BEYOND PANOPTIC SURVEILLANCE: ON THE ETHICAL DILEMMAS OF THE CONNECTED WORKPLACE

Research Paper

Tobias Mettler, University of Lausanne, Lausanne, Switzerland, tobias.mettler@unil.ch

Dana Naous, University of Lausanne, Lausanne, Switzerland, dana.naous@unil.ch

Abstract

Technological advances such as the Internet-of-Things, big data, and artificial intelligence have enabled new ways of managerial oversight moving away from panoptic surveillance to what we call "connected surveillance". The COVID-19 pandemic has accelerated the adoption of connected surveillance, which purpose is not only scrutinizing employees' work performance, but also health, personal beliefs, and other private matters. With the implementation of connected workplaces, therefore, various ethical dilemmas arise. We highlight four emerging dilemmas, namely: (1) the good of the individual versus the good of the community, (2) ownership versus information disclosure, (3) justice versus mercy, and (4) truth versus loyalty. We discuss those ethical dilemmas for the case of corporate wellness programs which is frequently being used as guise to introduce connected surveillance. Following a socio-technical perspective, we discuss ethical responses that focus on people involvement and technology assessment. We highlight practical responses that can aim at mitigating the dilemmas.

Keywords: Connected Surveillance, Internet-of-Things, Ethical Dilemmas, Ethics of Technology

1 Introduction

The Covid-19 pandemic has altered many aspects of our daily lives. If we take a positive stance, the crisis has finally pushed and accelerated the adoption of remote work in many branches of economy (Baig et al., 2020), where it was previously considered impossible that employees work from home or that they are not versatile enough to adapt to digitally-enabled ways of working (Kudyba, 2020). As the experience has shown, this challenge has been mastered quite well by many employees in different industry sectors.

Shifting the view from that of a user to that of a supervisor, while still recognizing that supervisors are equally users of technology, coping with the crisis has been even more complicated. Covid-19 exacted a high toll on the psychological health among teleworkers (Schmitt et al., 2021), which is why taking care of the well-being of team members during lockdowns and guaranteeing their safe return to the workplace after the social distancing rules were removed, has required a lot of personal investment and a sensible way to demonstrate digital leadership (Chamakiotis et al., 2021). For those less concerned with employee health and well-being and more concerned with regaining control over the emerging flexibilization of work and digital nomadism (Wang et al., 2020), the last few months have been difficult as well. With the emergence of capitalism, clocking in, counting, weighing, or grading have become accepted practices for organizations to quantify an individual's performance and to exert control (Ball, 2010). Critical questions emerge on how to surveil the home-stranded workforce who is not working at their desks or during regular office hours anymore, and how to control their performance and monitor their activities in times of flexible work arrangements.

According to Olson (2021) the organizational response to these questions is simple: by adopting new work surveillance technology. A large number of private and public institutions –the more positive ones taking health concerns and the more negative ones taking evanescent managerial control as legitimate reason– have ramped up surveillance to contain the spread of the virus as well as to enhance oversight (Urbaczewski and Lee, 2020). As we describe in this paper, the recent adoption of new tools for monitoring and spying on employees entails a *change in the regime of work surveillance*, moving away from visual surveillance relying on human overseers (e.g., shift supervisors, office managers, project managers, chief nurses, prison guards) or computerized surveillance which captures online behavior only (e.g., keystrokes, use of computer time, committed transactions) to a more varied, pervasive, widespread, and connected mode of work surveillance. Key characteristics of these new surveillance technologies are, amongst others, (i) treating the employee's body as a central data source, (ii) extending the locus of surveillance from the online or offline sphere to integrated observation and monitoring, and (iii) using the collected surveillance information for subtle changes of social dynamics (e.g., by means of nudging or gamification). Companies specializing in work surveillance have shifted their attention from mass or group surveillance, to much more personalized behavioral forms of surveillance (Chen and Ross, 2007). For example, the Boston-based company Humanyze integrates information from multiple collaboration tools and smart office sensors (e.g. sociometric badges, which employees have to wear during work time) with the promise to *"drive the desired outcomes*" (Humanyze, 2021). Enaible.io, equally located in Boston, has designed an algorithm that quantifies employees' productivity through a "*multi-dimensional calculation of capacity utilization, consistency and quality impact*" (Enaible.io, 2021).

The question arises whether is this legal? Following the European General Data Protection Regulation (GDPR), organizations are allowed to process personal data –without requiring any explicit consent from their employees– "*for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services […]*" (Art. 9.2 h GDPR). In this sense, under GDPR, an organization may use an employee's health data if the employer can prove that such processing is necessary for improving health and well-being at work. With the Covid-19 such an argumentation seems to be fairly easy. Also, this could be the reason why many organizations prefer to use the term "corporate wellness programs" and not "work surveillance" when implementing technology whose primary purpose is to collect and analyze employees' personal data. According to Grand View Research (2020), the market for corporate wellness is seeing rapid growth and expected to reach USD 93.4 billion by 2028.

We believe that paternalistic or economic motives of organizations will inevitably raise some ethical dilemmas. As Leclercq-Vandelannoitte and Aroles (2020) rightly point out, one must ask whether the end justifies the means? The objective of this paper is to present the differences between the old and the new regime of work surveillance (which we refer to as "*connected surveillance*" in this article). Especially, we highlight ethical dilemmas that may become more prominent with the implementation of connected surveillance; namely: (1) the good of the individual versus the good of the community, (2) ownership versus information disclosure, (3) justice versus mercy, and (4) truth versus loyalty. We provide examples within the specific case of "corporate wellness programs". Following a socio-technical perspective that focuses on technology and people, we contribute through theoretical and practical responses to ethical dilemmas emerging from connected surveillance. From a theoretical perspective, we discuss how people involvement and technology assessment are essential aspects in the implementation of connected surveillance at work. We propose practical advice and explain what an organization can do to respect its employees and address their ethical concerns.

2 Changing from Visual Surveillance to Connected Surveillance

Most historic accounts of work surveillance go back to the emergence of capitalism (Zuboff, 2015). For many organizations work surveillance and the counting, recording, and measurement of their employees' performance is a legitimate means of evaluating their return on investment (Ball, 2010).

As we elaborate in the following sub-sections, a change in the way how work surveillance is happening, that is moving away from human-based oversight and extending locus of control (see Figure 1). This evolution of the work surveillance regime can be described in three stages. First, we discuss the visual surveillance that is mainly associated to the analog sphere with an overseer in traditional work settings. Second, the computerized surveillance corresponds to a shift to office cubicles with desks and computers with data logs and transactions. Finally, the connected surveillance in a cyber-physical sphere involves a plethora of advanced technologies and control mechanisms that change the way of work.

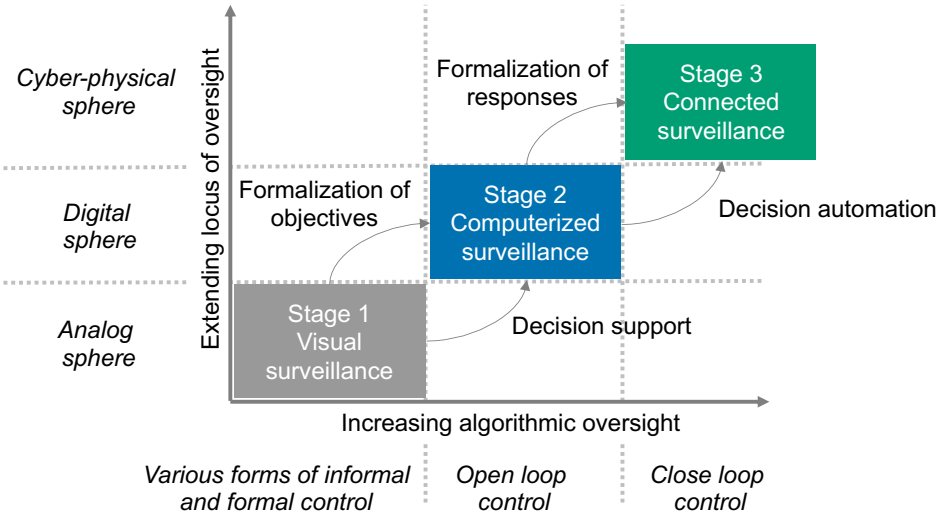

Figure 1. Stage model from visual surveillance to connected surveillance.

