION NETS

**Aljona Zorina**
Leeds University Business School,
Charles Thackrah Building, Leeds, LS2 9JT UK
e-mail: A.Zorina@leeds.ac.uk

**France Bélanger**
Virginia Tech,
880 West Campus Drive
Blacksburg, VA 24061, USA,
e-mail: belanger@vt.edu

**Nanda Kumar**
Zicklin School of Business
Baruch College, City University of New York
e-mail: nanda.kumar@baruch.cuny.edu

**Stewart Clegg**
University of Technology Sydney,
MDG, Business Faculty
15 Broadway, Ultimo NSW 2007, Australia,
e-mail: stewart.clegg@uts.edu.au

***Accepted for publication in Organization Science***

***Abstract***

Despite increasing studies of 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 pre-defined 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 heterogenous 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 heterogenous 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.

***Keywords:*** monitoring, veillance, IT 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 heterogenous participants engaging in diverse alliances and conflict that are able to challenge previously exclusive rights of watchers[1] to manipulate visibility and anonymity (Anteby and Chan 2018; Scott and Orlikowski 2014). 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) while, 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, while 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 to maximize the visibility of those being surveyed while minimizing the visibility of its practice, situated in a watchtower. Foucault argued that panoptic observation trains those under surveillance to conduct themselves as if they are being watched even while they may not be. Knowing that one and one's fellows are potentially under surveillance induces their 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

[1] Formal definitions of watchers, watched, and other monitoring terms are provided in Table 1.

disciplinary relationships between the watcher and watched and ignored attributes of contemporary monitoring practices not neatly fitting the panoptic frame (Haggerty 2006; Lyon 2007). Contemporary monitoring requires different framing (e.g., Haggerty 2006; Leclercq-Vandelannoitte et al. 2014; Mann and Ferenbok 2013; Zuboff 2015; 2016). While some recent work on IT monitoring either extends the panoptical model while still focusing on actors (e.g. portable-, post-, and super-panopticon, synopticon) (e.g., De Saulles and Horner 2011; Lyon 2006); others remove actors from central focus by developing models based on data flows (e.g., dataveillance, 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, re-programmable and open for contributions from potentially unbounded heterogenous participants (Garud et al. 2008; Kallinikos et al. 2010; Manovich 2001; 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[2] 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

[2]We conceptualise organizational control as attempts to align individual behaviors with organizational objectives "based on monitoring and evaluation of behavior and outputs" (Ouchi, 1977, p. 95); thus, incorporating a broader set of organizational practices compared to monitoring.

the net, influencing dispositions of 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., Leclercq-Vandelannoitte et al. 2014; Mann and Ferenbok 2013; Zuboff 2016). Second, the action net is built on neither particular pre-defined patterns of actor relationship as watcher/watched nor on prior organizational boundaries (Czarniawska 2004). Participant relationships and IT enactments performative to actor roles, flexible system elements and boundaries, enabling multiple dynamic foci, continuously re-establish 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 non-linear 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 one or the other of the watcher, 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.

--- Insert Table 1 here ---

The relationship implied between the watcher and the watched, from the watchers' perspective, is either top-down or bottom-up, conceptualized as *surveillance* or *sousveillance.* Surveillance is the most widely used approach, associated with centralized control (Foucault 1977) predicated on IT monitoring (Boyne 2000; Iedema and Rhodes 2010). Sousveillance, in which watchers are decentralized and flexible actors (Baudrillard 2006; Bogard 1996; 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 video recording of Mr. George Floyd's death in 2020, sparked widespread civil unrest in the USA. Organizational members' digital devices can capture or report actions of other members (Silverman 2019). The leak of the U.K.'s National Security Council decision to allow Huawei to provide non-core parts of the UK'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 panopticon term include electronic, information, portable, post-, and super-panopticon (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 those 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 Dijck 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 (1991)'s *panspectron* focuses on new, previously unavailable, zones for monitoring enabled by decentralized, pervasive, 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 co-existing 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 overviewing 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-, post-, and super-panopticon, synopticon) (e.g., De Saulles and Horner 2011; Poster 1996), while others develop models of data flows specific and exceptional for IT contexts (e.g., dataveillance, assemblages, panspectron) (e.g., DeLanda 1991). Second, despite substantial differences, these studies assume 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 re-thinking fundamental assumptions and explanations of IT processes and outcomes (e.g., Nambisan et al. 2017; Zittrain 2008).

--- Insert Table 2 here ---

As the table illustrates, IT artifacts are increasingly seen as possessing unique characteristics of being editable and re-programmable during the process of IT use (Kallinikos et al. 2010; Manovich 2001;

Yoo et al. 2010), What is enabled are potentially unbounded and heterogenous participant contributions guided by multiple logics of organizing (Lyytinen et al. 2016; Majchrzak and Malhotra 2013). 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, *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[3] to incorporate both IT and non-IT monitoring and avoids pre-defined a priori relationships between the watcher and the watched (as sur- and sous-veillance 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 soul, to commitment, to productive resistance. We build on this classification by proposing

[3] A principle attributed to William of Occam that in explaining something one should make no more assumptions than are necessary.

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 sous and peer-veillance when those being watched also constitute perceptions of the body, soul and commitment of their watchers (Kenny 2019; Sewell 1998)[4]. Table A1 in Appendix A provides examples of the VF typology for non-IT and IT veillance.

**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 (Clegg et al. 2006; Foucault 2003). A shift in the paradigm of organizational monitoring was introduced with Scientific Management that justified the scrutiny of "productive hands" (Clegg et al. 2006), surveying employees' bodies and behaviors using simple productivity metrics. While 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 bio-health markers such as blood pressure and heart rate, as well as 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.

**Veillance of soul (VoS).** Th 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

[4] 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 'fatshionistas' 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 demeanour of the soul; they entail correctly identifying policy approved options in online quizzes. No discretion is allowed; answers are only 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. Non-compliant commitment to organizational culture is a mark of being a whistle-blower 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).

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[5] (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 life, 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 Relation 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 that 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.

**Veillance of commitment (VoC).** Veillance of commitment strives to make visible the commitment of those watched in non-standardized 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

[5] 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 only deserving workers received high wages (e.g., the famous "five-dollar a day), the Department collected information on workers from the government, churches, civic organizations, banks, as well as regularly visiting workers' homes to ensure compliance with company standards for better morals, sanitary conditions, and "habits of thrift and saving" (Clegg et al. 2006a; Meyer 1981).

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 a 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 homeworking work practices established during the coronavirus pandemic. VoC implies a substantial internalization of (or at least high sensitivity towards) the watcher's goals and values (Levay and Waks 2009; Rhodes 2007) 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.

--- Insert Figure 1 here ---

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 actor*s) 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 explain below, 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 literature in top eight MOS[6] and IS[7] journals using the VW framework as a basis for our analysis. While 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 Business Source EBSCO database. Finally, we conducted a citation analysis to ensure 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 Appendix B.

### *3.1 Coding*

An iterative in-depth coding process coded empirical papers identified (e.g., Bélanger et al. 2014; Shapira 2011), a process involving initially reading several articles, identifying initial codes, grouping codes into categories and re-coding 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* include 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

[6]Financial Times list of top 50 business journals, available at https://www.ft.com/content/3405a512-5cbb-11e1-8f1f-00144feabdc0.
[7] Eight leading IS journals in the Association for Information Systems Senior Scholars' list (https://aisnet.org/?SeniorScholarBasket).

how veillance is conducted. For example, hard mechanisms could include coercion, physical markings, and inspections to generate fear; soft mechanism examples 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 Appendix B, while the resulting codes for the 132 papers are shown in 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 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 either in non-IT or in 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 while 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 (Anderson et al. 2017; Poppo and Zhou 2014) (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., Long et al. 2011; Riad 2005). 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 below 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.

--- Insert Table 3 here ---

*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. 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 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; 2017b). Another shared pattern concerned transformations in work practices that IT veillance brings to traditional industries, such as healthcare (e.g., Doolin 2004; Staats et al. 2017; Stahl et al. 2012), universities (Alvarez 2008), trading and retailing (Marsden and Tung 1999; Wareham et al. 1998), 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), 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 multi-

directional 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 (Clemons and Wilson 2015; Singh et al. 2011). Summarizing our analysis, we propose:

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

*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 to 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 to non-IT veillance.

--- Insert Table 4 here ---

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 is 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., Brynjolfsson et al. 2016; Dellarocas 2005; 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 (co)watcher regulating 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., Adjerid et al. 2016Li et al. 2015). 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:

*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 co-created 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 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 co-goals 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., Dellarocas 2005; Karwatzki et al. 2017a; 2017b), 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., Anandarajan 2002; Marsden and Tung 1999). 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 (Li and Sarkar 2013; Twyman et al. 2014), similar to the goal of *documentation* in veillance of physician clinical activities (Rizq 2013) as well in 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 (Anderson et al. 2017; Kohli and Kettinger 2004) and improved quality prediction of watched behaviors (Brynjolfsson et al. 2016; Singh et al. 2011; Xu et al. 2009). 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 (Adjerid et al. 2016; Vance et al. 2015). Therefore, we propose:

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

*4.2.2 Emergent and Co-created Goals.* As the relationships between watcher and watched unfold, novel properties of goals emerge and evolve in IT veillance. For example, while 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 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 (Leclercq-Vandelannoitte et al. 2014; Mazmanian et al. 2013).

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 co-creation 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 co-create 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 co-develop 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:

*Proposition 5. IT enables emergent and co-created 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., Bernstein 2012; Courpasson 2000; Rutherford et al. 2007). 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 to cases discussing hard mechanisms.

--- Insert Table 5 here---

IT enables location-based tracking of customers (Xu et al. 2009-10) 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 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; e.g., 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., RFID tags, mobile devices, sensors) enable 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) as well as 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 (Levay and Waks 2009). Dissolving traditionally bounded organizational veillance spaces can transform traditional panopticon veillance into a portable panopticon (De Saulles and Horner 2011), also referred to as 'free control' (Leclercq-Vandelannoitte et al. 2014, p. 543), and post-panopticon (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 (Stahl et al. 2012; Williams 1996). 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 above analysis, we propose:

*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, i.e. 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, knowing

how these are designed, 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 co-creation 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:

> *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 manipulative effects of IT monitoring 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., Buhl and Mueller 2010; Jonsson 2006), 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 (Howard and Woolley 2016; Kosinski et al. 2013). 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 lock-downs) 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 subject. 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 (Clegg et al. 2006) that internalize goals and comply 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 video-observed (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 (Cunha 2013; Visser et al. 2018) and to present a false visibility to management providing an impression of compliance (e.g., Cunha and Carugati 2009). IT users can exchange visibility/privacy aspects for some benefits (e.g., Bélanger and Crossler 2019; Crossler and Bélanger 2019; Dinev et al. 2006; Pavlou 2011). 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:

*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 pre-conceptualized 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 monitoring of employee bodies and behaviors while VoS focuses on specially planned and established organizational or team culture.

--- Insert Table 6 here ---

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 e-mails, and online activities is often complemented by emerging norms for continuous responsiveness, availability and engagement. These 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, 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 veillance of traces of their past. IT automatically facilitates 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 hardworking employee" (Lyon 2001, p. 41), anticipating the patterns of future behavior of the watched (Stanko and Beckman 2015), 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, its use for veillance of future and related manipulations and consequences for the democracy, provides an illustrative example in this regard (Clegg et al, 2017; 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 pre-fixed 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:

*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 veillance action net model is produced by the actants and actions of heterogenous veillance 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 veillance), with goals being defined prior to veillance. The participating actors are known in advance and the apparatus of veillance is constructed before the act of monitoring to enable a particular focus for the veillance (body, soul or commitment). Each conceptualization requires a different design in terms of actors, goals and veillance mechanisms; they are not mutually exclusive and can be used additively. In the action net model of IT veillance, 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 veillance, relating to participating actors who are multiple, heterogenous, 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 data bases, 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 veillance system and multiple veillance foci. Figure 2 illustrates the IT Veillance action net model.

--- Insert Figure 2 here ---

Existing models, such as the panopticon, 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 veillance differs significantly. It brings the relationships between actors to the center of analysis and presents veillance as a flexible and emergent decentralized interconnected web with flexible boundaries, roles, and relationships between heterogenous actors and actants involved in the system of veillance. It illustrates that the net is not defined by the structural/hierarchical position of the actors but by the relationships between heterogenous veillance participants and their cumulative abilities to organize, impact and otherwise manipulate the net, including influences on dispositions of roles, visibilities and inclusion/exclusion of other relevant actors and intermediates. In this regard, our model builds on and extends calls to re-think the role of the watched in IT monitoring as no longer passive (Anteby and Chan 2018; Scott and Orlikowski 2014; Visser et al. 2018).

The action net does not define a particular pre-defined actor relationship pattern or set of organizational boundaries (Czarniawska 2004) but is continuously re-established by flexible system relationships, enabling multiple dynamic foci co-shaped by inputs from flexible watchers, watched and intermediate devices and actants. In the action net model there are diverse veillance 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 movement by governments (Ameripour et al. 2010). Additionally, research can focus on those that are watched who become self-aware and learn to co-create and manage how they might be (in)visible, self-present, attract resources and attention to the watched (Anteby and Chan 2018; Brivot and

Gendron 2011; Doolin 2004; Visser et al. 2018). By changing their visibility, actors can manipulate the action net, thus blurring boundaries between pre-established 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 pre-defined 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 (e.g. 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 of veillance. For example, as debates on obligatory use of Covi-passes (https://www.covipass.com/) reveal, while COVID-19 contact tracing might start as VoB, it may soon evolve into VoS/VoC (McCurry 2020).

The action net model of veillance 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; Leclercq-Vandelannoitte et al. 2014; Mann and Ferenbok 2013; 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 IT veillance 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 re-programmability (Garud et al. 2008; Kallinikos et al. 2010; Manovich 2001; Yoo et al. 2010) (see Table 2), which existing studies on veillance 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 IT veillance 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 Appendix D summarizes our arguments.

*5.2.1 Flexibility of Veillance Elements.* The elements of the action net model of IT veillance 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-mediated veillance 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 IT veillance system.

Unique characteristics enable the functioning of IT veillance 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 of veillance, such as changing veillance goals, mechanisms (e.g. changing between OFF to ON settings for exposure notifications) or the focus during the process of veillance 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, i.e. 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 OS (Apple, Google), apps on top of OS, as well as privacy advocates, miscellaneous technology vendors and so on (Nambisan et al. 2017). Diffused agency of veillance acts as another source of flexibility; diverse veillance 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., Baudrillard 2006; Marwick 2014; Marx 2002; Mayer-Schönberger and Cukier 2013;

O'Harrow 2006; Van Dijck 2014). *IT granularity* enables multiple actors to introduce tailored changes to veillance goals, mechanisms, and foci, increasing flexibility of the veillance 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 veillance over outsiders is easier than IT veillance 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 re-invention of veillance 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 veillance 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, while Clearview AI face recognition technology can use scraped images for completely different purposes. When Clearview scraped images from sites such as Facebook and Linkedin over their objections, while clearly unethical, is borderline legal. Finally, *IT reprogramability* further extends veillance flexibility, enabling dynamic adjustments of veillance elements (goals, foci, mechanisms) as veillance proceeds (Jonsson 2006; Stanko and Beckman 2015; Warkentin et al. 2017).

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

*5.2.2 Diffused Actor Roles.* The action net IT veillance system implies that various veillance participants might engage in multiple roles simultaneously on an emergent diffused basis. In contrast to non-IT veillance, where the watcher and the watched acquire their role 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 conceptualization of the watchers as a

central and coherent group of actors. Instead, it implies 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 veillance. Instead, the watched in the action net can be actively involved in the veillance process through IT-enabled manipulations, activation of various intermediators, shaping the boundaries between the watcher and the watched as changeable, ambiguous and subject to networked relationships.

The above logics are enabled in important ways by the IT characteristics discussed in Table 2. *IT editability* enables easy alliance with new veillance actors as well as exit from existing ones, 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 on to operators such as bounty hunters (Valentino-DeVries 2020). *IT distributedness* enables the watched to collect and store information with multiple IT devices, thus co-creating their veillance (Brivot and Gendron 2011; Leclercq-Vandelannoitte et al. 2014) as well as reversing the visibility of veillance 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., Cunha and Carugati 2013; Howard and Woolley 2016; Kosinski et al. 2013; Pierce et al. 2015) while also unintendedly increasing their visibility to third parties (Leonardi 2014; Leonardi and Vaast 2017). Instead of being known through a pre-designed veillance apparatus that has a specific focus for monitoring, those watched become known through the network of mobilized mediating actors and actants. Such mediation allows veillance 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 (co)-construction of veillance mechanisms by deciding what to make visible within the veillance system. *IT granularity* also contributes to the diffusion of actor roles by enabling some devices of IT veillance 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 co-creators of IT veillance systems (Alvarez 2008; Anteby and Chan 2018; Brivot and Gendron 2011; Doolin 2004) thus blurring pre-assigned roles. Finally, *IT re-programmability* 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 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 above logics condition areas for future research on the dynamics of veillance systems, including the formation of the diffused actor roles, their continuous change, (re)negotiation, interplay, and tensions. Table D5 in Appendix D details areas for future research in this area.

