CHAPTER 5

Smart Technology in the Workplace: Threats and Opportunities for Trusting Employers

Xuchang Zheng, Simon Daniel Schafheitle, and Lisa van der Werff

Abstract In this chapter, we discuss the implications of how smart technology is experienced in the workplace for employee trust. Focusing on the defining features of smart technology and how these influence social interaction, we explore how trends in the permeation of technology in workplaces can influence employee trust in their employers creating both threats and opportunities for trust in this relationship. Realising the benefits of technological development requires employees to trust the intentions and capability of their employers to manage smart technology in ways that protect employee interests. We highlight the features of smart technology that may hamper this trust and discuss how addressing

X. Zheng (✉) • L. van der Werff
DCU Business School, Dublin City University, Dublin, Ireland
e-mail: xuchang.zheng@dcu.ie; lisa.vanderwerff@dcu.ie

S. D. Schafheitle
University of St. Gallen, St. Gallen, Switzerland
e-mail: simondaniel.schafheitle@unisg.ch

T. Lynn et al. (eds.), *The Future of Work*, Palgrave Studies in Digital Business & Enabling Technologies,
https://doi.org/10.1007/978-3-031-31494-0_5

concerns related to data privacy, situational normality, structural assurance, and employees' participation in the process is crucial for protecting and building trust in the workplace.

Keywords Smart technology • Trust • Organisation • Data privacy • Situational normality • Structural assurance • Employee participation

5.1 Introduction

The rapid growth of enterprise digital technology adoption has an increasing influence on organisational life impacting all stages of the employee life cycle (Schneider & Sting, 2020; von Krogh, 2018). In this chapter, we discuss how the use of digital technology in workplaces is critical to employee trust in their employing organisation. Useful reviews of the functioning logics and technological specificities of machine learning (ML) and deep learning (DL) algorithms can be found elsewhere (Alloghani et al., 2020; Jordan & Mitchell, 2015). In contrast, our focus in this chapter is on employees' experiences of technology and how cutting-edge technologies such as algorithm-based applications might become perceptible and tangible in organisations on a day-to-day-basis. Specifically, we highlight the trust impact of such technology through the lens of its socio-technological materialisations.

The remainder of this chapter considers employee trust in organisations in the context of smart technology. We outline why trust is critical to the success of smart technology adoption in the workplace before discussing challenges for protecting trust in employers in a technology-rich environment and opportunities for building employee trust in their organisation.

5.2 Employees' Trust in Organisations and Smart Technology

Trust, as a willingness to be vulnerable based on positive expectations of others, is often described as the foundation of social interaction (Lewis & Weigert, 2012; Mayer et al., 1995) or the lubricant that allows people to effectively interact and collaborate (Simpson, 2007). In the context of an organisation, trust is vital in facilitating effective interaction between co-workers, teams, and departments, as well as across these levels (Gillespie et al., 2021).

Employees' trust in their employer refers to the whole entity of the employing organisation as the target of trust (Fulmer & Gelfand, 2012).

Similar to trust in individuals (McKnight et al., 1998), the foundation of employees' trust in their employer can be broadly categorised into two domains (Mishina et al., 2012). The first aspect relates to the character of the organisation: what the organisation *intends* to do. It is usually reflected as an organisation's goals, preferences, and values (e.g., Love & Kraatz, 2009) and has close parallels with benevolence and integrity (Mayer et al., 1995). In the context of technology implementation, for instance, trust in the character of the organisation may influence whether employees infer that the goal of introducing new technology is to yield labour cost-savings or to provide additional staff support. The second aspect concerns employees' assessments of employer capability or competence: what the organisation *can* do (Mishina et al., 2012). Depending on the nature of the task in question, the capability of the employer may be assessed based on the knowledge or resources that enable the organisation to fulfil its goal. The question of whether introducing novel technologies in the workplace facilitates or complicates the distribution of resources or the outcome of employees' work remains particularly relevant given the broadened options available to the employer. Particularly in times of rapid change, uncertainty regarding an employer's character or capability can create doubts and anxieties that hamper trust in the employer and create resistance to the adoption of these unfamiliar methods and patterns of work.