2.1 Visual Surveillance

Early forms of work surveillance primarily centered on visual practices (Zureik, 2003), that is overseers using gaze gestures to indicate laborers that their behavior and outcome are under scrutiny. The *power of gaze* has been intensively studied in research (Ball and Wilson, 2000; Willcocks, 2004; De Moya and Pallud, 2020). The most prominent example has been Michel Foucault's (1973) study on how the architectural, "panoptic" design of institutions, like asylums and hospitals, could be arranged so that the overseers' capacity to invigilate and control the behavior of the watched (e.g., employees, prisoners, patients) is optimal, while their visibility is minimal. Although such an architectural arrangement may help to reduce the total number of overseers needed, the most important psycho-social effect still is the possibility that an overseer may pass by physically at some point.

A frequent notion about surveillance and control that is portrayed in the IS literature (in particular the research on IS project management and outsourcing) has therefore been that work performance is most effectively managed and enacted through *agreements, arrangements, and social contracts* (which ultimately require *social contacts* in order to become properly established) (Kirsch et al., 2002; Huang Chua and Myers, 2018). Control, in this regard, refers to actions taken by the overseer for measuring, evaluating, and altering laborers' outcomes and behaviors, mainly through rewards and penalties (Eisenhardt, 1985). Outcome controls are exercised by monitoring compliance of a laborer's products of work with predefined milestones, quality standards, or expected levels of performance (Gallivan, 2001; Soh et al., 2011). Behavior controls, instead, attempt to ensure that a laborer's work process is in line with the desired conduct and behavior at the workplace (Kirsch, 1996). This is done, for example, by construing a laborer's expectations through job descriptions, professional conduct policies, or a code of ethics (Gotterbarn et al., 1999), by mandating the use of project and process methodologies (Maruping et al., 2009), or by organizing meetings, conference calls, and walkthroughs (Choudhury and Sabherwal, 2003). It is important to notice that control must not necessarily be formal, that is,

relying on institutional power to effectively encourage a particular outcome or behavior (Ouchi, 1980). Several studies have found formal controls to be problematic (Lim et al., 2011; Huang Chua and Myers, 2018) or more effective in combination with informal controls (Soh et al., 2011; Remus et al., 2020), which are enacted with minimal reliance on hierarchy, take advantage of common values, philosophy of work, and problem-solving approaches, or which regulate behavior and outcomes based on clan or self-control (Tiwana and Keil, 2009; Keil et al., 2013). To sum, surveillance and control are understood as a mix of formal and informal practices happening mainly in the analog sphere enacted by humans.

2.2 Computerized Surveillance

With work shifting from factory halls to office cubicles, and employees operating most of their time in front of computers instead of workbenches, it has become increasingly difficult for overseers to determine performance through gazing alone. Alongside the introduction of enterprise resource planning systems, many companies in the early 1980s were keen to implement computerized performance monitoring systems (CPMS), which allowed them, for example, to record keyboard strokes, mouse movements, transactions committed, or gave them access to an employee's website and file history. While these systems help supervisors to scrutinize use-related data, they rarely go beyond open loop control and, therefore, lack automatic response mechanisms for admonishing employees who step outside the norm. Nevertheless, this has stimulated a first, major debate on IS ethics (Irving et al., 1986; Mason, 1986; Zuboff, 1988) and led the U.S. Government Office of Technology Assessment (1987) to commission a multi-disciplinary study entitled "*The Electronic Supervisor: New Technologies, New Tensions*". The report revealed that the proportion of laborers under computerized surveillance at that time was approximately 25 to 35 percent. The report concluded that while such systems may, indeed, be beneficial for formalizing and measuring job efficiency and overall productivity, it also comes at the expense of the quality of a laborer's work life. Although the term "technostress" (Ragu-Nathan et al., 2008) was not explicitly mentioned, this report provided initial evidence of the potentially harmful consequences of computerized surveillance due to increased levels of pressure, particularly among under-trained employees, with low job security, or whose wages depend on the measurement scores. Some years later, a study by Grant and Higgins (1991) demonstrated that computerized surveillance does not necessarily result in productivity increases. Hawk (1994) reported somewhat puzzling findings by showing that CPMS do not inevitably lead to more stressful workplaces, but rather negatively affect the perceived evaluation fairness. This is due to the fact that in most instances CPMS require more formalized and standardized ways for evaluating performance and, therefore, are less attuned to contextual or personal circumstances that may explain performance differences between employees. To sum, the emphasis of surveillance and control has shifted from the analog to the digital sphere and become more formalized.

2.3 Connected Surveillance

New advancements in datafication, artificial intelligence, internet-of-thing (IoT) represented by sensor networks, wearables and body implants have created new opportunities for organizations to move beyond measuring the time spent at the workplace by means of time clocks and punch cards or monitoring transactions and what employees do in front of their computer screens during working hours. Today, a smart combination of different technologies, for example, the use of biosensors together with sophisticated algorithmic decision making (as we discuss in section 3.2), allows organizations to shift from tracking behavior in the analog sphere through gazing and other panoptic techniques (visual surveillance) or scrutinizing online behavior through event logs, access history, or screen time (computerized surveillance), to a surveillance mode where real-time behavioral information about both, the digital and the analog sphere can be gathered with the purpose to actively or proactively counter performance losses and to consciously or covertly modify behaviors of employees. In fact, IoT and advanced data analysis techniques enable self-tracking and self-quantifying (Charitsis, 2019). In this sense, the key characteristics of a connected workplace is not

simply the use of more advanced technology for work surveillance. In line with *transhumanist ideals* (Levchuk, 2019), it has led organizations to comprehend an employee's body as additional data source in order to further maximize operations (Mettler and Wulf, 2019).

In practice, this trend manifests itself in two ways. First, inspired by the success of quantified-self practices in the consumer market (Agarwal and Dhar, 2014), organizations have started to adopt a variety of devices (e.g., badges, patches, rings, wrist bands, smartwatches) that link the measurement of body functions (e.g., pulse, sweat, respiration) and behavior (e.g. physical activity, calory intake) with algorithmic decision-making. Different use cases have been proposed to use the employees' health data and to decipher their intimate preferences, everyday routines, subjective well-being, or sentiments towards their employer, for predicting resignations (Fang et al., 2018), work accidents (Sarkar et al., 2019), or job burnout (Dai and Zhu, 2021). Second, fueled by the popularity of electronic fingerprints, hand geometry, face recognition, and other identity access management approaches applied in consumer electronics, more and more companies have started to systematically record certain biometric information about their employees (Ball, 2010). This has progressed up to the point where these data are no longer only used for identity and access control, but also as modern-day punch clocks which register an employee's attendance as well as physical and digital movements (Brooks, 2020), or for operating company devices and equipment as it is possible with the rice grain-sized radio-frequency identification skin implants developed by the Swedish company Epicenter (Rothschild, 2020).