*5.2.3 Cumulative Extended Manipulations.* The action net IT veillance system operates on a logic of cumulative extended manipulations of diverse veillance participants. As discussed in the findings section, in IT veillance both the watchers and the watched can engage in diverse manipulations previously impossible in non-IT veillance. Extended manipulative capabilities of the watchers include non-human oversight and action on the watched; possibilities to use veillance systems owned by other actors as well as tailored veillance mechanisms (e.g. predictive bets). The latter, in particular, enable the watchers significantly to surpass non-IT panoptical models derived from Foucault alert to the ever-present possibility of the experience of being under surveillance leading to normalization of the watched. In

contrast, IT veillance already takes patterning for granted as it merely needs to work with that which is already constituted; for example, through knowledge of Facebook likes and networks, for example, 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-IT veillance, including "systematic soldering" (Clegg et al. 2006), "workarounds" (Seaman and Erlen 2015), or "making out" games (Burawoy 1979; Roy 1959). In contrast, the watched in IT veillance can (co)create and manage their visibility and engage various intermediate actors to further manipulate veillance processes and results. Finally, intermediate actors can also engage in veillance 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, similarly to previous logics. *IT editability* enables the watched to be continuously engaged in managing their visibility. For example, the watched who use (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 IT veillance beyond direct watchers and watched and beyond particular organizational boundaries (Czarniawska 2004). As remarked when discussing sousveillance, 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 of veillance 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 adjusted veillance system. *Granularity of IT* facilitates unique tailoring and adjustment of veillance 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 (Bélanger and Crossler 2019; Bélanger and Xu 2015; Pavlou 2011), 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 new veillance 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 (Ball 2009; Howard and Woolley 2016; Jonsson 2006; Zuboff 2015). 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 re-programmability* 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 re-programmability* 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 re-tweet 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 system to function without need of supervisors to approve work, removing from the existing system established mechanism of checks and balances, while also allowing manipulations in new ways on a massive scale.

The above logics triggers 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 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 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 (Aral et al. 2013; Denyer et al. 2011; Dong and Wu 2015; Huang et al. 2015; Leonardi 2014; Leonardi and Vaast 2017; Miller and Tucker 2013). 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 Non-Linear Actor Relationships.* Classically, organization was founded on labor processes in which communication, coordination and control based on pre-planned 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 to 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, non-linear 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, by the influencers. IT distributedness further contributes to emergent and non-linear 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; Zuboff 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 reprogramability* contributes dynamic and emergent changes in the IT veillance system through enabling mobilizations of both human and non-human actants as networks of mediating agencies. In non-IT veillance, the mediating agencies are usually specialized personnel, such as front-line 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 above logics of emergent non-linear actor relationships imply a need to re-think the effectiveness, design and power enactment in IT veillance systems, as no longer apparatus attuned to a particular type of veillance system. Instead, their effectiveness depends on incorporating multiple related and networked actors within action nets, an ability to influence inclusion/exclusion of actors or to manipulate others, as well as to be able to defend their self from others' manipulations. The power of the watched and intermediate actors who can use IT to manipulate gaze and visibility, thus co-shaping the veillance system in emergent ways, needs to be taken into account. In particular, future research is needed to re-think 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 recommendations for future research noted above, 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 to 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 & Chernobai, 2017Goranova et al. 2017) and might benefit from studies of veillance enabled by IT. Further research on practices and implications of 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. 2008; 2006) with flexible boundaries and elements, examining whether and how the primary patterns of the watcher-watched relationships influence how veillance systems evolve, 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 non-liner relationships between heterogenous watchers who might compete in circuits of power to manipulate each other. The complex multi-actor and distributed nature of the watchers' impacts on the design of monitoring systems enabled by the specific properties of IT artifacts are yet to be incorporated by theories of monitoring and require further studies.

The logics of c*umulative actor manipulations* imply that the functioning of the veillance system, its boundaries, visibility design and power dispositions are co-created 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 re-conceptualize 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 non-linear 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 non-linear actor relationships? Do any systematic patterns exist in the emergent dynamics of actor relationships? How does 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

While 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 noting the necessity of doing so (e.g., Haggerty 2006; Leclercq-Vandelannoitte et al. 2014; Mann and Ferenbok 2013; Sewell 1998; 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 such 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, while 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.

## REFERENCES


Adelstein, J., S. Clegg. 2015. Code of Ethics: A Stratified Vehicle for Compliance. Journal of Business Ethics.

Adjerid, I., A. Acquisti, R. Telang, R. Padman, J. Adler-Milstein. 2016. The Impact of Privacy Regulation and Technology Incentives: The Case of Health Information Exchanges. Management Science 62(4) 1042-1063.

Ajunwa, I., K. Crawford, J. Schultz. 2017. Limitless worker surveillance. California Law Review 105 735-776.

Albrechtslund, A. 2008. Online Social Networking as Participatory Surveillance First Monday.

Allen, M.W., S.J. Coopman, J.L. Hart, K.L. Walker. 2007. Workplace Surveillance and Managing Privacy Boundaries. Management Communication Quarterly 21(2) 172.

Allmer, T. 2011. Critical surveillance studies in the information society. Communication, Capitalism & Critique 9(2) 566-592.

Alvarez, R. 2008. Examining Technology, Structure and Identity during an Enterprise System Implementation Information Systems Journal 18 203-224.

Ameripour, A., B. Nicholson, M. Newman. 2010. Conviviality of Internet Social Networks: an Exploratory Study of Internet Campaigns in Iran. Journal of Information Technology 25(2) 244-257.

Anandarajan, M. 2002. Profiling Web Usage in the Workplace: A Behavior-Based Artificial Intelligence Approach. Journal of Management Information Systems 19(1) 243-266.

Anderson, C., R.L. Baskerville, M. Kaul. 2017. Information Security Control Theory: Achieving a Sustainable Reconciliation Between Sharing and Protecting the Privacy of Information. Journal of Management Information Systems 34(4) 1082-1112.

Angst, C.M., E.S. Block, J. D'Arcy, K. Kelley. 2017. When Do IT Security Investments Matter? Accounting for the Influence of Institutional Factors in the Context of Healthcare Data Breaches. MIS Quarterly 41(3) 893-A898.

Anteby, M., C.K. Chan. 2018. A self-fulfilling cycle of coercive surveillance: Workers' invisibility practices and managerial justification. Organization Science 29(2) 247-263.

Aral, S., C. Dellarocas, D. Godes. 2013. Introduction to the special issue—Social media and business transformation: A framework for research. Information Systems Research 24(1) 3–13.
Arthurs, J.D., R.E. Hoskisson, L.W. Busenitz, R.A. Johnson. 2008. Managerial Agents Watching Other Agents: Multiple Agency Conflicts Regarding Underpricing in IPO Firms. Academy of Management Journal 51(2) 277-294.
Astor, P.J., M.T.P. Adam, P. Jerčić, K. Schaaff, C. Weinhardt. 2013. Integrating Biosignals into Information Systems: A NeuroIS Tool for Improving Emotion Regulation Journal of Management Information Systems 30(3) 247-278.
Ayyagari, R. 2011. Technostress: Technological Antecedents and Implications. MIS Quarterly 35(4) 831–858.
Ball, K. 2009. Exposure: Exploring the subject of surveillance. Information. Communication & Society 12(5) 639-665.
Ball, K., D.C. Wilson. 2000. Power, Control and Computer-based Performance Monitoring: Repertoires, Resistance and Subjectivities. Organization Studies 21(3) 539-565.
Barad, K. 2007. Meeting the universe halfway: Quantum physics and the entanglement of matter and meaning. Duke University Press.
Baudrillard, J. 2006. Simulacra and Simulation. University of Michigan, Michigan.
Baudrillard, J. 2007. Forget Foucault. Semiotext(e), Los Angeles.
Beatty, R.P., E.J. Zajac. 1994. Managerial Incentives, Monitoring, and Risk Bearing: A Study of Executive Compensation, Ownership, and Board Structure in Initial Public Offerings. Administrative Science Quarterly 39(2) 313-335.
Bélanger, F., M. Cefaratti, T. Carte, S.E. Markham. 2014. Multilevel Research in Information Systems: Concepts, Strategies, Problems and Pitfalls. Journal of the Association for Information Systems 15(9) Article 1.
Bélanger, F., R.E. Crossler. 2019. Dealing with digital traces: Understanding protective behaviors on mobile devices. The Journal of Strategic Information Systems 28 34-49.
Bélanger, F., H. Xu. 2015. The role of information systems research in shaping the future of information privacy Information Systems Journal, 573-578.
Belot, M., M. Schröder. 2016. The Spillover Effects of Monitoring: A Field Experiment. Management Science 62(1) 37-45.
Benaroch, M., & Chernobai, A. (2017). Operational It Failures, It Value Destruction, and Board-Level It Governance Changes. MIS Quarterly, 41(3), 729-A726.
Bennett, S., K. Maton, L. Kervin. 2008. The 'digital natives' debate: A critical review of the evidence. British Journal of Educational Technology 39(5) 775-786.
Bernstein, E. 2012. The Transparency Paradox: A Role for Privacy in Organizational Learning and Operational Control. Administrative Science Quarterly 57(2) 181-216.
Bogard, W. 1996. The Simulation of Surveillance: Hypercontrol in Telematic Societies. Cambridge University Press, Cambridge, UK.
Boyne, R. 2000. Post-panopticism. Economy and Society 29(2) 285-307.
Brivot, M., Y. Gendron. 2011. Beyond panopticism: on the ramifications of surveillance in a contemporary professional setting. Accounting, Organizations and Society 36(3) 135-155.
Brocklehurst, M. 2001. Power, Identity and New Technology Homework: Implications for New Forms' of Organizing. Organization Studies 22(3) 445-466.
Browne, R. 2020. Why coronavirus contact-tracing apps aren't yet the 'game changer' authorities hoped they'd be CNBS News.
Brynjolfsson, E., T. Geva, S. Reichman. 2016. Crowd-Squared: Amplifying the Predictive Power of Search Trend Data. MIS Quarterly 40(4) 941-961.
Buhl, H.U., G. Mueller. 2010. The "Transparent Citizen" in Web 2.0. Business & Information Systems Engineering 2(4) 203-206.
Burawoy, M. 1979. Manufacturing Consent: Changes in the Labor Process Under Monopoly Capitalism. University of Chicago Press, Chicago.

Busvine, D., A. Rinke. 2020. Germany flips to Apple-Google approach on smartphone contact tracing Reuters. Reuters.
Clegg, S., M.P. Cunha, A. Rego. 2012. The Theory and Practice of Utopia in a Total Institution: The Pineapple Panopticon. Organization Studies 33(12) 1735-1757.
Clegg, S., D. Dunkerley. 2013. Organization, Class and Control. Routledge, London.
Clegg, S.R. 1989. Frameworks of power. Sage, London, UK.
Clegg, S.R., D. Courpasson. 2004. Political hybrids: Tocquevillean views on project organizations. Journal of Management Studies 41(4) 525–547.
Clegg, S.R., D. Courpasson, N. Phillips. 2006. Power and Organizations. Sage, Thousand Oaks, CA..
Clegg, S.R., T. Pitsis, T. Rura-Polley, M. Marosszeky. 2002. Governmentality Matters: Designing an Alliance Culture of Inter-organizational Collaboration for Managing Projects. Organization Studies 23(3) 317-337.
Clegg, S.R., J. Schweitzer, M. van Rijmen. 2019. The Politics of Openness. D.v.K. Seidl, G., R. Whittington, eds. The Cambridge Handbook of Open Strategy. Cambridge University Press, Cambridge.
Clemons, E.K., J.S. Wilson. 2015. Family Preferences Concerning Online Privacy, Data Mining, and Targeted Ads: Regulatory Implications. Journal of Management Information Systems 32(2) 40-70.
Collinson, D.L. 1999. ‘Surviving the Rigs': Safety and Surveillance on North Sea Oil Installations. Organization Studies 20(4) 579-600.
Combs, J.G., D.J. Ketchen, A.A. Perryman, M.S. Donahue. 2007. The Moderating Effect of CEO Power on the Board Composition–Firm Performance Relationship. Journal of Management Studies 44(8) 1299-1323.
Constantiou, I.D., J. Kallinikos. 2015. New Games, New Rules: Big data and the changing context of strategy. Journal of Information Technology 30(1) 44-57.
Courpasson, D. 2000. Managerial Strategies of Domination. Power in Soft Bureaucracies. Organization Studies 21(1) 141-161.
Crossler, R.E., F. Bélanger. 2019. Why Would I Use Location-Protective Settings on My Smartphone? Motivating Protective Behaviors and the Existence of the Privacy Knowledge–Belief Gap. Information Systems Research 30(3) 995-1006.
Crossler, R.E., C. Posey. 2017. Robbing Peter to Pay Paul: Surrendering Privacy for Security's Sake in an Identity Ecosystem. Journal of the Association for Information Systems 18(7) 487-515.
Culnan, M.J. 1993. 'How Did They Get My Name?': An Exploratory Investigation of Consumer Attitudes Toward Secondary Information Use. MIS Quarterly 17(3) 341-363.
Culnan, M.J., P.K. Armstrong. 1999. Information Privacy Concerns, Procedural Fairness and Impersonal Trust: An Empirical Investigation. Organization Science 10(1) 104-115.
Cunha, J.V.d. 2013. A dramaturgical model of the production of performance data. MIS Quarterly 37(3) 723-748.
Cunha, J.V.d, A. Carugati. 2009. Information technology and the first-line manager's dilemma: Lessons from an ethnographic study. 17th European Conference on Information Systems, ECIS 2009.
Czarniawska, B. 2004. On Time, Space, and Action Nets. Organization 11(6) 773-791.
D’Arcy, J., A. Hovav, D. Galletta. 2009. User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach. Information Systems Research 20(1) 79-98.
De Saulles, M., D.S. Horner. 2011. The Portable Panopticon: Morality and Mobile Technologies. Journal of Information Communication and Ethics in Society 9(3) 206-216.
Deery, S., R. Iverson, J. Walsh. 2002. Work Relationships in Telephone Call Centres: Understanding Emotional Exhaustion and Employee Withdrawal. Journal of Management Studies 39(4) 471-496.
Degli Esposti, S. 2014. When big data meets dataveillance: The hidden side of analytics. Surveillance & Society 12(2) 209-225.
DeLanda, M. 1991. War in the age of intelligent machines. Zone Books.
Deleuze, G. 1992. Postscript on the Societies of Control October, 3-7.
Deleuze, G., F. Guattari. 1987. Introduction: Rhizome. In A Thousand Plateaus: Capitalism And Schizophrenia. University of Minnesota Press, Minneapolis.

Dellarocas, C. 2005. Reputation Mechanism Design in Online Trading Environments with Pure Moral Hazard. Information Systems Research 16(2) 209-230.
Denyer, D., E. Parry, P. Flowers. 2011. "Social", "Open" and "Participative"? Exploring personal experiences and organisational effects of enterprise 0 use. Long Range Planning 44(5-6) 375–396.
Dinev, T., M. Bellotto, P. Hart, V. Russo, I. Serra, C. Colautti. 2006. Privacy calculus model in e-commerce - a study of Italy and the United States. European Journal of Information Systems 15(4) 389-402.
Dinev, T., P. Hart, M.R. Mullen. 2008. Internet privacy concerns and beliefs about government surveillance – An empirical investigation. The Journal of Strategic Information Systems 17(3) 214-233.
Dong, J.Q., W. Wu. 2015. Business value of social media technologies: Evidence from online user innovation communities. Journal of Strategic Information Systems 24(2) 113–127.
Doolin, B. 2004. Power and Resistance in the Implementation of a Medical Management Information System. Information Systems Journal 14(4) 343-362.
du Gay, P. 2004. Against 'Enterprise' (But Not Against 'Enterprise', For That Would Make No Sense). Organization 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 & Society 8(2) 200-220.
Eslami, M., A. Rickman, K. Vaccaro, A. Aleyasen, A. Vuong, K. Karahalios, C. Sandvig. 2015. I always assumed that I wasn't really that close to [her]: Reasoning about Invisible Algorithms in News Feeds 33rd Annual ACM Conference on Human Factors in Computing Systems. ACM, 153-162.
Foucault, M. 1977. Discipline and Punish: The Birth of the Prison. Penguin, Harmondsworth.
Foucault, M. 1982. The subject and power. Critical Inquiry 8(4) 777-795.
Foucault, M. 2003. Society Must Be Defended: Lectures At The College De France, 1975–76, trans. David Macey. Picador, New York, NY.
Fowler, G.A. 2020. One of the first contact-tracing apps violates its own privacy policy Washington Post.
Garud, R., S. Jain, P. Tuertscher. 2008. Incomplete by design and designing for incompleteness. Organization studies 29(3) 351-371.
Garud, R., A. Kumaraswamy, V. Sambamurthy. 2006. Emergent by design: Performance and transformation at Infosys Technologies. Organization Science 17(2) 277-286.
Gentry, R.J., W. Shen. 2013. The Impacts of Performance Relative to Analyst Forecasts and Analyst Coverage on Firm R&D Intensity. Strategic Management Journal 34(1) 121-130.
George, J.F. 1996. Computer-Based Monitoring: Common Perceptions and Empirical Results. MIS Quarterly 20(4) 459-480.
Gilliom, J., T. Monahan. 2012. SuperVision: An introduction to the surveillance society. University of Chicago Press.
Gino, F., Krupka, E. L., and Weber, R. A. (2013). License to Cheat: Voluntary Regulation and Ethical Behavior. Management Science, 59(10), 2187-2203.
Goffman, E. 1961. Asylums. Penguin, Harmondsworth.
Goranova, M.L., R.L. Priem, H.A. Ndofor, C.A. Trahms. 2017. Is there a 'Dark Side' to Monitoring? Board and Shareholder Monitoring Effects on M&A Performance Extremeness. Strategic Management Journal 38(11) 2285-2297.
Gozman, D., W. Currie. 2014. The Role of Investment Management Systems in Regulatory Compliance: A Post-Financial Crisis Study of Displacement Mechanisms. Journal of Information Technology 29(1) 44-58.
Grant, R.A., C.A. Higgins. 1991. The Impact of Computerized Performance Monitoring on Service Work: Testing a Causal Model. Information Systems Research 2(2) 116-142.
Guillemette, M.G., I. Fontaine, C. Caron. 2009. A Hybrid Tracking System of Human Resources: A Case Study in a Canadian University. Communications of the Association for Information Systems 24(Artcile 15) 255-268.
Haggerty, K., R. Ericson. 2000. The surveillant assemblage. British Journal of Sociology 51(4) 605-622.

Haggerty, K.D. 2006. Tear down the walls: on demolishing the Panopticon. D. Lyon, ed. Theorizing Surveillance. Willan Publishing, Devon.
Harju, A. A., & Huovinen, A. (2015). Fashionably voluptuous: Normative femininity and resistant performative tactics in fatshion blogs. Journal of 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.
Howard, P., S.C. Woolley. 2016. Political Communication, Computational Propaganda, and Autonomous Agents — Introduction. International Journal of Communication 10 4882-4890.
Huang, J., J. Baptista, S. Newell. 2015. Communicational ambidexterity as a new capability to manage social media communication within organizations. Journal of Strategic Information Systems 24(2) 49–64.
Iedema, R., C. Rhodes. 2010. The Undecided Space of Ethics in Organizational Surveillance. Organization Studies (01708406) 31(2) 199-217.
Jonsson, K. 2006. The Embedded Panopticon: Visibility Issues of Remote Diagnostics Surveillance. Scandinavian Journal of Information Systems 18(2, Article 3) 22 pages.
Kallinikos, J., A. Aaltonen, A. Marton. 2010. A theory of digital objects. First Monday 15(6).
Kallinikos, J., A. Aaltonen, A. Marton. 2013. The Ambivalent Ontology of Digital Artifacts. MIS Quarterly 37 357–370.
Karanasios, S., D. Allen. 2013. ICT for development in the context of the closure of Chernobyl nuclear power plant: an activity theory perspective. Information Systems Journal 23(4) 287-306.
Karwatzki, S., O. Dytynko, M. Trenz, D. Veit. 2017a. Beyond the Personalization–Privacy Paradox: Privacy Valuation, Transparency Features, and Service Personalization. Journal of Management Information Systems 34(2) 369-400.
Karwatzki, S., M. Trenz, V. Tuunainen, D. Veit. 2017b. Adverse consequences of access to individuals' information: an analysis of perceptions and the scope of organisational influence. European Journal of Information Systems 26(6) 688-715.
Kenny, K. 2019. Whistleblowing: Toward a New Theory. Harvard University Press, Cambridge, MA.
Kim, K.K., N.S. Umanath, B.H. Kim. 2005. An Assessment of Electronic Information Transfer in B2B Supply-Channel Relationships Journal of Management Information Systems 22(3) 294–320.
Klein, H.K., M.D. Myers. 1999. A Set of Principles for Conducting and Evaluating Interpretive Field Studies in Information Systems. MIS Quarterly 23(1) 67-93.
Kohli, R., W.J. Kettinger. 2004. Informating the Clan: Controlling Physicians' Costs and Outcomes. MIS Quarterly 28(3) 363-394.
Kordzadeh, N., J. Warren. 2017. Communicating Personal Health Information in Virtual Health Communities: An Integration of Privacy Calculus Model and Affective Commitment. Journal of the Association for Information Systems 18(1) 45-81.
Kosinski, M., D. Stillwell, T. Graepel. 2013. Private traits and attributes are predictable from digital records of human behavior National Academy of Sciences of the United States of America, 5802–5805.
Kubitschko, S. 2015. The role of Hackers in Countering Surveillance and Promoting Democracy. Media and Communication 3(2) 77-87.
Lazega, E. 2000. Rule Enforcement among Peers: A Lateral Control Regime. Organization Studies 21(1) 193-214.
Leclercq-Vandelannoitte, A., H. Isaac, M. Kalika. 2014. Mobile information systems and organisational control: beyond the panopticon metaphor? European Journal of Information Systems 23(5) 543-557.
Lee, D. 2017. Facebook Team Working On Brain-Powered Technology BBC News.
Leonardi, P.M. 2014. Social Media, Knowledge Sharing, And Innovation: Toward a Theory of Communication Visibility. Information Systems Research 25(4) 796-816.
Leonardi, P.M., E. Vaast. 2017. Social Media and Their Affordances for Organizing: A Review and Agenda for Research. Academy of Management Annals 11(1) 150–188.
Levay, C., C. Waks. 2009. Professions and the Pursuit of Transparency in Healthcare: Two Cases of Soft Autonomy. Organization Studies 30(5) 509-527.

Li, X.-B., J. Qin. 2017. Anonymizing and Sharing Medical Text Records. Information Systems Research 28(2) 332-352.
Li, X., S.X. Sun, K. Chen, T. Fung, H. Wang. 2015. Design Theory for Market Surveillance Systems. Journal of Management Information Systems 32(2) 278-313.
Liang, F., V. Das, N. Kostyuk, M.M. Hussain. 2018. Constructing a data-driven society: China's social credit system as a state surveillance infrastructure. Policy & Internet 10(4) 415-453.
Lindberg, K., B. Czarniawska. 2006. Knotting the action net, or organizing between organizations. Scandinavian journal of Management 22(4) 292-306.
Long, C.P., C. Bendersky, C. Morrill. 2011. Fairness Monitoring: Linking Managerial Controls and Fairness Judgments in Organizations. Academy of Management Journal 54(5) 1045-1068.
Loughran, J. 2019. Ministers could be prosecuted under the Official Secrets Act over Huawei 5G leak Engineering & Technology.
Lyon, D. 2001. Surveillance Society: Monitoring Everyday Life. Open University Press, Buckingham.
Lyon, D. 2006. 9/11, synopticon, and scopophilia: Watching and being watched. K.D. Haggerty, R.V. Ericson, eds. The new politics of surveillance and visibility. University of Toronto Press, Toronto, 35-54.
Lyytinen, K., Y. Yoo, R. Boland. 2016. Digital product innovation within four classes of innovation networks. Information Systems Journal 26(1) 47-75.
Majchrzak, A., A. Malhotra. 2013. Towards an information systems perspective and research agenda on crowdsourcing for innovation. The Journal of Strategic Information Systems 22(4) 257-268.
Mann, S., J. Ferenbok. 2013. New Media and the Power Politics of Sousveillance in a Surveillance-Dominated World. Surveillance & Society 11(1/2) 18-34.
Manovich, L. 2001. The language of new media. MIT press.
Marquis, C., C. Qian. 2014. Corporate Social Responsibility Reporting in China: Symbol or Substance? . Organization Science 25(1) 127-148.
Marsden, J.R., Y.A. Tung. 1999. The Use of Information System Technology to Develop Tests on Insider Trading and Asymmetric Information. Management Science 45(8) 1025-1040.
Martin, A.K., R.E. Van Brakel, D.J. Bernhard. 2009. Understanding resistance to digital surveillance: Towards a multi-disciplinary, multi-actor framework. Surveillance & Society 6(3) 213-232.
Marwick, A.E. 2014. How Your Data Are Being Deeply Mined New York Review of Books, 9.
Marx, G.T. 2002. What's New About the" New Surveillance"? Classifying for Change and Continuity. Surveillance & Society 1(1) 9-29.
Mathiesen, T. 1997. The Viewer Society Michel Foucault's Panopticon' Revisited. Theoretical Criminology 1(2) 215-234.
Mayer-Schönberger, V., K. Cukier. 2013. Big Data: A revolution That Will Transform How We Live, Work, and Think. Houghton Mifflin Harcourt, Boston, MA.
Mayo, E. 1975. The Social Problems of an Industrial Civilization. Routledge & Kegan Paul, London.
Mazmanian, M., W.J. Orlikowski, J. Yates. 2013. The Autonomy Paradox: The Implications of Mobile Email Devices for Knowledge Professionals. Organization Science 24(5) 1337-1357.
McCurry, J. 2020. Test, trace, contain: how South Korea flattened its coronavirus curve The Guardian.
Mehra, A., M. Kilduff, D.J. Brass. 2001. The Social Networks of High and Low Self-Monitors: Implications for Workplace Performance. Administrative Science Quarterly 46(1) 121-146.
Metcalf, J. 2018. Facebook may stop the data leaks, but it’s too late: Cambridge Analytica’s models live on MIT Technology Review.
Miller, A.R., C. Tucker. 2013. Active social media management: The case of health care. Information Systems Research 24(1) 52–70.
Muldoon, J. 2017. The Hawthorne studies: an analysis of critical perspectives, 1936-1958. Journal of Management History 23(1) 74-94.
Munro, I. (2019). An interview with Chelsea Manning’s lawyer: Nancy Hollander on human rights and the protection of whistleblowers. Organization, 26(2), 276-290.
Nambisan, S., k. Lyytinen, A. Majchrzak, m. song. 2017. Digital Innovation Management: Reinventing Innovation Management Research in a Digital World. MIS Quarterly 41(1) 223-238.

Natividad, G. 2014. Integration and Productivity: Satellite-Tracked Evidence. Management Science 60(7) 1698-1718.
Newell, S., M. Marabelli. 2015. Strategic opportunities (and challenges) of algorithmic decision-making: A call for action on the long-term societal effects of 'datification'. The Journal of Strategic Information Systems 24(1) 3-14.
Niehoff, B.P., R.H. Moorman. 1993. Justice as a Mediator of the Relationship between Methods of Monitoring and Organizational Citizenship Behavior. Academy of Management Journal 36(3) 527-556.
O'Harrow, R. 2006. No Place To Hide. Free Press.
Orlikowski, W.J., S.V. Scott. 2014. What Happens When Evaluation Goes Online? Exploring Apparatuses of Valuation in the Travel Sector Organization Science 25(3) 868-891.
Ouchi, W.G. 1977. The Relationship between Organizational Structure and Organizational Control. Administrative Science Quarterly 22(1) 95-113.
Ouchi, W.G., M.A. Maguire. 1975. Organizational Control: Two Functions. Administrative Science Quarterly 20(4) 559-569.
Pavlou, P.A. 2011. State of the Information Privacy Literature: Where Are We Now and Where Should We Go? MIS Quarterly 35(4) 977-988.
Pecora, V.P. 2002. The Culture of Surveillance. Qualitative Sociology 25(3) 345-358.
Pierce, L., D.C. Snow, A. McAfee. 2015. Cleaning House: The Impact of Information Technology Monitoring on Employee Theft and Productivity. Management Science 61(10) 2299-2319.
Pierce, L., M.W. Toffel. 2013. The Role of Organizational Scope and Governance in Strengthening Private Monitoring. Organization Science 24(5 ) 1558-1584.
Poppo, L., K.Z. Zhou. 2014. Managing Contracts for Fairness in Buyer--Supplier Exchanges. Strategic Management Journal 35(10) 1508-1527.
Poster, M. 1996. Databases as Discourse; or, Electronic Interpellations. D. Lyon, E. Zureik, eds. Computers, Surveillance, and Privacy. University of Minnesota Press, Minneapolis, 175-192.
Rhodes, R.A. 2007. Understanding Governance: Ten Years On. Organization Studies 28(8) 1243-1264.
Riad, S. 2005. The Power of 'Organizational Culture' as a Discursive Formation in Merger Integration Organization Studies 26(10) 1529-1554.
Rizq, R. 2013. States of Abjection. Organization Studies (01708406) 34(9) 1277-1297.
Rodríguez, G.C., C.A.-D. Espejo, R.V. Cabrera. 2007. Incentives Management During Privatization: An Agency Perspective. Journal of Management Studies 44(4) 536-560.
Roy, D. 1959. "Banana time": Job satisfaction and informal interaction. Human Organization 18(4) 158–168.
Ruolian, F., B. Landis, Z. Zhen, M.H. Anderson, J.D. Shaw, M. Kilduff. 2015. Integrating Personality and Social Networks: A Meta-Analysis of Personality, Network Position, and Work Outcomes in Organizations. Organization Science 26(4) 1243-1260.
Rutherford, M.A., A.K. Buchholtz, J.A. Brown. 2007. Examining the Relationships Between Monitoring and Incentives in Corporate Governance. Journal of Management Studies 44(3) 414-430.
Sarkar, S., R.S. Sriram. 2001. Bayesian Models for Early Warning of Bank Failures. Management Science 47(11) 1457-1475.
Sarker, S., Valacich, J. S., and Sarker, S. (2005). Technology Adoption by Groups: A Valence Perspective. Journal of the Association of Information Systems, 6(2), 37-71.
Sasovova, Z., A. Mehra, S.P. Borgatti, M.C. Schippers. 2010. Network Churn: The Effects of Self-Monitoring Personality on Brokerage Dynamics. Administrative Science Quarterly 55(4) 639-670.
Scott, B.A., C.M. Barnes, D.T. Wagner. 2012. Chameleonic or Consistent? A Multilevel Investigation of Emotional Labor Variability and Self-Monitoring. Academy of Management Journal 55(4) 905-926.
Scott, S.V., W.J. Orlikowski. 2014. Entanglements in Practice: Performing Anonymity through Social Media. MIS Quarterly 38(3) 873-893.
Seaman, J.B., J.A. Erlen. 2015. Workarounds in the Workplace: A Second Look. Orthopedic 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 Magazine.
Sewell, G. 1998. The Discipline of Teams: The Control of Team-based Industrial Work through Electronic and Peer Surveillance. Administrative Science Quarterly 43(2) 397-428.
Sewell, G., J. Barker. 2006. Coercion Versus Care: Using Irony To Make Sense Of Organizational Surveillance. Academy of Management Review 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. . Organization science 22(5) 1312-1321.
Shaw, J.D., N. Gupta, J.E. Delery. 2000. Empirical Organizational-Level Examinations of Agency and Collaborative Predictions of Performance-Contingent Compensation. Strategic Management Journal 21(5) 611-623.
Short, J.L., M.W. Toffel. 2010. Making Self-Regulation More Than Merely Symbolic: The Critical Role of the Legal Environment. Administrative Science Quarterly 55(3) 361-369.
Silva, S. (2020). Coronavirus: How map hacks and buttocks helped Taiwan fight Covid-19. BBC News.
Silva, L., J. Backhouse. 2003. The Circuits-of-Power Framework for Studying Power in Institutionalization of Information System. Journal of the Associations of Inf. Sys. 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. The New York Times.
Singh, R., L. Mathiassen, M.E. Stachura, E.V. Astapova. 2011. Dynamic Capabilities in Home Health: IT-Enabled Transformation of Post-Acute Care. Journal of the Association for Information Systems 12(2) 163-188.
Spiekermann, S., J. Korunovska. 2017. Towards a value theory for personal data. Journal of Information Technology (Palgrave Macmillan) 32(1) 62-84.
Staats, B.R., H. Dai, D. Hofmann, K.L. Milkman. 2017. Motivating Process Compliance Through Individual Electronic Monitoring: An Empirical Examination of Hand Hygiene in Healthcare. Management Science 63(5) 1663-1685.
Stahl, B.C., D.N. F., M. Shaw. 2012. Information security policies in the UK healthcare sector: a critical evaluation. Information Systems Journal 22(1) 77-94.
Stanko, T.L., C.M. Beckman. 2015. Watching you watching me: Boundary control and capturing attention in the context of ubiquitous technology use. Academy of Management Journal 58(3) 712-738.
Statt, N. 2020. ACLU sues facial recognition firm Clearview AI, calling it a 'nightmare scenario' for privacy, May 28, 2020, ed.
Tas, J., J. Kimpen. 2020. Health systems are in need of radical change; virtual care will lead the way MIT Technology Review.
Trahair, R. 2001. George Elton Mayo Biographical Dictionary of Management. Thoemmes, Bristol, 326.
Tung, A., J.R. Marsden. 2000. Trading Volumes with and Without Private Information: A Study Using Computerized Market Experiments. Journal of Management Information 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.
Twyman, N.W., P.B. Lowry, J.K. Burgoon, J.F. Nunamaker. 2014. Autonomous Scientifically Controlled Screening Systems for Detecting Information Purposely Concealed by Individuals. Journal of Management Information Systems 31(3) 106-137.
Vaast, E. 2007. What goes online comes offline: Knowledge management system use in a soft bureaucracy. Organization Studies 28(3) 283-306.
Valentino-DeVries, J. 2020. F.C.C. to Fine Cellphone Carriers for Selling Customers' Locations New York Times.
Van Dijck, J. 2014. Datafication, Dataism and Dataveillance: Big Data between Scientific Paradigm and Ideology Surveillance & Society 12(2) 197-208.
Vance, A., P.B. Lowry, D. Egget. 2015. Increasing accountability through userinterface design artifacts: A new approach to addressing the problem of access-policy violations. MIS Quarterly 39(2) 345-366.