An additional characteristic of connected surveillance tools has been to extend the locus of surveillance beyond the premises of the organization. For example, it has become a common practice to some organizations to check for the whereabouts of their employees, not only during office hours but also when they are off the clock or commuting. With the flexibilization of labor contracts, dissolution of the 9-to-5 workday, and emergence of digital nomadism (Wang et al., 2020), it has certainly become harder to set a clear line between work and leisure time. Moreover, on-site visual, or remote computerized surveillance relying on human overseers has also become impractical, which is why more and more organizations seek to supplant human with algorithmic oversight using sensor networks, wearable devices, or body implants combined with data tracking algorithms.

Therefore, trying to move away from pure human judgment or computerized decision support to more automated decision making and execution, where machine learning algorithms not only rule about the next steps to initiate but also directly communicate formalized resolution strategies to employees (Bader and Kaiser, 2019; Gal et al., 2020; Lindebaum et al., 2020), can be considered another key characteristic of connected surveillance. The goal is to implement closed loop control that not only captures performance information (as with computerized surveillance) but also initiates specific actions to solve the identified problems. Companies, as the above-mentioned Humanyze, have developed devices that use speech recognition and sentiment analysis which should enable employers to examine how and in what tone employees talk to one another, or how long and with whom they share their coffee or lunch breaks. Similarly, Walmart has patented a system named "*Listening to the frontend*" (Jones et al., 2017), which monitors and filters specific noises (e.g., the beeps of item scanners or the rustling of bags) for recording and analyzing the conversations between employees and customers. While it is not transparent what these companies will do with all these data, much pointing to the direction that companies are starting to develop an interest to experiment with paternalistic approaches, such as nudging or gamification, in order to trigger modifications of attitudes, perceptions, motivations, and actions (Pellegrini and Scandura, 2008; Feng et al., 2019). To sum, connected surveillance can be understood as ensemble of technologies which are not bound to collecting information about performance, behavior, or other work-related matters (Ball, 2010) as the preceding computerized surveillance tools. These technologies extend the locus of surveillance to new data sources (i.e., health data of employees), new places (i.e., whereabouts outside the office building or office hours), as well as make use of machine learning in combination with behavioral strategies, such as nudging, gamification, and others to pressure, persuade, or seduce employees to behave in a manner as the organization desires.

3 Emerging Ethical Problems from Connected Surveillance

3.1 IS Ethics in the Context of Work

Since its beginnings, the IS field has dealt, albeit with varying emphasis (Myers, 2021), with the bright and the dark side of information technology. Besides providing strong evidence concerning the numerous positive aspects that IS has provided us with, a number of scholars have been troubled by the question if the adoption and use of technology jeopardizes some of our fundamental rights and liberties (Mason, 1986; Laudon, 1995; Walsham, 1996). Different terms, such as "ethical dilemmas", "ethical issues" or "ethical trade-offs" have been used over the years to refer to situations in which, on *moral grounds*, individuals, or organizations ought to sacrifice something to obtain something else. There are two implications from this: (i) there is a *choice* to do or not to do something, and (ii) a certain action or the omission of it are related to morals which can be understood as "*the conformity to socially accepted standards of conduct*" (Myers and Miller, 1996). But what is perceived to be socially acceptable for one person, may be seen as ethical problem by someone else, and for yet another one, to be a practical problem, and for yet another one, to be a political problem (O'Neill and Hern, 1991). Studies have also shown that there are cultural differences in the perception of what is ethical and moral (Davison et al., 2009). Consequently, we do not emphasize the boundaries between morals and ethics (Myers and Miller, 1996), or how to name the underlying issue. Rather, we highlight two concerns, which are particular to the context of work.

First, the question of choice is a delicate one. While no one is forced to use abusive social media or e-commerce websites –although the decision of dropping out might cause a lot of individual compromises (Kim et al., 2020)– choice is limited in the case under study. Most people are in the situation of having to work for a living. Due to disadvantageous circumstances in life, for some individuals the choice options for whom to work are even more limited. Quitting a job because one may disagree with the way the employer surveils one's work is something not everyone can afford. Especially, workers in low income sectors or the gig economy are suffering from harsh surveillance practices (Gurley, 2021). More recently, the Covid-19 pandemic has intensified this problem, requiring workers to disclose their vaccination status, for example, or potentially losing their jobs (e.g., in the aviation industry). The point here is that the matter of *choice* mostly applies to employers. Therefore, the responses to the identified emerging ethical problems (see section 4) will be formulated from an employer's perspective.

Second, what is a socially accepted conduct at work may depend on the organizational values, industry standards, and professional code of ethics (Pearson et al., 1996). Hence, not only an individual's different moral conception may lead to a different perception of what is ethically problematic, but also the social norms which are shared and defined by various groups. The range of possible ethical problems which can be raised is, therefore, infinite. Thus, we highlight only several recurring dilemmas which are often treated in the IS ethics literature:

The good of the individual versus the good of the community: This issue has been discussed from different lenses, such as for example the enforcement of the use of standards by individual software providers so that systems become interoperable (Anderson et al., 2017), or the implementation of piracy/copyright protection so that software developers are rewarded for their efforts and new software continues to be released on the market (Cheng et al., 1997). The same rationale is applied in the context of work surveillance, where excessive data collection practices violate employees' privacy with the justification of the public interest of preventing major accidents or improving community health with the purpose to minimize the (financial and social) burden for society. Certain professions and sectors, hence, may be more prone to ethical infringements than others (e.g., air traffic controllers, pilots, firefighters, bus drivers, operators of nuclear reactors).

Ownership versus information disclosure: Many studies in IS have emphasized the delicate balance between disclosing/non-disclosing information, and the complex interrelation of individual/organizational ownership and possession of information (Constant et al., 1994; Mettler and

Winter, 2016). A good example for this dilemma is the case of *Loomis versus the State of Wisconsin*, more widely known as the COMPAS case (California Courts, 2016). There, the question was investigated as to whether intellectual property rights of companies should be valued more highly than public transparency (respectively whether citizens who are subject of algorithmic decision-making by the state have the right to access the code of the proprietary third-party software, which is used, amongst others, for processing their personal data). To a similar extent, the *Arias v. Intermex Wire Transfer* case dealt with the question whether employers have the right to track their employees outside working hours when they use company property such as work phones, notebooks, etc. (U.S. Courts Opinions, 2015). Although accentuating different aspects, these two cases illustrate nicely what Mason (1986) referred to as the PAPA issues, that is *privacy* (what things can people and organizations keep to themselves and not be forced to reveal to others?), *accuracy* (who is responsible for the authenticity, fidelity and accuracy of information?), *property* (who owns information?) and *accessibility* (what information does a person or an organization have a right or a privilege to obtain, under what conditions and with what safeguards?). It is, however, important not to make the mistake of confounding lawfulness and ethics here. As we mention above, under GDPR, companies are allowed to process employees' health data that is collected for example with wristbands, smart watches or smart rings offered as part of corporate wellness programs or workplace safety initiatives. The question is rather, is this behavior ethically justified? This brings us to the next ethical dilemma.

Justice versus mercy: Another fundamental ethical dilemma revolves around the trade-off of doing what is right (or lawful) as to doing what seems to be emotionally compelling and feels right (Kidder, 1995). With regard to the former, the IS ethics literature often refers to the concept of *organizational justice,* which can be understood as the perception of fair treatment from a source or focal entity in a relationship (Li et al., 2014; Mirchandani and Lederer, 2014). Organizational justice can further be subdivided into *systemic justice* (perception of overall fairness), *distributive justice* (perception of fairness of outcomes in comparison to the outcomes of others), *interpersonal justice* (perception of fairness of the manner in which outcomes are administered), *informational justice* (perception of fairness of information or knowledge received about procedures), and *procedural justice* (perception of fairness of policies and processes contributing to outcomes). The concept of mercy is less well articulated in the IS literature, but in essence relates to situations where exception handling feels appropriate or compelling. For example, should managers treat employees with disabilities different than their co-workers in order to facilitate their integration? Is it justified that managers are not subjected to work surveillance to the same extent as regular employees? As pointed out by Smith (2002), possible ethical problems emerge when company standards and rules contain contradictory principles (that is when they tell you to do two different things) or when the professional code of ethics is in conflict with one's own moral compass. Therefore, some authors raise the question whether there are higher and lower order obligations, and if the lower order obligations can be trumped.