Vance, A., P.B. Lowry, D. Eggett. 2013. Using Accountability to Reduce Access Policy Violations in Information Systems. Journal of Management Information Systems 29(4) 263-290.
Visser, L.M., I.L. Bleijenbergh, Y.W.M. Benschop, A.C.R. van Riel. 2018. Prying Eyes: A Dramaturgical Approach to Professional Surveillance. Journal of Management Studies 55(4) 703-727.
Wareham, J., N. Bjørn-Andersen, P. Neergaard. 1998. Reinterpreting the Demise of Hierarchy: A Case Study in Information Technology, Empowerment and Incomplete Contracts. Information Systems Journal 8(4) 257-272.
Warkentin, M., S. Goel, P. Menard. 2017. Shared Benefits and Information Privacy: What Determines Smart Meter Technology Adoption? Journal of the Association for Information Systems 18(11) 758-786.
Weber, M. 1949. The Methodology of the Social Sciences. Free Press, New York.Whetten, D.A. 1989. What Constitutes a Theoretical Contribution? Academy of Management Review 14(4) 490-495.
Williams, T. 1996. Government Regulation through Voluntary Cooperation: A Follow-up Study of the Strategic Impact of Information Technology. Journal of Strategic Information Systems 5 149-156.
Wood, D. 2002. Foucault and Panopticism Revisited. Surveillance & Society 1(3) 234-239.
Woolley, S.C., P.N. Howard. 2016. Automation, Algorithms, and Politics| Political Communication, Computational Propaganda, and Autonomous Agents — Introduction. International Journal of Communication 10(0) 9.
Xu, H., H.-H. Teo, B.C.Y. Tan, R. Agarwal. 2009. The Role of Push--Pull Technology in Privacy Calculus: The Case of Location-Based Services. Journal of Management Information Systems 26(3) 135-173.
Xu, H., H. Teo, B.C. Tan, R. Agarwal. 2009-10. The role of push-pull technology in privacy calculus: the case of location-based services. Journal of Management Information Systems 26(3) 135-174.
Yates, J. 1993. Control Through Communication: The Rise of System in American Management. Johns Hopkins University Press, Baltimore, MD.
Yoo, Y., O. Henfridsson, K. Lyytinen. 2010. Research commentary—the new organizing logic of digital innovation: an agenda for information systems research. Information systems research 21(4) 724-735.
Zhang, X., V. Venkatesh. 2013. Explaining Employee Job Performance: The Role of Online and Offline Workplace Communication Networks. MIS Quarterly 37(3) 695-722.
Zittrain, J. 2008. The future of the internet--and how to stop it. Yale University Press.
Zuboff, S. 2015. Big other: surveillance capitalism and the prospects of an information civilization. Journal of Information Technology 30(1) 75-89.
Zuboff, S. 2016. The Secrets of Surveillance Capitalism Frankfurter Allgemeine Feuilleton.
Zuboff, S. 2019. The age of surveillance capitalism: the fight for the future at the new frontier of power. Profile Books.

**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:<br>• Above (i.e. from French "sur" ("over") and 'veiller' ("see/watch")),<br>• Below (i.e. from French "sous" ("under") and "veiller" ("see/watch")) | Government watching citizens; managers watching employees; firms watching customers | Doolin 2004; Lyon 2001; 2006; Zuboff 2015; 2018 | • Offers contradictory insights on the nature of the watcher<br>• Implies hierarchical top-down relationships between watchers and watched<br>• Prioritizes actor on particular hierarchical side (e.g. from the sur- or the sous- type)<br>• Assumes IT tools as stable objects |
| **Sousveillance** | | | Protestors filming police; corporate; citizens watching government; CCTV; peer monitoring on social media | Brivot & 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 | Clegg et al. 2012; Foucault 1977 | • Does not account for agency of watched, implies their consciousness<br>• Fails to include flexible organizational spaces<br>• Fails to include IT-enabled reciprocal interconnections of watcher and watched<br>• Assumes IT tools as stable objects |
| *Electronic/ information* | | Monitoring with enhanced visibility of all IT-mediated actors and processes | Employees and customers monitored by corporations via IT systems | Jonsson 2006; Lyon 1994; Orlikowski 1991; | • Fails to include IT-enabled reciprocal interconnections of watcher and watched<br>• Assumes IT tools as stable objects |
| *Portable (free control)* | | Monitoring of all IT-mediated spaces | Corporate monitoring of distanced work | De Saulles & Horner 2011; Leclercq-Vandelannoitte et al. 2014 | • Fails to incorporate IT-enabled reciprocal interconnections of watcher and watched<br>• Implies consciousness of being tracked by watched<br>• Assumes IT tools as stable objects |
| *Super-* | | IT-enhanced monitoring "without walls, windows, towers or guards" (Poster 1996, p. 93) | Electronic databases | Poster 1995; 1996 | • Fails to incorporate interconnections between the watcher and the watched<br>• Assumes IT tools as stable objects |
| *Post-* | | Monitoring enabling softer and more distributed forms of control | Participatory management; corporate transparency culture; total quality management | Baudrillard 2006; 2007; du Gay 2004; Iedema & Rhodes, 2010; Sewell & Barker 2006 | • Fails to incorporate IT-enabled reciprocal interconnections between the watcher and the watched<br>• Implies consciousness of being tracked by the watched<br>• Assumes IT tools as stable objects |
| **Synopticon** | | Monitoring where many watch the few (from Greek "syn" ("with/ together") & "opticon" ("observed")) | Politicians scrutinized via the masses; celebrities or favorite organizations followed on social media | Boyne 2000; Lyon 2006; Mathiesen 1997 | • Fails to incorporate IT-enabled reciprocal interconnections of watcher and watched (does consider top-down & centralized control) |

| | | | | | |
|---|---|---|---|---|---|
| **Dataveillance** | Data flows | IT-enabled systematic monitoring of people or groups in order to regulate or govern their behaviour | Customer loyalty cards; swipe corporate cards; monitoring of truck drivers; Google search engine; EyeSee Mannequins[8] ; Google maps app[9] | Clarke 1988; 2003; Van Dijck 2014; Degli Esposti 2014; Zimmer 2008 | • Does not include non-IT monitoring<br>• Assumes IT tools as stable objects |
| **Assemblages** | | Monitoring of multi-directional temporary data flows (i.e. rhizome-like structures without one centre) created by multiple heterogenous actors | Facebook app; data generated, searched, and collected from IPhone; contemporary policing collecting information from aggregated databases and multiple agents | Deleuze & Guattari 1987; Haggerty 2006; Haggerty & Ericson 2000; Hess 2008 | • Analytically challenged for what to include/exclude: filtering of IT precludes heterogenous and multidirectional connections<br>• Assumes IT tools as stable objects |
| **Panspectron** | | Monitoring that bypasses visible practices (e.g., base for panopticon) and shifts attention to non-visible practices enabled by IT | Encryption techniques, wireless technologies, AI that offers new, invisible or hard to detect monitoring dimensions | DeLanda 1991 | • Focusses on IT-enabled monitoring only<br>• Does not take the co-existing forms of hierarchical control into account<br>• Assumes IT tools as stable objects |

**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; Leonardi and Vaast 2017; Lyytinen et al. 2016) |
| 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 broken down into self-sufficient blocks (or modules) down to elementary units. | (Kallinikos et al. 2013; Manovich 2001; Yoo et al. 2010; Zittrain 2008) |
| 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) |
| Re-programmability | Ability of IT to be accessible and modifiable by other digital objects. | (Kallinikos et al. 2013; Leonardi and Vaast 2017; Yoo et al. 2010; Zittrain 2008) |

[8] EyeSee Mannequin, produced by the Italian company Almax, uses facial recognition technology to reveal customers: age range; gender; race; number of people and time and voice recognition applications to listen to what shoppers say about mannequins Degli Esposti, S. 2014. When big data meets dataveillance: The hidden side of analytics. *Surveillance & Society* **12**(2) 209-225.

[9] 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 (Economist 2010).

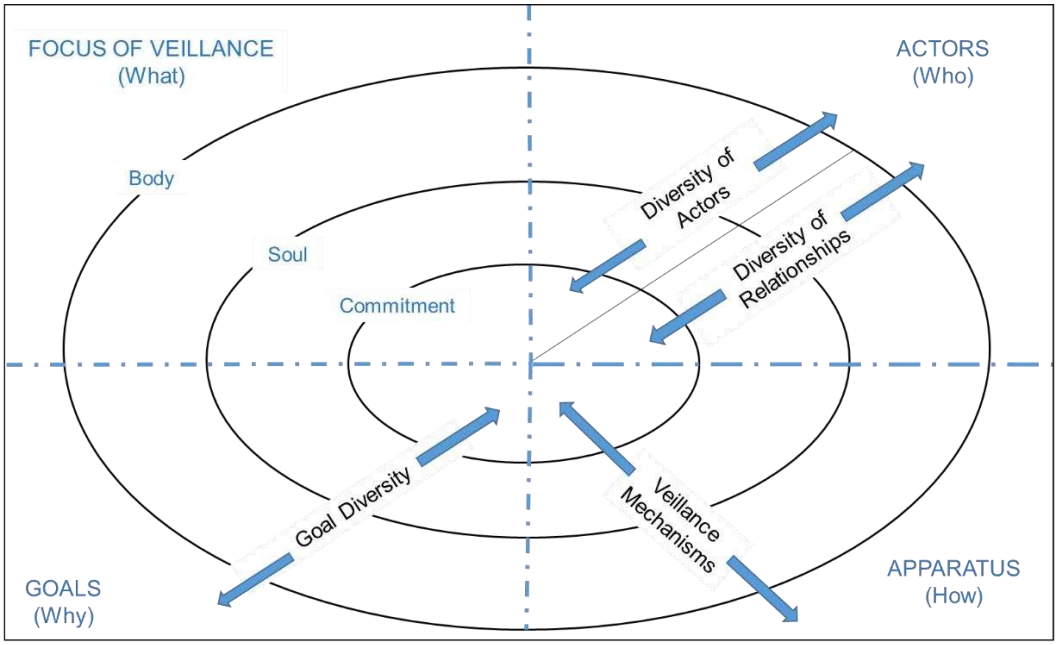


**Figure 1. Conceptual Veillance Web Framework**

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

| | ACTORS | | | | | IT or Non-IT | Citation counts | Key topics |
|---|---|---|---|---|---|---|---|---|
| | Org | Emp | Cust | Other | Gov | | | |
| **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); transforamtions of work practices |
| 2 | | Ww | | | | NON IT | 15 | Impacts of employee self-awareness, self-regulation and peer monitoring on job performance |
| | | | | | | IT | 1 | Third party online and offline surveillance in teams |
| 3 | | | | Ww | | 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 | Inter-organizational veillance in traditional industries (e.g. construction, sport) |
| | | | | | | IT | 3 | Inter-organizational veillance in indusries that were transformed or enabled by IT |
| 6 | W | | w | | | NON-IT | 1 | Custormer secondary data collection via catalogs and magazine subscriptions |
| | | | | | | IT | 7 | Custormer 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 prvatization 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 | Ww | | | | | 8 | IT-enhanced capability of making employees visible to their managers and peers |
| 4 | W | | Ww | | | | 1 | Predictions in crowd generated data |
| 5 | Ww | | Ww | | | | 4 | Multi-directional monitoring on online platforms |
| 6 | w | | W | | W | | 1 | Impact of customers' culture and state regulation on corporeate 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 |

**Table 4. Actor Involvement in IT and non-IT veillance**

| | 3 or more actors | 2 or more Watchers (W) | 2 or more Watched (w) | Has both W and w (Wv 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* |

**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% |
| *Total across papers* | 62 | 25 | 45 | 132 | | | |

**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 | | | |

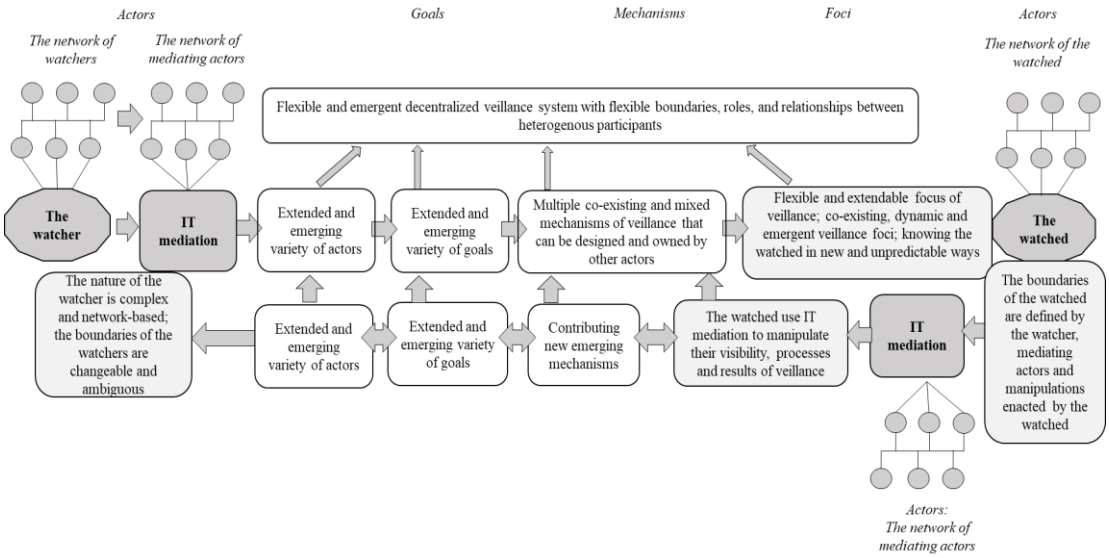


**Figure 2. Action Net Model of IT Veillance**

## APPENDIX A. CONCEPTUAL FRAMEWORK

**Table A1. Veillance Typology[a] and Examples**

| Veillance Types | Focus of Veillance: **BODY** *Body and behavior* | **SOUL** *Social, informal and emotional life of the watched* | **COMMITMENT** *Self-monitoring, teamwork, peer scrutiny* |
|---|---|---|---|
| **NON-IT** | • Direct observation from managers in Taylor-like factories with body and motion routines | • Ford Sociological Department's monitoring of employee work and life experiences, thoughts and feelings that guide their work (to know about their lives outside of work) | • Team peer monitoring<br>• Academic freedom (self-regulation)<br>• Total institutions where all parts of life of an individual are under control[b] |
| **IT-MEDIATED** | • Use of CCTV cameras<br>• Use of ERP systems<br>• Use of biometrics identification<br>• Use of health monitoring tools (heart rate, activity, etc.)<br>• Organizational collection of price matching data | • Collection of information about personality traits, preferences, likes, etc. by social media companies<br>• Company monitoring of the blogosphere and employee social media accounts<br>• Viewing/participating in reality TV<br>• Digital documentation and display of personal life on social networks | • Peer monitoring in virtual teams<br>• Norms of continuous online accessibility and responsiveness<br>• Co-author scrutiny of collaborative work in the cloud<br>• Pre-employment screening and simulations to discover the extent to which the employee would be hard-working and committed |

[a] While the distinction between foci of veillance is analytical (e.g., Clegg and Courpasson 2004; Clegg et al. 2006), it helps us to illustrate differences between a variety of veillance practices and their results in the form of Weberian ideal types (Weber 1949).
[b] Clegg et al. (2012) and Goffman (1961) provide more details.

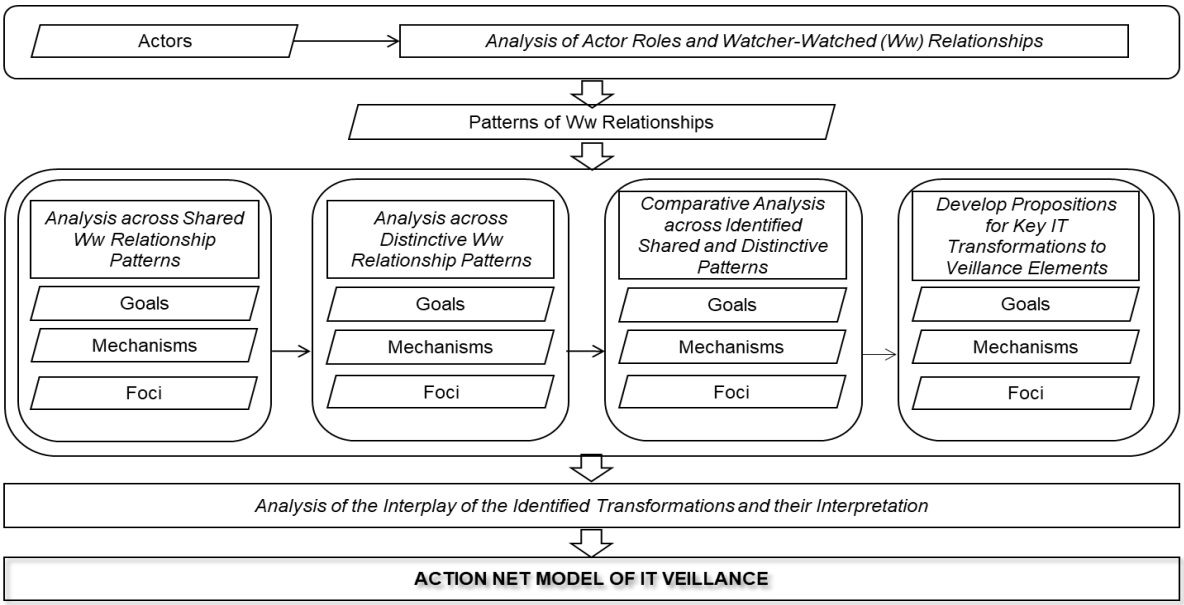


**Figure A1. Data Analysis Process**

## APPENDIX B. LITERATURE REVIEW AND CODING PROCESS

### Literature Review Process and Sample Selection

The literature review was conducted on the top eight MOS[10] and top eight IS[11] journals. The search was conducted on all articles published from each journal's inception[12]. To ensure articles that discussed veillance concepts were included even if they did not explicitly recognize such concepts, we used a broad set of search keywords related to monitoring practices: *surveillance, panopticon, monitoring, privacy* and *audit*. The latter three keywords generated many false positives (e.g., articles identified because of the audit keyword but discussing accounting concepts or articles identified with the privacy keyword that did not include any concepts related to veillance). We also searched for the keyword 'surveillance' in the Business Source EBSCO database and conducted a citation analysis. Table A1 provides detailed counts of the identified papers as well as counts of papers removed during the various screenings discussed below.

**Table B1. Number of Articles Identified and Screened in Literature Review**

| Journal | Identified by keyword search | Initial screening | Initial sample | Deep screening - remove | Screened sample | Added at citation analysis | Final sample |
|---|---|---|---|---|---|---|---|
| **Management and Organization Studies (MOS)** | | | | | | | |
| AMJ | 67 | 48 | 19 | 5 | 14 | 0 | 14 |
| AMR | 27 | 15 | 12 | 12 | 0 | 0 | 0 |
| ASQ | 32 | 17 | 15 | 2 | 13 | 1 | 12 |
| JMS | 47 | 33 | 14 | 6 | 8 | 1 | 9 |
| MS | 109 | 89 | 20 | 8 | 12 | 0 | 13 |
| OrgSc | 25 | 16 | 9 | 1 | 8 | 2 | 10 |
| OrgStu | 42 | 29 | 13 | 1 | 12 | 3 | 15 |
| SMJ | 27 | 13 | 14 | 4 | 10 | 0 | 10 |
| | 376 | 260 | 116 | 37 | 79 | 7 | **83** |
| **Information Systems (IS)** | | | | | | | |
| EJIS | 28 | 20 | 8 | 6 | 2 | 0 | 2 |
| ISJ | 15 | 10 | 5 | 4 | 1 | 5 | 6 |
| ISR | 34 | 26 | 8 | 4 | 4 | 0 | 4 |
| JAIS | 31 | 23 | 8 | 5 | 3 | 3 | 6 |
| JIT | 27 | 19 | 8 | 5 | 3 | 0 | 3 |
| JMIS | 55 | 36 | 19 | 6 | 13 | 0 | 13 |
| JSIS | 21 | 16 | 5 | 2 | 3 | 0 | 3 |
| MISQ | 42 | 24 | 18 | 9 | 9 | 3 | 12 |
| | 253 | 174 | 79 | 38 | 41 | 11 | **49** |
| **SUM** | **629** | **434** | **195** | | **114** | **18** | **132** |

AMJ: Academy of Management Journal, AMR: Academy of Management Review, ASQ: Administrative Science Quarterly, EJIS: European Journal of Information Systems, ISJ: Information Systems Journal, ISR: Information Systems Research, JIT: Journal of Information Technology, JMIS: Journal of Management Information Systems, JMS: Journal of Management Studies, JSIS: Journal of Strategic Information Systems, JAIS: Journal of the Association of Information Systems, MS: Management Science, MISQ: MIS Quarterly, OrgSc: Organization Science, OrgStu: Organization Studies, and SMJ: Strategic Management Journal.

In the initial screening, one co-author reviewed all identified papers' abstracts and keywords to remove articles that were (1) clearly not related to the concepts surrounding veillance, (2) editorials, (3) panels and workshops, (4) commentaries, (5) teaching cases, (6) purely scale development papers, (7) calls for papers and (8) book reviews. In case of doubt, the paper was retained in the sample for an in-depth screening. Of the initial 629 articles, 195 articles were retained after the first screening. The second

[10]Financial Times list of top 50 business journals, available at https://www.ft.com/content/3405a512-5cbb-11e1-8f1f-00144feabdc0.

[11] Consistent with prior literature reviews of IS journals (e.g., Bélanger and Carter 2012; Roberts et al. 2012), we used the eight leading IS journals in the Association for Information Systems Senior Scholars' list, available at https://aisnet.org/?SeniorScholarBasket.

[12] We collected and coded all papers until early 2018. We also include in our discussions papers that were published in 2019 and 2020. Overall, newer papers did not provide additional insights from the coded sample.

screening involved a second co-author who reviewed the complete articles that were marked for in-depth screening and evaluated these in terms of their relevance for veillance research. Any article that was not clearly related to veillance research was then screened by a third co-author to confirm its removal or debate its relevance. To illuminate what is made visible and how, in non-IT and IT monitoring, we coded only empirical articles while we also considered conceptual papers in our review and discussion. After the second screening, 114 papers were retained and marked for in-depth coding. Concurrently with the in-depth coding of the screened sample, a citation analysis was conducted to identify key additional articles from the top journals, which led to the inclusion of an additional 18 papers. The final sample is therefore 132 articles.

**Coding**

Guided by the VW framework, empirical papers were coded as follows. Initially, three co-authors separately and iteratively coded four articles and then compared their coding, discussing differences and reaching agreement on coding categories. Then each co-author coded a set of articles, which was then verified by a different co-author. Any code that was unclear was marked for discussion. In the end, most articles were double or triple coded to ensure consistency across coders and that there were no coding disagreements left.

Once all coding was completed, we reflected on the process to ensure there was consistency between interpretation of the data and emergent veillance concepts (Klein and Myers 1999). Many articles did not explicitly recognize the veillance theme in their work, discussing veillance as a side concept or as part of another phenomenon. Examples included how noncompliance with security policies leads to the need for veillance (D'Arcy et al. 2009; Vance et al. 2013) or how veillance creates issues regarding information privacy (e.g., Allen et al. 2007; Bennett et al. 2008). Importantly, along with articles that primarily focused on monitoring, these articles provided an important basis for our analysis, helping us to explore the key factors underlying how IT transforms relationships between the watcher and the watched. These factors contributed to the iterative development of the key elements of the VW framework. The final coding categories and sub-categories are shown in Table A2.

**Table B2. Final Coding Categories and Attributes of the VF**

| Category | Description | Sub-category | Description |
|---|---|---|---|
| Veillance type | Discusses whether veillance is conducted or driven by IT or not. Can be both. | Non-IT Veillance | Social operation of making visible. |
| | | IT Veillance | IT-mediated social operation of making visible. |
| Veillance actors and relationships | Actors refer to both the watchers and the watched. Actors can be watchers (W), watched (w) or both (Ww). | Organizations | Subjects discussed or studied are organizations. |
| | | Employees | Subjects discussed or studied are employees of organizations. |
| | | Customers | Subjects used in study are customers or clients of commercial organizations. |
| | | Governments | Subjects discussed or studied are states, nations, governments, or governmental agencies. |
| | | Other people (students, citizens, etc.) | Subjects discussed or studied are other people such as students, friends (social media), citizens, or other actors. |
| Veillance goals | Describes the purpose of veillance; veillance effort may seek to achieve multiple concurrent goals. | Compliance | When the goal of veillance is to ensure subjects' compliance with rules and/or standards. |
| | | Discovery | When a situation requires a search for a person and/or specific details via veillance. Different from prevention in that discovery is focused on current situation (and prevention is about stopping future occurrence of a situation). |
| | | Documentation | When veillance is about getting fundamental documentation of subjects' activity; can include documenting agent's |

| | | | |
|---|---|---|---|
| | | | interaction with subjects according to procedures when applicable. |
| | | Entertainment | When veillance is a form of entertainment (e.g., Big Brother TV program). |
| | | Influence/ persuasion | When veillance is strategically conducted to influence subjects' action (e.g., behavioral targeting of consumers online). |
| | | Prevention/ protection | When veillance is used to protect resources and to prevent future occurrence of risky events (e.g., security breaches, spread of infectious diseases). |
| | | Profit | When veillance is used to turn a profit through a variety of intermediate goals (compliance, influence, among others). |
| | | Provision of benefits (resources) | When veillance is used to ensure that is being done; typically works in conjunction with verification; e.g., verification is needed to get access to benefits. |
| | | Self-improvement | Veillance of self to understand oneself better and/or to improve self. |
| | | Verification | Veillance that is used to scrutinize and verify that eligibility criteria are met. The subject agrees to be scrutinized to gain some benefit (or access to resources). |
| Veillance foci | Describes the focus of the social operation of veillance, describing what is visible and knowable | Veillance of body (VoB) | Social operation of making visible the bodies and behaviors of the watched |
| | | Veillance of soul (voS) | Social operation of making visible the informal work relationship or private life of the watched. Encompasses veillance of body but stresses the priority of knowing informal work relations, consciousness and unconsciousness driving the watched |
| | | Veillance of commitment (VoC) | Social operation of making visible the commitment of the watched. |
| Veillance mechanisms | How veillance is conducted | Hard | Veillance mechanisms such as coercion (forcing others to be visible usually by physical power), marking of the body, physical inscription (using the architecture, geometry and design to visualize those inscribed into the spatial boundaries), inspection and fear inducement (making visible by a source of external motivation such as fear expectations). |
| | | Soft | Veillance mechanisms such as seduction (making others visible by making them desiring to do so by intriguing, emotionally or sensually involving them so they are self-interested and involved in being visible), deception (when those made visible are deceived into thinking that there is a mutual benefit and self-interest in visibility), reward inducement (making visible by a source of external motivation such as reward expectations) and internalization (making others visible because they freely and willingly assume this is in their best interest and part of the values and culture that they share). |

## APPENDIX C. DETAILED CODING OF PAPERS

**Table C1. Leading Eight MOS Journals Coding (n = 83)**

| | | | NON-IT VEILLANCE | | | | | | | | | | | | | | | | | | | | | IT-VEILLANCE | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | FOCI | | | Goals | | | | | | | | | | | Mechanisms | | ACTORS W = Watchers w = watched | | | | | FOCI | | | Goals | | | | | | | | | | | | Mechanisms | | ACTORS W = Watchers w = Watched | | | | |
| Authors | Year | Journal | BODY | SOUL | COMMITMENT | Documentation | Verification | Prevention/protection | Discovery | Influence/persuasion | Profit | Provision of benefits+ | Self-improvement | Compliance | Entertainment | Hard | Soft | Organizations | Employees | Customers | Other people | Government | BODY | SOUL | COMMITMENT | Documentation | Verification | Prevention/protection | Discovery | Influence/persuasion | Profit | Provision of benefits+ | Self-improvement | Compliance | Entertainment | Hard | Soft | Organizations | Employees | Customers | Other people | Government |
| Adjerid et al. | 2016 | MS | | | | | | | | | | | | | | | | | | | | | x | | | | x | x | | | | | | | x | W,w | | w | | W |
| Arthurs et al. | 2008 | AMJ | | x | | | | | | | x | | | | | | x | W | w | | | | | | | | | | | | | | | | | | | | | | | |
| Ball et al. | 2000 | OrgStu | | | | | | | | | | | | | | | | | | | | | x | x | | | | | | | | | x | | | x | x | W | w | | | |
| Banker et al. | 1996 | AMJ | x | | | | | | | | x | | | x | | x | | W | w | | | | | | | | | | | | | | | | | | | | | | | |
| Barrett et al. | 2012 | OrgSc | x | | | x | | | x | | | | | | | x | | | W,w | | | | | | | | | | | | | | | | | | | | | | | |
| Beatty & Zajac | 1994 | ASQ | | x | | | | | | | x | | | | | | x | W | w | | | | | | | | | | | | | | | | | | | | | | | |
| Belot & Schröder | 2016 | MS | x | | | | x | | | | | | | | | x | | | | | W,w | | | | | | | | | | | | | | | | | | | | | |
| Bernstein | 2012 | ASQ | x | | | | | | | | x | | | x | | x | | W | W | | | | x | | | | | | | | | x | | | | x | | W | w | | | |
| Brocklehurst | 2001 | OrgStu | x | x | | | | | | | | | | x | | x | x | W | w | | | | x | | | | x | | | | | | x | | | x | | W | w | | | |
| Campbell et al. | 2005 | MS | | | | | | | | | | | | | | | | | | | | | x | | | | | | | | x | | | x | | x | | W,w | | W,w | | |
| Clegg et al. | 2012 | OrgStu | | | x | | | | | | | | | x | | x | x | | | | w | W | | | | | | | | | | | | | | | | | | | | |
| Clegg et al. | 2002 | OrgStu | | | x | | | | | | | | | x | | | x | W,w | | | | | | | | | | | | | | | | | | | | | | | | |
| Collinson | 1999 | OrgStu | x | | | | | x | | | x | | | | | x | | W | W | | | | | | | | | | | | | | | | | | | | | | | |
| Combs et al. | 2007 | JMS | | x | | | | | | | x | | | | | | x | W,w | W,w | | | | | | | | | | | | | | | | | | | | | | | |
| Conlon & Parks | 1990 | AMJ | x | | | | | | | | x | | | x | | x | | W | w | | | | | | | | | | | | | | | | | | | | | | | |
| Culnan & Armstrong | 1999 | OrgSc | | | | | | | | | | | | | | | | | | | | | x | | | | | | | | x | x | | | | x | | W | | w | | |
| Deary et al. | 2002 | JMS | | | | | | | | | | | | | | | | | | | | | x | | | | | | | | x | | | x | | x | | W | w | | | |
| Dejong & Elfring | 2010 | AMJ | | x | | | | | | | | | | x | | | x | | W,w | | | | | | | | | | | | | | | | | | | | | | | |
| Dencker | 2009 | ASQ | x | x | | | | | | | | | | x | | x | x | W | w | | | | | | | | | | | | | | | | | | | | | | | |
| Desender et al. | 2013 | SMJ | | x | | | | | | | x | | | | | | x | W | w | | | | | | | | | | | | | | | | | | | | | | | |
| Dharwadkar | 2008 | OrgSc | | x | | | | | | | x | | | | | | x | W | w | | | | | | | | | | | | | | | | | | | | | | | |
| Ezzamel et al. | 1998 | ASQ | x | | | | | | | | x | | | x | | x | x | W | w | | | | x | | | | x | | x | | | x | | | | x | | | | | | |
| Fineman | 1998 | OrgStu | x | | | | | | | | | | | x | | x | | w | | | | W | | | | | | | | | | | | | | | | | | | | |
| Finkelstein et al. | 1994 | AMJ | | x | | | | | | | x | | | | | | x | W | w | | | | | | | | | | | | | | | | | | | | | | | |
| Gentry & Shen | 2013 | SMJ | x | x | | | | | | | x | | | | | x | x | W,w | | | | | | | | | | | | | | | | | | | | | | | | |
| Gino et al. | 2013 | MS | x | | | | | | | | | | | x | | x | | w | | | W | | | | | | | | | | | | | | | | | | | | | |
| Goranova | 2010 | SMJ | x | | | | | | | | x | | | | | x | | W | w | | | | | | | | | | | | | | | | | | | | | | | |
| Greenwood | 2007 | OrgStu | x | x | | | | | | | x | | | | | x | x | W | w | | | | | | | | | | | | | | | | | | | | | | | |
| Guillaume | 2014 | AMJ | | x | | | | | | | | | x | | | | x | | W,w | | | | | | | | | | | | | | | | | | | | | | | |