Truth versus loyalty: As consequence of the above-mentioned dilemma, employees and employers alike may face situations in which they need to decide whether to remain true to themselves or to maintain loyalty to a person, organization, or the general standards of a profession (Kidder, 1995). For example, studies have shown that in certain branches (e.g., law, medicine, education) the pursuit of a second opinion may be perceived as a breach of loyalty in the client-provider relationship and result in the uncomfortable task of balancing professional courtesy (i.e., not discrediting a colleague's judgement) against one's professional opinion of the situation (i.e., what one thinks is the true response). In the work context, the weighing up of individual morals and values against organizational and professional norms is strongly biased by issues of dependency, intimacy, and trust relations (Simbeck, 2019). As mentioned above, employees with good market prospects may resolve this dilemma differently than employees with economic hardships, living in remote areas, or low qualifications.

3.2 Connected Surveillance under the Guise of Corporate Wellness

Corporate wellness programs (CWP) are health initiatives at the workplace that are designed to improve the physical and mental health of employees and prevent occupational diseases (Ajunwa et al., 2016; Kelly and Snow, 2019). Studies show that well-designed CWP can improve employees' fitness levels and mood, which can reduce healthcare costs, job stress and absenteeism (Giddens et al., 2017; Kelly and Snow, 2019). Ultimately, CWP are said to improve employees' quality of life, work performance and productivity (Souza et al., 2017). However, CWP can be considered as a particular class of work surveillance as it requires employees to share health data, wear specific monitoring devices, or even implants. With the rapid development of ubiquitous IoT devices, many organizations are relying on the use of wearables within their CWP to monitor employees and collect data related to health, fitness, location, emotion and sleep patterns (Giddens et al., 2017; Manokha, 2020). Wearables are equipped with multiple sensors –such as accelerometers, heart rate sensors, geolocation sensors, thermometers– that allow continuous collection of data about the employee's body and the environment (Souza et al., 2017). Wearables can provide information or hidden insights about the employee based on fine-grained data on interaction patterns, speaking patterns, movements or locations (Gaur et al., 2019). Fitbit Care is one example of health platforms that rely on wearable technology to support CWP. It provides comprehensive offerings that include self-tracking tools and digital interventions such as challenges, social groups, and guided workouts as part of a corporate health and workplace wellness plan (Charitsis, 2019). With COVID-19, special IoT initiatives have been designed to assist companies in "going back to normal" (Chamola et al., 2020). Fitbit Care Ready for Work is one solution proposed for COVID-19 impact management to help employees returning to the workplace through measuring key health metrics.

Although legal frameworks govern the processing of personal data in general (such as Europe's GDPR that points out some specific vulnerabilities and potential liabilities), there is a lack of ethical guidelines that help organizations to cope with the risks associated to the use of CWP (Tursunbayeva et al., 2021). In specific, how organizations can deal with implications of monitoring employees at work including *choice, privacy, discrimination, and control*. These are critical aspects to be considered when discussing the ethical dilemmas (as presented in section 3.1).

When it comes to the first dilemma *–the good of the individual versus the good of the community–* CWP raise questions on the power relationship between the employer and employees. While the participation in CWP is voluntary in most cases, there are organizations that impose mandatory participation in such programs (Ajunwa et al., 2016). As a result, the employee's choice to opt out and share information is jeopardized. For example, if the company can get more favorable health insurance or work accident insurance through sharing employees' data with the insurer, participation in CWP becomes a critical aspect to increase the greater good for the community and resolve the principal-agent issue through allowing the insurers to know their customers by data. However, this becomes problematic when companies do not profit from any decrease in cost, respectively the cost reduction is not shared with employees.

The second dilemma *–ownership versus information disclosure–* also stems from the privacy implications associated to employee monitoring at the workplace. When it comes to information disclosure, Dinev and Hart (2006) theorize that individual behavior depends on a rational process that weighs benefits over privacy risks for decision-making. This is also governed by individual trust in the medium of sharing for information disclosure. In the context of CWP, privacy risks exist due to tracking and surveillance of employees. Manokha (2020) explains that the data collected by employers include information on employee aptitudes, health, psychological state, and locations, which threatens the privacy and autonomy of the individual due to their sensitive nature and the possibility to extrapolate knowledge about the employee. For example, inferring employee attitudes and preferences and more critically which employees might develop serious illnesses or which female workers might get pregnant (Ajunwa et al., 2016). All this information can have an influence on the employer's fair treatment, and thus, the employee's career development. Therefore, the right of the employee to agree/disagree to share certain data from selected locations when participating in CWP is questioned

(Gaur et al., 2019). Whether the program is voluntary or not, the temporal and spatial aspects of the data shared should be discussed. While it is difficult to avoid information sharing from private life when participating in a fitness challenge that uses a smartwatch or smart jewelry that accompany employees in their everyday activities, the safeguards put in place for managing employee's data in terms of confidentiality and anonymity are very important. More specifically, how the employer addresses Mason's (1986) PAPA issues in the design of the CWP is critical. In addition to the privacy issue, accuracy is another critical aspect. While connected surveillance relies on large amounts of data to recommend actions, the process is not considered free of bias (Gal et al., 2017). Thus, the accuracy of the data collected by IoT devices, and algorithms applied to this data are of major concern. Errors or misinterpretations of the data can influence the decision-making process, which can affect the employee's behavior and the employer's judgement as well. For example, initiatives for stress detection at work heavily rely on the accuracy of data collected from physiolytics (Mettler and Wulf, 2019), and malfunctioning of the sensors collecting this data or in the algorithms analyzing this data can lead to false positives and wrong recommendations in the stress management program.

For the third dilemma *–justice versus mercy–* we must take into consideration how the data collected through IoT within CWP has the potential to result in discrimination acts (Ajunwa et al., 2016). Manokha (2020) explains that discrimination is an issue that overlaps with privacy concerns related to CWP. Employers collect data on employee's health and activities, which can result in potential discrimination with respect to promotions and bonuses based on the analyzed data and predictions on performance. From another perspective, self-tracking tools can lead to discrimination between people who can produce good data and those who cannot, including less performant employees, chronically ill or poor (Charitsis, 2019). In addition, Tursunbayeva et al. (2021) emphasize how people analytics may result with inconvenience and income insecurity to employees, especially in the category of "gig" workforce. For instance, Uber drivers that deviate from the company's algorithms could be penalized or banned from the platform. Organizational justice with all its subcategories come into play within this type of dilemma, where fairness of information, procedure and outcomes become essential topics. While connected surveillance relies on algorithms, designed algorithms can encode implicit biases and deep-learning algorithms can detect patterns in existing data which could also be based on biased decisions (Gal et al., 2017). Therefore, mitigating bias within algorithms is a critical requirement when discussing this dilemma. This however requires human oversight of unfair decisions taken by AI to accommodate exceptions in the system. However, how unfair decisions are detected and judged remains a question of perspective.