**Table C1 (Cont.). Leading Eight MOS Journals Coding (n = 83)**

| | | | NON-IT VEILLANCE | | | | | | | | | | | | | | | | | | | | | IT-VEILLANCE | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | FOCI | | | Goals | | | | | | | | | | | Mechanisms | | ACTORS W = Watchers w = watched | | | | | FOCI | | | Goals | | | | | | | | | | | | Mechanisms | | ACTORS W = Watchers w = Watched | | | | |
| Authors | Year | Journal | BODY | SOUL | COMMITMENT | Documentation | Verification | Prevention/protection | Discovery | Influence/persuasion | Profit | Provision of benefits+ | Self-improvement | Compliance | Entertainment | Hard | Soft | Organizations | Employees | Customers | Other people | Government | BODY | SOUL | COMMITMENT | Documentation | Verification | Prevention/protection | Discovery | Influence/persuasion | Profit | Provision of benefits+ | Self-improvement | Compliance | Entertainment | Hard | Soft | Organizations | Employees | Customers | Other people | Government |
| He & Wang | 2009 | AMJ | x | x | | | | | | | x | | | | | x | x | W | w | | | | | | | | | | | | | | | | | | | | | | | | |
| Huddart | 1993 | MS | x | | | | | | | | x | | | | | x | | W | w | | | | | | | | | | | | | | | | | | | | | | | | |
| Iedema et al | 2006 | OrgStu | | x | | | | | | | | | x | x | | x | x | | W,w | | | | | | | | | | | | | | | | | | | | | | | | |
| Iedema & Rhodes | 2010 | OrgStu | | | | | | | | | | | | | | | | | | | | | | | x | x | | x | x | | | | x | | | x | | W | W,w | | | | |
| Jensen | 2006 | ASQ | x | | | | | | | x | | | | | | x | | W,w | | | | | | | | | | | | | | | | | | | | | | | | | |
| Kurland & Egan | 1999 | OrgSc | | | | | | | | | | | | | | | | | | | | | x | | | | | | | | | | x | | | x | | W | w | | | | |
| Lane et al. | 1998 | SMJ | x | x | | | | | | | x | | | | | x | x | W | w | | | | | | | | | | | | | | | | | | | | | | | | |
| Langfred | 2004 | AMJ | x | x | | | | | | | | | | x | | x | x | | W,w | | | | | | | | | | | | | | | | | | | | | | | | |
| Lazega | 2000 | OrgStu | x | x | | | | | | | x | | | x | | x | x | | W,w | | | | | | | | | | | | | | | | | | | | | | | | |
| Levay & Waks | 2009 | OrgStu | | | x | | | | | | | | x | x | | | x | | W,w | | | | | | | | | | | | | | | | | | | | | | | | |
| Li & Sarkar | 2013 | MS | | | | | | | | | | | | | | | | | | | | | | x | | | | | x | | | | x | | | x | | W | w | w | | | |
| Long et al. | 2011 | AMJ | x | x | x | | x | | | | | | | x | | | x | W,w | W,w | | | | | | | | | | | | | | | | | | | | | | | | |
| Loughry & Tosi | 2011 | OrgSc | x | | | | | | | | | | | x | | x | x | | W,w | | | | | | | | | | | | | | | | | | | | | | | | |
| Marquis & Qian | 2014 | OrgSc | x | | | | x | | | | | x | | x | | x | | w | | | | W | | | | | | | | | | | | | | | | | | | | | |
| Marsden & Tung | 1999 | MS | | | | | | | | | | | | | | | | | | | | | x | | | x | x | | | | | | x | | | x | | W | w | | | | |
| Mazmanian et al. | 2013 | OrgSc | | | | | | | | | | | | | | | | | | | | | x | x | | | | | | | | | x | | | x | x | W | W,w | | | | |
| Mehra et al. | 2001 | ASQ | | x | | | | | | x | | x | | | | | x | | W,w | | | | | | | | | | | | | | | | | | | | | | | | |
| Milberg et al. | 2000 | OrgSc | | | | | | | | | | | | | | | | | | | | | x | | | | | | | | | | x | | | x | | w | | W | | W | |
| Natividad | 2014 | MS | | | | | | | | | | | | | | | | | | | | | x | | | x | | | x | | x | | | | | x | | W,w | w | | | | |
| Niehoff & Moorman | 1993 | AMJ | x | | | | | | | | | | | x | | x | x | W | w | | | | | | | | | | | | | | | | | | | | | | | | |
| Ogbonna & Wilkinson | 2003 | JMS | x | | | | x | | | | x | | | x | | x | | W | w | | | | | | | | | | | | | | | | | | | | | | | | |
| Ouchi | 1977 | ASQ | x | | | | x | | | | x | | | x | | x | | W | w | | | | | | | | | | | | | | | | | | | | | | | | |
| Ouchi & Maguire | 1975 | ASQ | x | | | | x | | | | x | | | x | | x | | W | w | | | | | | | | | | | | | | | | | | | | | | | | |
| Perlow | 1998 | ASQ | x | x | | | | | | | x | | | x | | x | x | W | w | | | | | | | | | | | | | | | | | | | | | | | | |
| Pierce & Toffel | 2013 | OrgSc | x | | | | x | | | | | | | x | | x | | Ww | | | | | | | | | | | | | | | | | | | | | | | | | |
| Pierce et al. | 2015 | MS | | | | | | | | | | | | | | | | | | | | | x | | | | x | | | | x | | | x | | x | | W | w | | | | |
| Poppo & Zhou | 2014 | SMJ | x | | | | x | | | | | | | | | x | | W,w | | | | | | | | | | | | | | | | | | | | | | | | | |
| Premeaux & Bedeian | 2003 | JMS | | x | | | | | | | | | | x | | | x | | W,w | | | | | | | | | | | | | | | | | | | | | | | | |
| Rediker & Seth | 1995 | SMJ | | x | | | x | | | | | | | x | | x | | W | w | | | | | | | | x | | | | | | x | | | | | W | w | | | | |

**Table C1 (Cont.). Leading Eight MOS Journals Coding (n = 83)**

| | | | NON-IT VEILLANCE | | | | | | | | | | | | | | | | | | | | IT-VEILLANCE | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | FOCI | | | Goals | | | | | | | | | | Mechanisms | | ACTORS W = Watchers w = watched | | | | | FOCI | | | Goals | | | | | | | | | | | Mechanisms | | ACTORS W = Watchers w = Watched | | | | |
| Authors | Year | Journal | BODY | SOUL | COMMITMENT | Documentation | Verification | Prevention/protection | Discovery | Influence/persuasion | Profit | Provision of benefits+ | Self-improvement | Compliance | Entertainment | Hard | Soft | Organizations | Employees | Customers | Other people | Government | BODY | SOUL | COMMITMENT | Documentation | Verification | Prevention/protection | Discovery | Influence/persuasion | Profit | Provision of benefits+ | Self-improvement | Compliance | Entertainment | Hard | Soft | Organizations | Employees | Customers | Other people | Government |
| Reuer et al. | 2014 | SMJ | | x | | | x | | | | | | | x | | x | | W | w | | | | | | | | | | | | | | | | | | | | | | | |
| Riad | 2005 | OrgStu | | x | | | | | x | x | | | | | | | x | W,w | W,w | | | | | | | | | | | | | | | | | | | | | | | |
| Rizq | 2013 | OrgStu | | | | | | | | | | | | | | | | | | | | | x | | | x | | | | x | x | | | | x | | w | w | | W | |
| Rodríguez et al. | 2007 | JMS | x | | | | x | | | | x | | | x | | x | | W | w | | | W | | | | | | | | | | | | | | | | | | | |
| Ruolian et al. | 2015 | OrgSc | | x | | | | | | x | | | | | | | x | | W,w | | | | | | | | | | | | | | | | | | | | | | | |
| Rutherford et al. | 2007 | JMS | x | | | | x | | | | x | | | x | | x | | W | w | | | | | | | | | | | | | | | | | | | | | | | |
| Sarkar and Sriram | 2001 | MS | | | | | | | | | | | | | | | | | | | | | x | | | | x | | x | | | | | | x | | w | | | W | |
| Sasovova et al. | 2010 | ASQ | | x | | | | | | x | | | | | | | x | | W,w | | | | | | | | | | | | | | | | | | | | | | | |
| Scott et al. | 2012 | AMJ | | x | | | | | | x | | x | | | | | x | | W,w | | | | | | | | | | | | | | | | | | | | | | | |
| Sewell | 1998 | ASQ | | | | | | | | | | | | | | | | | | | | | | x | | | | | | | x | | | x | | | x | W | W,w | | | |
| Shaw et al., | 2000 | SMJ | x | | | | x | | | | x | | | x | | x | | W | w | | | | x | | | | x | | | | x | | | x | | x | | W | w | | | |
| Short &Toffel | 2010 | ASQ | x | x | | | | | | | | | | x | | x | x | w | | | | W | | | | | | | | | | | | | | | | | | | |
| Staats et al. | 2017 | MS | | | | | | | | | | | | | | | | | | | | | x | | | | | x | | | | | | x | | x | | W | w | | | |
| Stanko & Beckman | 2015 | AMJ | | x | | | | x | | x | x | | | x | | x | x | W | w | | | | | x | | | | x | | x | x | | | x | | x | x | W | w | | | |
| Stern | 1981 | ASQ | | x | | | | | | | | | | x | | x | x | W,w | | | | | | | | | | | | | | | | | | | | | | | |
| Sweeting & Wong | 1997 | JMS | x | | | | x | | | | x | | | | | x | | W,w | | | | | | | | | | | | | | | | | | | | | | | |
| Tosi et al. | 1997 | AMJ | x | | | | | | | | x | | | | | x | x | W | w | | | | | | | | | | | | | | | | | | | | | | | |
| Tosi et al. | 1989 | ASQ | x | | | | | | | | x | | | | | x | x | W | w | | | | | | | | | | | | | | | | | | | | | | | |
| Tosi et al. | 2003 | JMS | x | | | | | | | | x | | | | | x | x | W | w | | | | | | | | | | | | | | | | | | | | | | | |
| Tuggle et al. | 2010 | SMJ | | x | | | | | | | x | | | | | x | | W | w | | | | | | | | | | | | | | | | | | | | | | | |
| Vaast | 2007 | OrgStu | | | | | | | | | | | | | | | | | | | | | | | x | x | | | | | | x | | | | | | W | W,w | | | |
| Visser et al. | 2017 | JMS | | | | | | | | | | | | | | | | | | | | | x | | x | | | | | | x | | x | | | x | x | | W,w | W,w | | |
| Weiss | 2005 | OrgStu | x | | | | | | | x | x | | | | | x | x | W | w | | | | | | | | | | | | | | | | | | | | | | | |
| Welbourne et al. | 1995 | AMJ | x | x | | x | x | | | | x | | | x | | x | | | W,w | | | | | | | | | | | | | | | | | | | | | | | |
| Zajac & Westphal | 1994 | SMJ | x | | | | | | | | x | | | | | x | | W | w | | | | | | | | | | | | | | | | | | | | | | | |

**Table C2. Leading Eight IS Journals Coding (n = 49)**

| | | | NON-IT VEILLANCE | | | | | | | | | | | | | | | | | | | | | | IT-VELLANCE | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | FOCI | | | Goals | | | | | | | | | | | Mechanisms | | ACTORS W=Watchers; w=watched | | | | | | FOCI | | | Goals | | | | | | | | | | | | | Mechanisms | | ACTORS W= Watchers w= watched | | | | | |
| Authors | Year | Journal | BODY | SOUL | COMMITMENT | Documentation | Verification | Prevention/protection | Discovery | Influence/persuasion | Profit | Provision of benefits+ | Self-improvement | Compliance | Entertainment | Hard | Soft | Organizations | Employees | Customers | Other people | Government | BODY | SOUL | COMMITMENT | Documentation | Verification | Prevention/protection | Discovery | Influence/persuasion | Profit | Provision of benefits+ | Self-improvement | Compliance | Entertainment | Hard | Soft | Organizations | Employees | Customers | Other people | Government |
| Alvarez | 2008 | ISJ | | | | | | | | | | | | | | | | | | | | | x | | | | | | | | x | | | | | x | | W | w | | | |
| Ameripour et al. | 2010 | JIT | | | | | | | | | | | | | | | | | | | | | x | | x | | | x | x | x | | | | | x | x | | | | W,w | Ww |
| Anandarajan | 2002 | JMIS | | | | | | | | | | | | | | | | | | | | | x | | | x | | | | | | | | x | x | x | w | | | | |
| Anderson et al. | 2017 | JMIS | | | | | | | | | | | | | | | | | | | | | x | | | | x | x | | | | x | | | | x | W,w | | | | |
| Angst et al. | 2017 | MISQ | | | | | | | | | | | | | | | | | | | | | | x | | | | x | | x | | | | | x | x | W,w | | | | W |
| Astor et al. | 2013 | JMIS | | | | | | | | | | | | | | | | | | | | | x | | | | | | | | x | | x | | | x | | | | W,w | |
| Ayyagari et al. | 2011 | MISQ | | | | | | | | | | | | | | | | | | | | | x | x | | | | | | | | | | x | | x | x | W | w | | | |
| Benaroch & Chernobai | 2017 | MISQ | x | | | | | | | | x | | | | | x | | W | | w | | | | | | | | | | | | | | | | | | | | | | |
| Brynjolfsson et al. | 2016 | MISQ | | | | | | | | | | | | | | | | | | | | | x | x | | x | | | x | | | x | | | | | W | | W,w | | |
| Clemons & Wilson | 2015 | JMIS | | | | | | | | | | | | | | | | | | | | | x | x | | | | | | | x | x | | | | x | x | W | | w | | |
| Crossler & Posey | 2017 | JAIS | | | | | | | | | | | | | | | | | | | | | x | | | | x | | | | | | | | | x | x | W | | | w | |
| Culnan | 1993 | MISQ | x | | | | | | | | x | | | | | x | x | W | | w | | | x | | | | | | | | x | | | | | x | x | W | | w | | |
| D'Arcy et al | 2009 | ISR | | x | | | | x | | | | | | x | | | x | W | w | | | | x | | | | | x | | | | | | x | | | x | W | w | | | |
| Dellarocas | 2005 | ISR | | | | | | | | | | | | | | | | | | | | | x | | | | | | | x | x | | | | x | | W,w | | W,w | | |
| Dinev | 2008 | JSIS | | | | | | | | | | | | | | | | | | | | | x | | | | | x | | | | x | | | | x | x | | | | w | W |
| Doolin | 2004 | ISJ | | | | | | | | | | | | | | | | | | | | | | x | x | | x | | | x | x | | | x | | x | | W | w | | | |
| ElSawy | 1985 | MISQ | | | | | | | | | | | | | | | | | | | | | x | | | | | | | x | x | | | | x | x | W | w | w | | |
| George | 1996 | MISQ | | | | | | | | | | | | | | | | | | | | | x | | | | x | | | | x | | | | x | | W | w | | | |
| Gozman & Currie | 2014 | JIT | | | | | | | | | | | | | | | | | | | | | x | | | | | | | | | | x | | x | | W | w | | | |
| Grant & Higgins | 1991 | ISR | | | | | | | | | | | | | | | | | | | | | x | | | | x | | | | x | | x | x | x | | W | w | | | |
| Karanansios & Allen | 2013 | ISJ | | | | | | | | | | | | | | | | | | | | | x | | | | | x | x | | | x | | | | | x | | | W,w | W |
| Karwatzki et al. | 2017 | EJIS | | | | | | | | | | | | | | | | | | | | | x | x | | | | | | x | x | | | | x | x | W | | w | | |