The fourth dilemma *–truth versus loyalty–* relates to the concept of faithfulness and passion. Participation in CWP is based on free consent, however within the employer-employee relationship it might be difficult to oppose organizational decisions or opt out when desired. This is especially the case for certain occupations that require health monitoring for occupational safety and health. For example, police officers or pilots have obligations towards their jobs that do not give them the privilege of choice. Although they might be against the use of surveillance systems in truth, their loyalty to and passion for their job plays an important role. Also, the under-privileged workers in positions that do not require high qualifications and who can be replaced within the organization are another category of employees that face the same dilemma. CWP increase pressure on employees to be productive, perform better and beat targets. In addition, CWP often comprise "nudges", a principle from behavioral economics and persuasive psychology, to encourage the achievement of goals for the individual, team or organization (Tursunbayeva et al., 2021). For example, CWP that target physical well-being at work aim to improve employee's health through reminder messages to move more or drink more water, in addition to tips to eat healthier food or better sleep habits. Such behavior shaping and control practices within the workplace raise questions on the faith of the employer into their employees as they operate with hidden manipulations as opposed to straightforward communication.

4 Response to Ethical Dilemmas

4.1 A Socio-technical View of Technology Ethics

In light of the existing ethical dilemmas, organizations that aim at introducing connected surveillance at work have many challenges and different ethical considerations to address. This is mainly the purpose of technology ethics. Technology ethics is one branch of applied ethics that is concerned with the moral design and use of technology (Bock et al., 2021). This is the basis of technological mediation that concerns the role of technology in human action and experience. Verbeek (2006) explains that, on the one hand, technologies shape behaviors and actions of users, they have an intended purpose and can prescribe actions. On the other hand, ethics addresses the question of *how to act?*

As a response to the ethical dilemmas, the organization should be able to justify the design choices and use contexts of the implemented initiatives for connected surveillance. Given that connected surveillance represent a socio-technical system, there is a need to take a dual focus, that is on the people and technical artifacts, to discuss ethical remedies.

Considering the former, that is the human element, the organization needs to address the concerns of its employees seriously. Therefore, existing ethical frameworks suggest the involvement of users in the decisions regarding the introduction of new technologies and their use (Ajunwa et al., 2016; Tursunbayeva et al., 2021) in order to provide *a real choice*. Ajunwa et al. (2016) highlight that the voluntariness of participation and the value of the testing being offered are important to obtain employees' consent. In addition, they emphasize that the discussion about potential risks of monitoring is as important as the communication of the potential benefits. In general, it is a matter of transparency that can be the game changer (Tursunbayeva et al., 2021). Obtaining employees' opinions can highlight critical concerns and potential dilemmas that the management did not consider. Therefore, allowing this exchange and safe space for employees to discuss corporate ethics can "maximize transparency and minimize the dangers of whistle blowing" (Tursunbayeva et al., 2021). Assasi et al. (2014) highlight the importance of participatory approaches where stakeholders are involved in a bottom-up process of technology evaluation and decision-making. They emphasize that, with this approach, practitioners and ethicists can provide scientific and theoretical inputs to assist stakeholders in reaching consensus on certain ethical conflicts or concerns.

The latter, that is the artifacts, should be subject to *constructive technology assessments*. Unlike traditional technology assessment that only examines the implications of new technologies for quantifiable risks (Kiran et al., 2015), constructive technology assessments emphasize the importance of assessing the ethical and social implications of emerging technologies while it is still in development. This requires analyzing the complex dynamics of the technology development and integrating assessments from different stakeholders as feedback into the design process (Verbeek, 2006). In the context of the connected surveillance in the workplace, constructive technology assessment should be performed prior to the implementation or design of any initiative that can affect the actions and experience of the employees. Like designers, employers here share the responsibility of integrating technology ethics into their platforms and tools. Accordingly, ethical frameworks should govern the design and use of IoT technology that enables employee monitoring and tracking within the workplace. This entails assessing the data management practices within the organization including collection, storage, and analysis of employee data, which also involves the knowledge generated based on the analytics performed. For that, the constructive technology assessments should especially focus on *privacy* and potentials for bias or *discrimination*. It is important that the organization is transparent with respect to the data practices within the organization (Ajunwa et al., 2016). Specifically what steps are considered for data security and privacy. Giber (2016) discusses the ethical concerns that need to be considered when managing and processing big data resulting from advanced technologies such as IoT. Mainly, related concerns address a clear communication of the safeguards and measures taken to preserve data confidentiality, availability, accessibility, and quality. It is also important to transparently communicate for what purposes the data is being used and potential risks. The

processing of data should be completely transparent to users to avoid any potential misunderstanding or conflicts. This also involves information about the algorithms used. It goes without saying that data needs to be managed properly to prevent misuse and malicious use, and each action should be recorded for complete transparency (Wang and Siau, 2018). However, it is also important to have a proper debate on what data should be recorded and who can have access to these records. In fact, Mayer et al. (2021) highlight that there is a need for an ethical discussion on data processing. According to Feuerriegel et al. (2020), this helps to quantify bias and mitigate the discrimination against marginalized groups.

Finally, considering the behavior-steering nature of technology, especially in the case of connected surveillance, behavioral *control* becomes a key topic. This suggests incorporating ethical frameworks that address the issue of paternalistic manipulation, such as nudging (Lembcke et al., 2019). The main questions to be addressed are whether the nudge (1) preserves the individual's autonomy or freedom of choice (i.e., the employee is free to act in accordance to this nudge or ignore it), (2) is transparent in existence and form (i.e., the employee is aware that it exists and in which form it will occur), and (3) can be justified (i.e., the purpose is clear and aligned with the employee's needs and preferences) (Lembcke et al., 2019). However, the challenge remains to create interventions that fit all individual preferences because what might be appropriate behavior to some individuals can be seen differently by others. For companies justifying their actions by a utilitarian ethical model, actions are considered right if they produce the greatest amount of happiness to the greatest amount of people (Mill, 2001). In that sense, minority becomes collateral damage to the greater good. This is in line with the Rawlsian model which aims to minimize injustice through fair treatment and applicable standards and rules (Rawls, 2005). Pragmatic ethics (Dewey, 1983), on the other hand, is based on the assumption that efficacy of action determines rightness. The main outcome is a more intelligible, controllable, and orderly world where concepts are developed in a relation to a particular need or task. In this model, ethicality requires continual revision and empirical validation through user studies to ensure utmost accuracy, thus also referring to participatory design. In parallel, the ethics of care (Gilligan, 1993) complements the Rawlsian model through viewing dilemmas in their specific context and accommodating exceptions rather than the decontextualization in the ethics of justice. Based on these frameworks, Fox and Reece (2012) suggest a selection of criteria for an ethical framework for information organization including ethics of justice, ethics of care and pragmatism where outcomes must be regularly monitored and maintained through iterative feedback and testing with stakeholders.

4.2 Practical Responses to Ethical Dilemmas

We highlight in the previous section theoretical and ethical responses required to manage ethical dilemmas emerging from connected surveillance in the workplace. Below we address these dilemmas through practical responses that organizations can follow if they wish to mitigate ethical concerns prior to implementation of connected surveillance.

From a practice perspective, legal compliance is a building block for successful digitalization projects (Tursunbayeva et al., 2021). Although the technology is evolving rapidly and legislations might take some time to catch-up speed, the law provides fundamental guidelines that can help organizations adhere to certain standards that fit the current context or situation. However, as mentioned above, we need to be aware that "legal" does not necessarily mean "ethical", but it is a first step into ensuring legal responsibilities and accountability in case of conflicts rising from ethical dilemmas. In that regard, GDPR outlines roles and responsibilities for the entities involved in the collection, storage, and processing of personal data, which should be applied to the context of the connected workplace. This would ensure governance within the organization when it comes to managing technology and people, among those roles are (1) the controller who determines the purposes and means of processing data (in the work context, the employer), (2) the processor who processes personal data on behalf of the controller (in the work context, service providers of IoT technology), and (3) data protection officer who has expert knowledge of data protection laws and practices and guarantees the organization's legal compliance. Tursunbayeva et al. (2021) also emphasize that new organizational roles associated

to data management, such as Chief Data Officer and Chief Privacy Officer, are necessary to protect employees' privacy and avoid ethical conflicts. In addition, with the use of AI, Gal et al. (2017) suggest that an "algorithmist" role becomes increasingly important as auditors of probabilistic algorithms to avoid biases and systematic unfairness.