**Table C2 (Cont.). Leading Eight IS Journals Coding (n = 49)**

| | | | NON-IT VEILLANCE | | | | | | | | | | | | | | | | | | | | | IT-VELLANCE | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | FOCI | | | Goals | | | | | | | | | | | | Mechanisms | | ACTORS W=Watchers; w=watched | | | | | FOCI | | | Goals | | | | | | | | | | | | Mechanisms | | ACTORS W= Watchers w= watched | | | | |
| Authors | Year | Journal | BODY | SOUL | COMMITMENT | Documentation | Verification | Prevention/protection | Discovery | Influence/persuasion | Profit | Provision of benefits+ | Self-improvement | Compliance | Entertainment | Hard | Soft | Organizations | Employees | Customers | Other people | Government | BODY | SOUL | COMMITMENT | Documentation | Verification | Prevention/protection | Discovery | Influence/persuasion | Profit | Provision of benefits+ | Self-improvement | Compliance | Entertainment | Hard | Soft | Organizations | Employees | Customers | Other people | Government |
| Karwatzki et al. | 2017 | JMIS | | | | | | | | | | | | | | | | | | | | | x | x | | | | | | x | x | | | | | x | W | | w | | |
| Khansa et al. | 2017 | JMIS | | | | | | | | | | | | | | | | | | | | | x | | | | | x | | x | | | | | | x | W | w | | | |
| Kim et al. | 2005 | JMIS | | | | | | | | | | | | | | | | | | | | | x | | | | | | | | x | | | | | x | W,w | | | | |
| Kohli et al. | 2004 | MISQ | | | | | | | | | | | | | | | | | | | | | x | x | | x | | | | | | x | | x | | x | x | W | W,w | | | |
| Kordzadeh et al. | 2017 | JAIS | | | | | | | | | | | | | | | | | | | | | x | | | | | | | | x | x | | | | x | W,w | | W,w | | |
| Leclercq-Vandelannoitte et al. | 2014 | EJIS | | | | | | | | | | | | | | | | | | | | | x | | x | | | | | | x | x | x | x | | x | W | w | | | |
| Li et al. | 2015 | JMIS | | | | | | | | | | | | | | | | | | | | | x | | | | x | x | x | | | | | x | | x | W,w | | | w | W |
| Li et al. | 2017 | ISR | | | | | | | | | | | | | | | | | | | | | x | | | | | | | | | x | | | | x | W | | w | | |
| Li, Sarathy et al. | 2014 | ISJ | | | | | | | | | | | | | | | | | | | | | x | | | | | x | | | | | | x | x | x | w | | | | W |
| Lowry et al. | 2017 | JMIS | | | | | | | | | | | | | | | | | | | | | | x | | | | | | | | | | x | | x | W | | w | | W |
| Pavlou et al. | 2002 | JSIS | | | x | | | | | | | | | | | | | | | | | | x | | | | | | | | | | x | | x | | W,w | | | | |
| Sarker | 2005 | JAIS | | | | | | | | | | | | | | | | | | | | | x | | | | | | | | | | | x | | x | W | w | | | |
| Scott & Orlikowski | 2014 | MISQ | | | | | | | | | | | | | | | | | | | | | x | | | | | x | | | x | | | | | x | Ww | | Ww | | |
| Silva & Backhouse | 2003 | JAIS | x | | | | | | | | | | | x | | x | x | W | w | | | | x | | | | | | | | | x | | x | | x | W | w | | | |
| Singh et al. | 2011 | JAIS | | | | | | | | | | | | | | | | | | | | | x | | | | | | | | | x | | | | x | W | | | w | |
| Spiekermann et al. | 2017 | JIT | | | | | | | | | | | | | | | | | | | | | | x | | | | | | | | x | | | | x | W | | w | | |
| Stahl et al. | 2012 | ISJ | | | | | | | | | | | | x | | x | x | W | W,w | | | | | | x | | | | | | | | x | | x | W | W,w | | | |
| Tung & Marsden | 2000 | JMIS | | | | | | | | | | | | | | | | | | | | | x | | | | | | | | x | | | | | x | | w | | | W |
| Twyman et al. | 2014 | JMIS | | | | | | | | | | | | | | | | | | | | | x | | | | | | x | | | | | | | x | W | w | w | w | W |
| Vance et al. | 2013 | JMIS | | | | | | | | | | | | | | | | | | | | | x | | | | | x | | | x | x | | x | | x | W | W,w | | | |
| Vance et al. | 2015 | MISQ | | | | | | | | | | | | | | | | | | | | | x | | | | | x | | | x | x | | x | | x | W | W,w | | | |
| Vieira da Cunha | 2013 | MISQ | | | | | | | | | | | | | | | | W | w | | | | x | | | | | | | x | | | x | | x | | | | | | |
| Wareham et al. | 1998 | ISJ | | | | | | | | | | | | | | | | | | | | | x | x | | | | | | | x | | x | x | x | x | W | w | | | |
| Warkentin et al | 2017 | JAIS | | | | | | | | | | | | | | | | | | | | | x | | | | | | | | x | x | | x | | x | W | | w | | |
| Williams | 1996 | JSIS | | | | | | | | | | | | | | | | | | | | | x | | | | | | | | | | | x | | x | | | | w | W |
| Xu et al. | 2009 | JMIS | | | | | | | | | | | | | | | | | | | | | x | | | | | | | | | x | | x | | x | W | | w | | W |
| Zhang & Venkatesh | 2013 | MISQ | x | | | | | | | x | | x | | | | | x | | W,w | | | | x | | | | | | | x | | x | | | | x | | W,w | | | |

## APPENDIX D. DETAILS OF THEMATIC ANALYSES AND LOGICS OF ACTION NETS

**Table D1. Illustrative Examples of Veillance Goals in IT and non-IT Veillance**

| Goals | Sample Areas of Key Goals | Illustrative Examples |
|---|---|---|
| **Non-IT veillance** | | |
| Profit | • Monitoring of employees by managers to increase performance.<br>• Collection and monetization of customer data.<br>• Corporate governance monitoring.<br>• Peer control of members' contributions. | Arthurs et al. 2008; Bernstein 2012; Beatty & Zajac 1994; Combs et al. 2007; Culnan 1993; Desender et al. 2013; Ouchi & Maguire 1975; Rodríguez et al. 2007 |
| Compliance | • Monitoring of employees by managers/peer control to ensure compliance with organizational goals and culture.<br>• Monitoring of peer organizations.<br>• State monitoring of corporate social responsibility.<br>• Self-monitoring of work by professionals. | Bernstein 2012; Clegg et al. 2012; Dejong & Elfring 2010; Gino et al. 2013; Lazega 2000; Levay & Waks 2009; Ouchi & Maguire 1975; Ouchi 1977; Pierce & Toffel 2013 |
| Influence/ persuasion | • Monitoring to attract resources and knowledge from others.<br>• Disciplinary mechanisms to influence the employee behavior and attitudes. | Mehra et al. 2001; Ruolian et al. 2015 Sasovova et al. 2010; Zhang & Venkatesh 2013 |
| Verification | • Monitoring for verifying job outputs/ state indicators.<br>• Verifying eligibility and fairness of monitoring by employees. | Belot & Schröder 2016; Long et al.2011; Marquis & Qian 2014; Pierce & Toffel 2013 |
| Prevention/ protection | • Monitoring and reporting of accidents.<br>• Self-awareness to reduce risky behavior. | Collinson 1999; D'Arcy et al 2009 |
| **IT veillance** | | |
| Compliance | • IS as tools to instil discipline on the behavior of the watched.<br>• Monitoring to prevent potentially deviant behavior of employees.<br>• Diverse impacts of monitoring on compliance and productivity.<br>• Peer and self-monitoring for compliance. | D'Arcy et al. 2009; Doolin 2004; Pierce et al. 2015; Sewell 1998; Stahl et al. 2012; Vance et al. 2013; Bernstein 2012; Pierce et al. 2015; Lowry et al. 2017 |
| Profit | • New possibilities of IT enable new economic benefits and cost efficiencies.<br>• IT veillance conducted for compliance. | Ayyagari et al. 2011; Pierce et al. 2015; Sewell & Barker 2006; Astor et al. 2013; Karwatzki et al. 2017 a, b; Kim et al. 2005 |
| Provision of benefits | • IT monitoring for attracting and (re)allocating important resources.<br>• Provision of benefits or punishments depend on the compliance revealed by IT.<br>• Disclosure of customer data satisfies multiple parties. | Alvarez 2008; Anderson et al. 2017; Brynjolfsson et al. 2016; Kordzadeh and Warren 2017; Li et al. 2017; Vance et al. 2015; Visser et al. 2017; Xu et al. 2009; Warkentin et al. 2017 |
| Verification | • IT monitoring is enables scrutiny of information by multiple parties (e.g. organizations, customers).<br>• Verification influences the behavior of the monitored agents and leads to their different reactions. | Marsden & Tung 1999; Scott & Orlikowski 2014; George 1996; Niehoff & Moorman 1993; Sarkar and Sriram 2001; Scott & Orlikowski 2014 |
| Influence/ persuasion | • Online monitoring for advantageous network positions.<br>• State monitoring via obligatory reporting through IS.<br>• Customer and expert online reviews influences on organizations. | Doolin 2004; Rizq 2013; Scott & Orlikowski 2014; Zhang & Venkatesh 2013; |
| Prevention/ protection | • Decreasing risks in the areas of information and data management, healthcare, economic efficiency, and security. | Adjerid et al.2016; Angst et al. 2017; Iedema & Rhodes 2010; Staats et al. 2017; |
| Discovery | • Discovering of specificities of the watched not assumed by the watcher. | Ameripour et al. 2010; Iedema & Rhodes 2010; Twyman et al. 2014; |
| Documentation | • Collecting data and profiling employee online and offline behavior and/or location.<br>• Documenting and mining big data generated by crowds. | Anandarajan 2002; Brynjolfsson et al. 2016; Kohli et al. 2004; Marsden & Tung 1999; Natividad 2014; Rizq 2013; Vaast 2007 |

**Table D2. Total Counts for Veillance Goals across Shared and Distinctive Veillance Patterns**

| Veillance type | GOALS: Documentation | Verification | Prevention/ protection | Discovery | Influence/ persuasion | Profit | Provision of benefits | Self-improvement | Compliance | *Total across veillance type* |
|---|---|---|---|---|---|---|---|---|---|---|
| **Shared patterns** | | | | | | | | | | |
| Non-IT veillance | 1 | 7 | 7 | 1 | 8 | 33 | 4 | 4 | 31 | *96* |
| IT veillance | 2 | 10 | 4 | 1 | 5 | 18 | 8 | 4 | 23 | *75* |
| **Distinctive patterns** | | | | | | | | | | |
| Non-IT veillance | 0 | 2 | 0 | 1 | 2 | 2 | 0 | 0 | 1 | *8* |
| IT veillance | 5 | 4 | 7 | 7 | 8 | 12 | 8 | 1 | 14 | *66* |
| *Total cases across goals* | *8* | *23* | *18* | *10* | *23* | *65* | *20* | *9* | *69* | *245* |

**Table D3. Distribution of Veillance Goals across Shared and Distinctive Veillance Patterns**

| Patterns | IT/Non-IT (N) Veillance | Actors: Org | Empl | Cust | Other | Govern-ment | Goals: Documentation | Verification | Prevention/protection | Discovery | Influence/persuasion | Profit | Provision of benefits+ | Self-improvement | Compliance | *Total N of goals per pattern* | *N of papers per pattern* |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **DISTRIBUTION OF GOALS ACROSS SHARED PATTERNS** | | | | | | | | | | | | | | | | | |
| 1 | N | **W** | | **w** | | | | | | | | 1 | | | | *1* | *1* |
| | IT | | | | | | | | | | 2 | 4 | 2 | | 1 | *9* | *6* |
| 2 | N | **W** | **w** | | | | | 5 | 5 | | 2 | 29 | 1 | | 18 | *60* | *36* |
| | IT | | | | | | 2 | 9 | 2 | 1 | 2 | 12 | 3 | 3 | 21 | *55* | *24* |
| 3 | N | | **Ww** | | | | 1 | | | 1 | 5 | 1 | 3 | 4 | 8 | *23* | *15* |
| | IT | | | | | | | | | | 1 | | 1 | | | *2* | *1* |
| 4 | N | | | | **Ww** | | | 1 | | | | | | | 1 | *2* | *2* |
| | IT | | | | | | | | | | | 1 | | 1 | | *2* | *1* |
| 5 | N | | | | **w** | **W** | | | | | | | | | 1 | *1* | *1* |
| | IT | | | | | | | | 1 | | | | 1 | | | *2* | *1* |
| 6 | N | **Ww** | | | | | | 1 | 2 | | 1 | 2 | | | 3 | *9* | *7* |
| | IT | | | | | | | 1 | 1 | | | 1 | 1 | | 1 | *5* | *3* |
| Total N of cases per each goal | | | | | | | *3* | *17* | *11* | *2* | *13* | *51* | *12* | *8* | *54* | ***171*** | ***98*** |
| **DISTRIBUTION OF GOALS ACROSS DISTINCTIVE PATTERNS** | | | | | | | | | | | | | | | | | |
| 1 | N | **Ww** | **Ww** | | | | | 1 | | 1 | 1 | 1 | | | 1 | *5* | *3* |
| 2 | | **W** | **w** | | | **W** | | 1 | | | | 1 | | | | *2* | *1* |
| 1 | IT | **W** | **w** | **w** | | **W** | 1 | | | | 1 | 1 | | | | *3* | 1 |
| 2 | | **W** | **w** | **w** | | | | | | 1 | 1 | 1 | | | 1 | *4* | 2 |
| 3 | | **W** | **Ww** | | | | 3 | | 2 | 1 | 1 | 2 | 2 | 1 | 6 | *18* | 8 |
| 4 | | **W** | | **Ww** | | | 1 | | | 1 | | | 1 | | | *3* | 1 |
| 5 | | **Ww** | | **Ww** | | | | 1 | | | 2 | 3 | 1 | | 1 | *8* | 4 |
| 6 | | **w** | | **W** | | **W** | | | | | | | | | 1 | *1* | 1 |
| 7 | | **W** | | **w** | | **W** | | | | | | | 1 | | | *1* | 1 |
| 8 | | **Ww** | | **w** | | **W** | | 1 | 1 | | | | | | | *2* | 1 |
| 9 | | **W** | **w** | **w** | **w** | **W** | | | | 1 | | | | | | *1* | 1 |
| 10 | | **Ww** | | | **w** | | | 1 | | | | | | | | *1* | 1 |
| 11 | | **W** | | **w** | | | | | | | 1 | 2 | 2 | | | *5* | 3 |
| 12 | | **Ww** | | | **w** | **W** | | 1 | 1 | 1 | | | | | 1 | *4* | 1 |
| 13 | | | **Ww** | **Ww** | | | | | | | | 1 | | | 1 | *2* | 1 |
| 14 | | | **w** | | | **W** | | | | | | 1 | | | 1 | *2* | 1 |
| 15 | | | | | **Ww** | **W** | | | 1 | 1 | | | 1 | | | *3* | 1 |
| 16 | | | | | **Ww** | **Ww** | | | 1 | 1 | 1 | | | | 1 | *4* | 1 |
| 17 | | | | | **w** | **W** | | | 1 | | 1 | 1 | | | 1 | *4* | 1 |
| Total N of cases per each goal | | | | | | | *5* | *6* | *7* | *8* | *9* | *14* | *8* | *1* | *15* | ***73*** | *34* |

**Table D4. Illustrative Examples of Dynamic and Emerging Foci in IT Veillance**

| Study | Original focus of veillance | Emerging focus of veillance |
|---|---|---|
| (Brocklehurst 2001) | VoB: as professionals moved from office to homeworkers management used monitoring electronic diary system that made transparent locations of homeworkers by logging e-mail time and frequencies. | VoC: the workers developed self-disciplining techniques: imposing time zones for work to avoid procrastination, adjusting home space for work, notifying secretaries if leaving home during working time, caring for impression management and visibility to others. |
| (Kohli and Kettinger 2004) | VoB: managers used physicians' profiling system to monitor and benchmark each physician's clinical activities, costs, and outcomes. | VoC: customized IS enabling peer- and self-veillance, visualizing each physician's activities and costs compared to other peers, resulting in closer congruence with management's goals. |
| (Leclercq-Vandelannoitte et al. 2014) | VoB: management using mobile IS to track activities of consultants working away from the office. | VoC: emerging norms of commitment to be constantly engaged, available online, and responsive during work and non-work time. |
| (Mazmanian et al. 2013) | VoB: using email communication devices to monitor the flow of ongoing communication with peers and clients, thus increasing productivity, staying "in the information loop", and choosing whether and when to participate. | VoS: emerging informal culture of continuous engagement; and addiction to email mobile devices during non-work time.<br>VoC: emerging norms of responsiveness and accessibility 24/7; using devices as key components of expressing competency and dedication to their work |
| (Stanko and Beckman 2015) | VoB: monitoring work activities of Navy personnel for securing and productivity. | VoS: emerging need to monitor all personnel nonwork and personal online activities to avoid security issued and maintain attention on work. |
| (Rizq 2013) | VoB: practices of mental health practitioners monitored for efficiency and compliance with required undertaking of measurement and reporting datasets and software. | (elimination of) VoS: increased pressure for intensity of reporting and available medical categories make apparent the dismissing articulation of social, emotional and informal contexts of care among healthcare professionals. |
| (Visser et al. 2018) | VoB: healthcare professionals using personal online health communities to monitor their caring activities for patients with specialized diseases. | VoC: using the IS as a means of displaying own professionalism and commitment to work. |

**Table D5. New Logics of Theorizing about Veillance Systems in the Digital Age**

| Challenged Assumptions | New Logics | Reasoning for IT-enabled Transformations | Implications and Future Research |
|---|---|---|---|
| • Elements of veillance system (actors, goals, mechanisms, and foci) designed for stability and known *a priori*<br>• Veillance actors and roles defined before the act of monitoring<br>• Veillance systems relying on bounded scope and nature of actors and their relationship patterns | **FLEXIBILITY OF VEILLANCE ELEMENTS**<br>• Unbounded, emerging, interactive, and dynamically involved actors<br>• Flexibility enabled by diverse veillance goals and mechanisms that are owned, designed, and implemented by the watchers and intermediates<br>• Dynamically changing and emergent goals and foci of veillance,<br>• Novel areas of monitoring in the body, senses, culture and aspirations of the watched<br>• Inclusion/exclusion of the watchers and intermediate actors is performative to the conceptualizations of the watched and their real-time and future behavior modifications<br>• The watchers and the watched are emerging and flexible net of multiple actors mediated by a variety of IT and intermediate actors | • *IT editability* allows the veillance system and its elements (actors, goals, mechanisms, and foci) to be continuously modified during the process of veillance, even after data have been collected, or when other elements of veillance systems change<br>• *IT distributedness* facilitates cumulative aggregation of data from multiple databases<br>• *IT granularity* enables tailored changes to veillance actors, goals, mechanisms and foci<br>• *IT interactivity* enables multiple interpretations and changes to the veillance elements based on the dynamic set of actors and their evolving goals, available mechanisms and desired foci<br>• *IT reprogrammability* enables adjustments in veillance goals, mechanisms and foci. | **Design of IT veillance systems:**<br>What methods and tools of design for incompleteness might be effective for the design of IT veillance systems with flexible boundaries and elements?<br>Whether and how the primary patterns of the watcher-watched relationships influence how veillance systems evolves?<br>How can compatibility of multiple designs be approached, i.e. how do we theorize and practice inputs from multiple designers with own visions of the veillance system boundaries and characteristics? |
| • Predefined roles of the watcher and the watched<br>• The watchers are individual or coherent group of actors who are central for monitoring<br>• The watched are passive recipients of monitoring who can resist or comply<br>• Clear boundaries between the watcher and the watched* | **DIFFUSED ACTOR ROLES**<br>• Diffused nature of the watchers, e.g. extended variety, networked nature incorporating the intermediate actors and assemblages of human and non-human actants<br>• Diffused nature of the watched, e.g. changing conceptualizations and blurring roles and their active involvement in the veillance process<br>• Complex inter-organizational relationships between the watchers<br>•The boundaries between the watcher and the watched are changeable, ambiguous and subject to networked relationships | • *IT editability* enables evolving set of veillance actors and roles, including intermediate actors<br>• *IT distributedness* facilitates veillance visibility to third-parties and its co-creation by multiple actors<br>• *IT granularity* enables the watched and non-human actants to be engaged in the (co)-construction of veillance mechanisms.<br>• *IT interactivity* enables blurring of the pre-assigned watcher-watched roles.<br>• *IT reprogrammability* enables inclusion/ exclusion of intermediate actors and actants | **Dynamics of IT veillance systems:**<br>What are the dynamics and formation in the distributed nature of the watchers, i.e. how do some watcher(s) engage, orchestrate and manage other heterogenous watchers? How does monitoring assembled from the elements of veillance systems owned by other actors takes place? How do veillance participants design, and manage veillance mechanisms and goals in unbounded veillance system? |

| | | | |
|---|---|---|---|
| • Limited manipulations by the watchers and watched<br>• Manipulations by the watcher to normalize and shape subjectivity the watched<br>• Limited resistance forms (e.g. informal practices) by the watched to manipulate the watchers' gaze | **CUMULATIVE EXTENDED MANIPULATIONS**<br>*Extended manipulative capabilities for the watchers:*<br>• Veillance mechanisms tailored to particular watched<br>• New ways of manipulations of the watched (e.g. predictive bets, non-human oversight)<br>• Possibilities to use veillance systems owned by other actors<br>*Extended manipulative capabilities for the watched*<br>• Both recipients and active manipulators of their visibility<br>• Possibility to engage a variety of intermediate actants and actors to manipulate veillance<br>• Power based on IT expertise in managing their visibility | • *IT editability* enables the watched to be continuously engaged in managing their visibility<br>• *IT distributedness* enables employment of the veillance system owned by others and possibilities for intermediate actors to manipulate the action net of IT veillance<br>• *IT granularity* facilitates unique tailoring and adjustment of veillance mechanisms<br>• *IT interactivity* enables users to activate different IT functions thus enabling empowering and beneficial manipulations<br>• *IT reprogrammability* enables replacing human oversight with IT and new concealed manipulative mechanisms (e.g. hyper-real simulation, data veillance, and real-time behavior modification) | **Functioning of IT veillance systems:** How does the interplay of various actor manipulations impact elements of veillance system? How does the interplay of various actor manipulations impact actor boundaries and roles? How do veillance actors in different roles manipulate veillance systems?<br>**Power:** What is the role of IT expertise and mastering for manipulation? How can veillance system be manipulated without ownership? How can participants opt out of monitoring? How can power be re-conceptualized in IT veillance systems? |
| • Pre-planned behavior and control of the watched are central to efficient monitoring and organizing<br>• Designed monitoring apparatus is attuned to a particular type of veillance system<br>• Changing the focus of veillance would require re-designing the whole system of monitoring<br>• The watched are known through the pre-designed apparatus of veillance with a specific focus | **EMERGENT NON-LINEAR ACTOR RELATIONSHIPS**<br>• Effectiveness depends on an ability mobilize diverse action net participants to create tailored and flexible apparatus (es)<br>• Possibility to dynamically change and combine monitoring apparatuses to produce diverse veillance foci and knowledge of the watched<br>• Inclusion/exclusion of certain watchers or intermediate actors is performative both to the conceptualizations of the watched and their real-time and future behavior modifications<br>• Active role of complex and branched mediating agencies (e.g. both human and non-human actants) that might influence the monitoring<br>• IT expertise in mobilizing and manipulative capacity are sources of power | • IT editability motivates diverse veillance actors to continuously update and re-thing their roles and participation roles and dynamics in IT veillance<br>• *IT distributedness* challenges previously established roles by allowing expansion to unplanned "others"<br>• IT *granularity* enables increased emerging and unpredictable of knowledge veillance actors<br>• As *IT interactivity* contributes to emergent roles by though interplay of compatibilities (or lack of these) across diverse actors<br>• *IT reprogrammability* enables mobilizations of both human and non-human actants and their emergent interplays | **Effectiveness, design, and power:** What particular criteria and sources of effectiveness might be applied to IT veillance systems with emergent and non-linear actor relationships? Do any systematic patterns exist in the emergent dynamics of actor relationships in the action nets of IT veillance? How does inclusion/exclusion of certain actors' changes conceptualizations of the watched and dispositions of other actors and roles?<br>What are the key sources and agents of power in the action net model of IT veillance? |

* questioned in the assemblage model (e.g. Haggerty 2006; Haggerty & Ericson 2000

## ADDITIONAL REFERENCES FROM APPENDICES


Campbell, C., G. Ray, W.A. Muhanna. 2005. Search and Collusion in Electronic Markets Management Science 51(3) 497-507.

Conlon, E. J. and Parks, J. M. (1990). Effects of Monitoring and Tradition on Compensation Arrangements: An Experiment with Principal-Agent Dyads. Academy of Management Journal, 33(3), 603-622.

De Jong, B.A., T.O.M. Elfring. 2010. How Does Trust Affect the Performance of Ongoing Teams? The Mediating Role of Reflexivity, Monitoring, and Effort Academy of Management Journal 53(3) 535-549.

Dencker, J.C. 2009. Relative Bargaining Power, Corporate Restructuring, and Managerial Incentives. Administrative Science Quarterly 54(3) 453-485.

Desender, K.A., R.V. Aguilera, R. Crespi, M. GarcÍa-cestona. 2013. When Does Ownership Matter? Board Characteristics and Behavior. Strategic Management Journal 34(7) 823-842.

Dharwadkar, R., M. Goranova, P. Brandes, R. Khan. 2008. Institutional Ownership and Monitoring Effectiveness: It's Not Just How Much but What Else You Own. Organization Science 19(3) 419-440.

El Sawy, O. 1985. Personal Information Systems for Strategic Scanning in Turbulent Environments: Can the CEO Go On-Line? MIS Quarterly 9(1) 53-60.

Ezzamel, M., H.C. Willmott. 1998. Accounting for Teamwork. Administrative Science Quarterly 43(2) 358-396.

Fineman, S. (1998). Street-level Bureaucrats and the Social Construction of Environmental Control. Organization Studies, 19(6), 953-974.

Finkelstein, S., R.A. D'Aveni. 1994. CEO Duality as a Double-Edged Sword: How Boards of Directors Balance Entrenchment Avoidance and Unity of Command. Academy of Management Journal 37(5) 1079-1108.

Greenblatt, A. 2020. Contact Tracing Apps Aren't Going to Solve the Pandemic Governing.

Greenwood, R., D.L. Deephouse, S.X. Li. 2007. Ownership and Performance of Professional Service Firms. Organization Studies 28(2) 219-238.

Guillaume, Y.R.F., D. Van Knippenberg, F.C. Brodbeck. 2014. Nothing Succeeds Like Moderation: A Social Self-Regulation Perspective on Cultural Dissimilarity and Performance. Academy of Management Journal 57(5) 1284-1308.

He, J., H.C. Wang. 2009. Innovative Knowledge Assets and Economic Performance: The Asymmetric Roles of Incentives and Monitoring Academy of Management Journal 52(5) 919-938.

Huddart, S. (1993). The Effect of a Large Shareholder on Corporate Value. Management Science, 39(11), 1407-1421.

Iedema, R., Flabouris, A., Grant, S., & Jorm, C. (2006). Narrativising Errors of Care: Critical Incident Reporting in Clinical Practice. Social Science and Medicine, 62(1), 134-144.

Jensen, M. (2006). Should We Stay or Should We Go? Accountability, Status Anxiety, and Client Defections. Administrative Science Quarterly, 51(1), 97-128.

Johnson, R.D., G.M. Marakas. 2000. Research report: The role of behavioral modeling in computer skills acquisition - Toward refinement of the model. Information Systems Research 11(4) 402-417.

Khansa, L., Kuem, J., Siponen, M., & Kim, S. S. (2017). To Cyberloaf or Not to Cyberloaf: The Impact of the Announcement of Formal Organizational Controls. Journal of Management Information Systems, 34(1), 141-176. doi:10.1080/07421222.2017.1297173

Kurland, N.B., T.D. Egan. 1999. Telecommuting: Justice and Control in the Virtual Organization Organization Science 10(4) 500-513.

Lane, P. J., Cannella, J. A. A., and Lubatkin, M. H. (1998). Agency Problems as Antecedents to Unrelated Mergers and Diversification: Amihud and Lev Reconsidered. Strategic Management Journal, 19(6), 555-578.

Langfred, C. W. (2004). Too Much of a Good Thing? Negative Effects of High Trust and Individual Autonomy in Self-Managing Teams. Academy of Management Journal, 47(3), 385-399.

Li, H., Sarathy, R., Zhang, J., and Luo, X. (2014). Exploring the Effects of Organizational Justice, Personal Ethics and Sanction on Internet Use Policy Compliance. Information Systems Journal, 24(6), 479-502.

Li, X.B., S. Sarkar. 2013. Class-Restricted Clustering and Microperturbation for Data Privacy. Management Science 59(4) 796–812.
Loughry, M.L., H.L. Tosi. 2008. Performance Implications of Peer Monitoring. Organization Science 19(6) 876-890.
Lowry, P. B., Moody, G. D., & Chatterjee, S. (2017). Using It Design to Prevent Cyberbullying. Journal of Management Information Systems, 34(3), 863-901. doi:10.1080/07421222.2017.1373012.
Milberg, S. J., Smith, H. J., & Burke, S. J. (2000). Information Privacy: Corporate Management and National Regulation. Organization Science, 11(1), 35.
Ogbonna, E., B. Wilkinson. 2003. The False Promise of Organizational Culture Change: A Case Study of Middle Managers in Grocery Retailing. Journal of Management Studies 40(5) 1151-1178.
Pavlou, P.A. 2002. Institution-based trust in interorganizational exchange relationships: the role of online B2B marketplaces on trust formation. The Journal of Strategic Information Systems 11(3–4) 215-243.
Perlow, L. A. (1998). Boundary Control: The Social Ordering of Work and Family Time in a High-Tech Corporation. Administrative Science Quarterly, 43(2), 328-357.
Premeaux, S. F. and Bedeian, A. G. (2003). Breaking the Silence: The Moderating Effects of Self-Monitoring in Predicting Speaking up in the Workplace. Journal of Management Studies, 40(6), 1537-1562.
Rediker, K. J. and Seth, A. (1995). Boards of Directors and Substitution Effects of Alternative Governance Mechanisms. Strategic Management Journal, 16(2), 85-99.
Reuer, J.J., E. Klijn, C.S. Lioukas. 2014. Board Involvement in International Joint Ventures. Strategic Management Journal 35(11) 1626-1644.
Stern, R.N. 1981. Competitive Influences on the Interorganizational Regulation of College Athletics Administrative Science Quarterly 26(1 ) 15-32.
Sweeting, R.C., C.F. Wong. 1997. A UK 'Hands-Off' Venture Capital Firm and the Handling of Post-Investment Investor-Investee Relationships. Journal of Management Studies 34(1 ) 125-152.
Tosi, H. L. and Gomez-Mejia, L. R. (1989). The Decoupling of CEO Pay and Performance: An Agency Theory Perspective. Administrative Science Quarterly, 34(2), 169-189.
Tosi, H.L., A.L. Brownlee, P. Silva, J.P. Katz. 2003. An Empirical Exploration of Decision-Making under Agency Controls and Stewardship Structure Journal of Management Studies 40(8) 2053-2071.
Tosi, H.L., J.P. Katz, L.R. Gomez-Mejia. 1997. Disaggregating the Agency Contract: The Effects of Monitoring, Incentive Alignment, and Term in Office on Agent Decision Making. Academy of Management Journal 40(3) 584-602.
Tuggle, C. S., Sirmon, D. G., Reutzel, C. R., and Bierman, L. (2010). Commanding Board of Director Attention: Investigating How Organizational Performance and CEO Duality Affect Board Members' Attention to Monitoring. Strategic Management Journal, 31(9), 946-968.
Weiss, R.M. 2005. Overcoming Resistance to Surveillance: A Genealogy of the EAP Discourse Organization Studies 26(7) 973-997.
Welbourne, T.M., D.B. Balkin, L.R. Gomez-Mejia. 1995. Gainsharing and Mutual Monitoring: A Combined Agency-Organizational Justice Interpretation. Academy of Management Journal 38(3) 881-899.
Williams, K., C. Haslam, J. Williams. 1992. Ford versus 'Fordism': The Beginning Of Mass Production? Work, Employment & Society 6 517–555.
Zajac, E.J., J.D. Westphal. 1994. The Costs and Benefits of Managerial Incentives and Monitoring in Large U.S. Corporations: When Is More Not Better? Strategic Management Journal 15 121-142.