In terms of technology design, the "Privacy by Design" (PbD) concept also emerge as "the philosophy and approach of embedding privacy into the design specifications of various technologies" (Cavoukian, 2009). This means that system designers and those who decide to implement specific designs (e.g., employers) should have privacy principles governing the design of platforms and tools to be used in the organization. The requirements of data protection must be considered at the very start of technology design. GDPR has imposed principles relating to the processing of personal data including: lawful, fair, and transparent processing, purpose limitation, data minimization, accuracy, storage limitation, integrity, confidentiality, and accountability. All these principles should be realized using dedicated safeguards that preserve data privacy. However, each company selects their most convenient technology realization, which creates challenges for ethically justifying each choice. For instance, which devices are used? where will the data be stored? or which service providers will be involved? Based on article 35 of the GDPR: *"Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data".* Thus, a privacy impact assessment (referred to as Data Protection Impact Assessment in GDPR) should be conducted to identify and reduce the risks of harm to individuals (Wagner and Boiten, 2018). This type of assessment allows to measure compliance to legislation, identify and reduce privacy risks and demonstrate accountability. In the context of connected surveillance, privacy impact assessment should include justification of the purpose for processing employee data and sharing with external parties, an assessment of the risks and employee rights in light of the data processing, and the necessary safeguards implemented. Accordingly, these measures can be considered pre-requisites for the ethical evaluation of the system implemented, as they mainly address issues of privacy, fairness, and accountability. As for the people aspect, practical responses are embodied in user-oriented approaches to the design of the intended initiatives or what we refer to as participatory design, for example, in ideation workshops, testing and feedback. While employees might be intimidated to share the truthful feedback or opinions with their employers in an open space discussion, anonymous participation can be supported. For instance, employers can create a space for sharing ideas and thoughts anonymously through a letter box or a forum, which can be a practical tool for ethical dilemmas reporting.

5 Conclusion

Under the guise of corporate wellness programs and post COVID-19 "going back to normal" initiatives, we have seen organizations moving away from panoptic surveillance to what we call connected surveillance. We present a model of work surveillance that highlights an evolution from formal or informal mechanisms to a closed loop control through the shift from an analog sphere to a cyber-physical sphere that entails the analog and digital world. We explain the characteristics of each stage and how the notion of surveillance and control evolves according to the environment and available technology.

Although employers promote the use of technology in the workplace for benevolent purposes, the other side of the coin can entail malicious or unethical practices. This raises ethical dilemmas that need to be taken into consideration for successful and fair use. In this paper, we address these dilemmas and highlight how technology ethics can provide guidelines for organizations in response to ethical dilemmas by addressing the two dimensions of people and the technology artifact. People's participation and technology assessment can support organizations to address ethical considerations regarding the good of the individual and the community, data ownership and disclosure of information, justice and exception handling, and finally truth about oneself.

In addition, we discuss some practical responses that are foreseen by existing legal frameworks. Although legal does not mean ethical, these responses can be considered a starting point for the ethical analysis of the technology mediation at the workplace. In this context, privacy impact assessment is proposed by law as one tool to ponder about privacy risks associated to excessive data processing. Yet, such assessments have been criticized for being highly subjective (Wagner and Boiten, 2018). Therefore, we see an avenue for future research in improving the methodology of how privacy assessments are conducted, as well as developing hands-on tools that allow organizations to conduct more objective assessments of the privacy risks associated to connected surveillance.

We recognize limitations in this paper with regards to addressing other ethical issues that might be relevant to the scenario of connected surveillance (e.g., chilling effect, repurposing, trustworthiness, etc.). However, we focus our discussion on most recurring ethical dilemmas in IS ethics literature and dig deeper into these issues with the concrete example of corporate wellness programs. Also, while COVID-19 accelerated the shift towards connected surveillance, we must emphasize that this trend has been already in place before due to the continuous development of sensor technologies and IoT devices for instance in facility and space management. However, the convenient use of this technology within the flexible work policies due to the pandemic has been the center of attention for developing solutions towards "going back to normal".

Acknowledgments

This research has been conducted within the Swiss National Research Programme (NRP77) on "Digital Transformation" and received funding from the Swiss National Science Foundation (grant no. 187429).

References

Agarwal, R. and Dhar, V. (2014). "Big data, data science, and analytics: The opportunity and challenge for IS research." *Information Systems Research* 25 (3), 443-448.

Ajunwa, I., Crawford, K. and Ford, J. S. (2016). "Health and big data: An ethical framework for health information collection by corporate wellness programs." *The Journal of Law, Medicine & Ethics* 44 (3), 474-480.

Anderson, C., Baskerville, R. L. and Kaul, M. (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.

Assasi, N., Schwartz, L., Tarride, J.-E., Campbell, K. and Goeree, R. (2014). "Methodological guidance documents for evaluation of ethical considerations in health technology assessment: A systematic review." *Expert Review of Pharmacoeconomics & Outcomes Research* 14 (2), 203-220.

Bader, V. and Kaiser, S. (2019). "Algorithmic decision-making? The user interface and its role for human involvement in decisions supported by artificial intelligence." *Organization* 26 (5), 655-672.

Baig, A., Hall, B., Jenkins, P., Lamarre, E. and McCarthy, B. (2020). *The COVID-19 recovery will be digital: A plan for the first 90 days.* McKinsey & Company.

Ball, K. (2010). "Workplace surveillance: An overview." *Labor History* 51 (1), 87-106.

Ball, K. and Wilson, D. C. (2000). "Power, control and computer-based performance monitoring: repertoires, resistance and subjectivities." *Organization Studies* 21 (3), 539-565.

Bock, A., España, S., Gulden, J., Jahn, K., Nweke, L. O. and Richter, A. (2021). "The Ethics of information systems: The present state of the discussion and avenues for future work," in: *Proceedings of the 2021 European Conference on Information Systems*. Marrakech, Morocco.

Brooks, C. (2020). *The biometric time and attendance system laws you should know*. https://www.businessnewsdaily.com/15104-biometric-time-attendance-system-laws.html (visited on November 12, 2021).

California Courts (2016). *State v. Loomis*. https://www.courts.ca.gov/documents/BTB24-2L-3.pdf (visited November 12, 2021).
Cavoukian, A. (2009). "Privacy by design: The 7 foundational principles." *Information and Privacy Commissioner of Ontario, Canada*.
Chamakiotis, P., Panteli, N. and Davison, R. M. (2021). "Reimagining e-leadership for reconfigured virtual teams due to Covid-19." *International Journal of Information Management* 60, 102381.
Chamola, V., Hassija, V., Gupta, V. and Guizani, M. (2020). "A comprehensive review of the COVID-19 pandemic and the role of IoT, Drones, AI, Blockchain, and 5G in managing its impact." *IEEE Access* 8, 90225-90265.
Charitsis, V. (2019). "Survival of the (data) fit: Self-surveillance, corporate wellness, and the platformization of healthcare." *Surveillance & Society* 17 (1/2), 139-144.
Chen, J. V. and Ross, W. H. (2007). "Individual differences and electronic monitoring at work." *Information, Communication & Society* 10 (4), 488-505.
Cheng, H. K., Sims, R. R. and Teegen, H. (1997). "To purchase or to pirate software: An empirical study." *Journal of Management Information Systems* 13 (4), 49-60.
Choudhury, V. and Sabherwal, R. (2003). "Portfolios of control in outsourced software development projects." *Information Systems Research* 14 (3), 291-314.
Constant, D., Kiesler, S. and Sproull, L. (1994). "What's mine is ours, or is it? A study of attitudes about information sharing." *Information Systems Research* 5 (4), 400-421.
Dai, W. and Zhu, Z. (2021). "Employee resignation prediction model based on machine learning," in: *Proceedings of the 2020 International Conference on Applications and Techniques in Cyber Intelligence*. Huainan, China. 367-374.
Davison, R. M., Martinsons, M. G., Ou, C. X., Murata, K., Drummond, D., Li, Y. and Lo, H. W. (2009). "The ethics of IT professionals in Japan and China." *Journal of the Association for Information Systems* 10 (11), 834-859.
De Moya, J.-F. and Pallud, J. (2020). "From panopticon to heautopticon: A new form of surveillance introduced by quantified-self practices." *Information Systems Journal* 30 (6), 940-976.
Dewey, J. (1983). *The middle works, 1899-1924*: SIU Press.
Dinev, T. and Hart, P. (2006). "An extended privacy calculus model for e-commerce transactions." *Information Systems Research* 17 (1), 61-80.
Eisenhardt, K. M. (1985). "Control: Organizational and economic approaches." *Management Science* 31 (2), 134-149.
Enaible.io (2021). https://www.enaible.io (visited on November 12, 2021).
Fang, M., Su, J., Liu, J., Long, Y., He, R. and Wang, T. (2018). "A model to predict employee turnover rate: Observing a case study of chinese enterprises." *IEEE Systems, Man, and Cybernetics Magazine* 4 (4), 38-48.
Feng, G., Zhu, J., Wang, N. and Liang, H. (2019). "How paternalistic leadership influences IT security policy compliance: The mediating role of the social bond." *Journal of the Association for Information Systems* 20 (11), 1650-1691.
Feuerriegel, S., Dolata, M. and Schwabe, G. (2020). "Fair AI: Challenges and opportunities." *Business & Information Systems Rngineering* 62 (4), 379-384.
Foucault, M. (1973). *The birth of the clinic*. London: Travistock Publications.
Fox, M. J. and Reece, A. (2012). "Which ethics? Whose morality?: An analysis of ethical standards for information organization." *Knowledge Organization* 39 (5), 377-383.
Gal, U., Jensen, T. B. and Stein, M.-K. (2017). "People analytics in the age of big data: An agenda for IS research," in: *Proceedings of the 2017 International Conference on Information Systems*. Seoul, South Korea.
Gal, U., Jensen, T. B. and Stein, M.-K. (2020). "Breaking the vicious cycle of algorithmic management: A virtue ethics approach to people analytics." *Information and Organization* 30 (2), 100301.
Gallivan, M. J. (2001). "Striking a balance between trust and control in a virtual organization: a content analysis of open source software case studies." *Information Systems Journal* 11 (4), 277-304.

Gaur, B., Shukla, V. K. and Verma, A. (2019). "Strengthening people analytics through wearable IOT device for real-time data collection," in: *Proceedings of the 2019 International Conference on Automation, Computational and Technology Management*. London, UK. 555-560.

Giber, L. (2016). "Ethical framework of big data application," in: *Proceedings of the 2016 International Conference Information Systems*. Moscow, Russia. 1-6.

Giddens, L., Leidner, D. and Gonzalez, E. (2017). "The role of Fitbits in corporate wellness programs: Does step count matter?," in: *Proceedings of the 2017 Hawaii International Conference on System Sciences.* Hawaii, USA. 3627-3635.

Gilligan, C. (1993). *In a different voice: Psychological theory and women's development*: Harvard University Press.

Gotterbarn, D., Miller, K. and Rogerson, S. (1999). "Software engineering code of ethics is approved." *Communications of the ACM* 42 (10), 102-107.

Grand View Research (2020). *Corporate wellness market size, share & trends analysis*. https://www.grandviewresearch.com/industry-analysis/corporate-wellness-market (visited on November 12, 2021).

Grant, R. A. and Higgins, C. A. (1991). "The impact of computerized performance monitoring on service work: Testing a causal model." *Information Systems Research* 2 (2), 116-142.

Gurley, L. K. (2021). *Amazon delivery drivers forced to sign 'biometric consent' form or lose job*. https://www.vice.com/en/article/dy8n3j/amazon-delivery-drivers-forced-to-sign-biometric-consent-form-or-lose-job (visited on November 12, 2021).

Hawk, S. R. (1994). "The effects of computerized performance monitoring: An ethical perspective." *Journal of Business Ethics* 13 (12), 949-957.

Huang Chua, C. E. and Myers, M. D. (2018). "Social control in information systems development: a negotiated order perspective." *Journal of Information Technology* 33 (3), 173-187.

Humanyze (2021). https://humanyze.com (visited on November 12, 2021).

Irving, R., Higgins, C. A. and Safayeni, F. R. (1986). "Computerized performance monitoring systems: Use and abuse." *Communications of the ACM* 29 (8), 794-801.

Jones, N. A., Vasgaard, A. J., Taylor, R. J. and Jones, M. A. (2017). *Listening to the frontend*. https://patents.google.com/patent/US10020004B2/en (visited on November 12, 2021).

Keil, M., Rai, A. and Liu, S. (2013). "How user risk and requirements risk moderate the effects of formal and informal control on the process performance of IT projects." *European Journal of Information Systems* 22 (6), 650-672.

Kelly, R. K. and Snow, S. (2019). The importance of corporate wellness programs for psychological health and productivity in the workplace. In: R.J. Burke and A.M. Richardsen (Eds.), *Creating Psychologically Healthy Workplaces*, p. 411–430. Cheltenham, UK: Edward Elgar Publishing.

Kidder, R. (1995). *How good people make tough choices*. New York: HarperCollins.

Kim, J., Baskerville, R. L. and Ding, Y. (2020). "Breaking the privacy kill chain: Protecting individual and group privacy online." *Information Systems Frontiers* 22 (1), 171-185.

Kiran, A. H., Oudshoorn, N. and Verbeek, P.-P. (2015). "Beyond checklists: Toward an ethical-constructive technology assessment." *Journal of Responsible Innovation* 2 (1), 5-19.

Kirsch, L. J. (1996). "The management of complex tasks in organizations: Controlling the systems development process." *Organization Science* 7 (1), 1-21.

Kirsch, L. J., Sambamurthy, V., Ko, D.-G. and Purvis, R. L. (2002). "Controlling information systems development projects: The view from the client." *Management Science* 48 (4), 484-498.

Kudyba, S. (2020). "COVID-19 and the acceleration of digital transformation and the future of work." *Information Systems Management* 37 (4), 284-287.

Laudon, K. C. (1995). "Ethical concepts and information technology." *Communications of the ACM* 38 (12), 33-39.

Leclercq-Vandelannoitte, A. and Aroles, J. (2020). "Does the end justify the means? Information systems and control society in the age of pandemics." *European Journal of Information Systems* 29 (6), 746-761.

Lembcke, T.-B., Engelbrecht, N., Brendel, A. B. and Kolbe, L. (2019). "To nudge or not to nudge: ethical considerations of digital nudging based on its behavioral economics roots," in: *Proceedings of the 2019 European Conference on Information Systems*. Stockholm & Uppsala, Sweden.

Levchuk, K. (2019). How transhumanism will get us through the third millennium. In: N. Lee (Ed.), *The Transhumanism Handbook*, p. 75-88. Cham, Switzerland: Springer.

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.

Lim, W.-K., Sia, S. K. and Yeow, A. (2011). "Managing risks in a failing IT project: a social constructionist view." *Journal of the Association for Information Systems* 12 (6), 414-440.

Lindebaum, D., Vesa, M. and Den Hond, F. (2020). "Insights from "the machine stops" to better understand rational assumptions in algorithmic decision making and its implications for organizations." *Academy of Management Review* 45 (1), 247-263.

Manokha, I. (2020). "The Implications of Digital Employee Monitoring and People Analytics for Power Relations in the Workplace." *Surveillance & Society* 18 (4), 540-554.

Maruping, L. M., Venkatesh, V. and Agarwal, R. (2009). "A control theory perspective on agile methodology use and changing user requirements." *Information Systems Research* 20 (3), 377-399.

Mason, R. O. (1986). "Four ethical issues of the information age." *MIS Quarterly* 10 (1), 5-12.

Mayer, A.-S., Haimerl, A., Strich, F. and Fiedler, M. (2021). "How corporations encourage the implementation of AI ethics," in: *Proceedings of the 2021 European Conference on Information Systems*. Marrakech, Morocco.

Mettler, T. and Winter, R. (2016). "Are business users social? A design experiment exploring information sharing in enterprise social systems." *Journal of Information Technology* 31 (2), 101-114.

Mettler, T. and Wulf, J. (2019). "Physiolytics at the workplace: Affordances and constraints of wearables use from an employee's perspective." *Information Systems Journal* 29 (1), 245-273.

Mill, J. S. (2001). *Utilitarianism*. 2nd edition: Indianapolis: Hackett Publishing Company.

Mirchandani, D. A. and Lederer, A. L. (2014). "Autonomy and procedural justice in strategic systems planning." *Information Systems Journal* 24 (1), 29-59.

Myers, M. D. (2021). "Is there a shift from positivity to negativity about technology in the field of IS?" *European Journal of Information Systems* 30 (4), 357-358.

Myers, M. D. and Miller, L. (1996). "Ethical dilemmas in the use of information technology: An Aristotelian perspective." *Ethics & Behavior* 6 (2), 153-160.

O'Neill, P. and Hern, R. (1991). "A systems approach to ethical problems." *Ethics & Behavior* 1 (2), 129-143.

Olson, P. (2021). *More bosses expected to track their staff through wearables in the next 5 years* https://www.forbes.com/sites/parmyolson/2015/06/01/wearables-employee-tracking/ (visited on Noovember 12, 2021).

Ouchi, W. G. (1980). "Markets, bureaucracies and clans." *Administrative Science Quarterly* 25 (1), 129-141.

Pearson, J. M., Crosby, L. and Shim, J. P. (1996). "Modeling the relative importance of ethical behavior criteria: a simulation of information systems professionals' ethical decisions." *The Journal of Strategic Information Systems* 5 (4), 275-291.

Pellegrini, E. K. and Scandura, T. A. (2008). "Paternalistic leadership: A review and agenda for future research." *Journal of Management* 34 (3), 566-593.

Ragu-Nathan, T., Tarafdar, M., Ragu-Nathan, B. S. and Tu, Q. (2008). "The consequences of technostress for end users in organizations: Conceptual development and empirical validation." *Information Systems Research* 19 (4), 417-433.

Rawls, J. (2005). *A theory of justice*. Cambridge, MA: Harvard University Press.

Remus, U., Wiener, M., Saunders, C. and Mähring, M. (2020). "The impact of control styles and control modes on individual-level outcomes: a first test of the integrated IS project control theory." *European Journal of Information Systems* 29 (2), 134-152.

Rothschild, N. (2020). "Chipping away at our privacy: Swedes are having microchips inserted under their skin. What does that mean for their privacy?" *Index on Censorship* 49 (1), 17-19.

Sarkar, S., Vinay, S., Raj, R., Maiti, J. and Mitra, P. (2019). "Application of optimized machine learning techniques for prediction of occupational accidents." *Computers & Operations Research* 106, 210-224.

Schmitt, J. B., Breuer, J. and Wulf, T. (2021). "From cognitive overload to digital detox: Psychological implications of telework during the COVID-19 pandemic." *Computers in Human Behavior* 124, 106899.

Simbeck, K. (2019). "HR analytics and ethics." *IBM Journal of Research & Development* 63 (4/5), 9:1-9:12.

Smith, H. J. (2002). "Ethics and information systems: Resolving the quandaries." *ACM SIGMIS Database: the DATABASE for Advances in Information Systems* 33 (3), 8-22.

Soh, C., Chua, C. E. H. and Singh, H. (2011). "Managing diverse stakeholders in enterprise systems projects: a control portfolio approach." *Journal of Information Technology* 26 (1), 16-31.

Souza, M., Miyagawa, T., Melo, P. and Maciel, F. (2017). "Wellness programs: Wearable technologies supporting healthy habits and corporate costs reduction," in: *Proceedings of the 2017 International Conference on Human-Computer Interaction*. Vancouver, Canada. 293-300.

Tiwana, A. and Keil, M. (2009). "Control in internal and outsourced software projects." *Journal of Management Information Systems* 26 (3), 9-44.

Tursunbayeva, A., Pagliari, C., Di Lauro, S. and Antonelli, G. (2021). "The ethics of people analytics: risks, opportunities and recommendations." *Personnel Review*, forthcoming.

U.S. Courts Opinions (2015). *Arias v. Intermex Wire Transfer* https://www.govinfo.gov/app/details/USCOURTS-caed-1_15-cv-01101/summary (visited on November 12, 2021).

U.S. Government Office of Technology Assessment (1987). *The electronic supervisor: New technology, new tensions.* Washington DC. OTA-CIT-333.

Urbaczewski, A. and Lee, Y. J. (2020). "Information technology and the pandemic: A preliminary multinational analysis of the impact of mobile tracking technology on the COVID-19 contagion control." *European Journal of Information Systems* 29 (4), 405-414.

Verbeek, P.-P. (2006). "Materializing morality: Design ethics and technological mediation." *Science, Technology, & Human Values* 31 (3), 361-380.

Wagner, I. and Boiten, E. (2018). Privacy risk assessment: from art to science, by metrics. In: (Eds.), *Data Privacy Management, Cryptocurrencies and Blockchain Technology*, p. 225-241: Springer.

Walsham, G. (1996). "Ethical theory, codes of ethics and IS practice." *Information Systems Journal* 6 (1), 69-81.

Wang, B., Schlagwein, D., Cecez-Kecmanovic, D. and Cahalane, M. C. (2020). "Beyond the factory paradigm: Digital nomadism and the digital future(s) of knowledge work post-COVID-19." *Journal of the Association for Information Systems* 21 (6), 1379-1401.

Wang, W. and Siau, K. (2018). "Ethical and moral issues with AI: a case study on healthcare robots," in: *Proceedings of the 2018 Americas Conference on Information systems*. New Orleans, USA.

Willcocks, L. P. (2004). Foucault, power/knowledge and information systems: Reconstructing the present. In: J. Mingers and L. P. Willcocks (Eds.), *Social theory and philosophy for information systems*, p. 238-296. Chichester: John Wiley & Sons.

Zuboff, S. (1988). *In the age of the smart machine: The future of work and power*. New York: Basic Books.

Zuboff, S. (2015). "Big other: Surveillance capitalism and the prospects of an information civilization." *Journal of Information Technology* 30 (1), 75-89.

Zureik, E. (2003). Theorizing surveillance: The case of the workplace. In: D. Lyon (Eds.), *Surveillance as social sorting*, p. 31-56. London and New York: Routledge.