Scholarly and industry sources repeatedly identify effective technology deployment in workplaces as being a critical challenge for firms over the next decade (Van den Heuvel & Bondarouk, 2017). Trust is vital in facilitating effective workplace interactions (Fulmer & Gelfand, 2012), allowing organisations to function successfully (Weibel et al., 2016), and to deploy technology smoothly (Bain & Taylor, 2000). Employee trust is crucial to the successful deployment of smart technologies, especially those involving ML/DL, as it shapes both the way employees are managed and their reaction to change (Zirkle & Staples, 2005; Bain & Taylor, 2000). Given the increasing uncertainty associated with the changing efficiency and patterns of the work that new technology can bring, a more nuanced understanding of technology's trust impact is critical (Lynn et al., 2021; van der Werff et al., 2021). In this chapter, we frame technology deployment effectiveness as a social process facilitated by a mutual awareness and protection of trust between the employee and employer.

Smart technology becomes a tangible part of employees' workplace experiences via two socio-technological materialisations: (1) appropriateness and (2) foresightedness (Nilsson, 2014). Using the example of a pocket calculator to illustrate the appropriateness of smart technology

(Stone et al., 2018), smart technology functions appropriately because, compared to humans, it performs complex calculations faster, more precisely, and with a much lower probability of error. However, facilitating the accuracy and efficiency of work by itself is not sufficient to be called a smart technology. The other crucial condition for technology to be perceived as smart is foresightedness, which helps refine work without human intervention (Chakraborty et al., 2017). Foresight, based on the various forms of supervised and unsupervised ML/DL, enables technology to autonomously "get better at what it does" and thus to apply its technological capabilities to the original but also to related and novel questions. IBM's Watson algorithm is an intuitive example of this. Although it was initially trained to recognise dog motifs from a large number of pictures, it is now employed to perform a wide range of other tasks including filtering future high potentials from a large number of job applications. It is this foresightedness of smart technology that brings out the potential for automation, not only with regard to work execution but also to aspects of leadership. Often this foresightedness creates anxiety and heightened vulnerability for humans interacting with the technology due to a lack of understanding and transparency regarding how particular decisions are made (Orlikowski & Scott, 2014; Nilsson, 2014).

Smart technology draws on developments in ML/DL processes and can be used within the employment relationship to (1) assist and support organisations in directing employees' attention, motivating or encouraging them to act in desirable ways, and (2) enable new ways of doing so, that have not been possible in the analogue world (Cardinal et al., 2010; Schafheitle et al., 2020). For instance, Gloor et al. (2018) have demonstrated how virtual mirroring (i.e., technology that captures communication behaviour including "between the lines") helps employees to adapt their communication styles to their peers' needs and supports leaders in designing employee needs-based development plans. Other examples of smart technology application in the employment relationship range from algorithmic automation of shortlisting as a part of the recruiting process (Hunkenschroer & Luetge, 2022), performance monitoring and evaluation software (Ravid et al., 2020), "smart" feedback solutions with algorithmic nudging capabilities for leaders (Buck & Morrow, 2018) to virtual career assistants which help employees increase their promotability, job mobility, and personal development (Stieglitz et al., 2021).

The potential benefits of smart technology application in these situations are increasingly clear; however, given the importance of trust in technology

adoption and organisational change more generally, realising those benefits requires organisations and their leaders to be cognisant of how smart technology can influence trust in the organisation. The extent to which smart workplace technology changes the levels of risk and trust employees experience in their organisation depends on the design and functionality of the technology in question. Common practices of advocating the technological strengths of smart technology, in particular relative to human performance in the workplace, is unlikely to be effective as it does little to support perceptions of organisational character or capability. In the remainder of this chapter, we explore the challenges and opportunities that smart technology poses for trust between employees and their organisations.

5.3 Challenges for Protecting Trust in the Organisation

Two of the key reasons why employees' trust in their employing organisation might be strained by smart technology deployment broadly relate to how employee perceptions of their organisation's character are influenced by changes in visibility and accountability and interest alignment. Specifically, employees' perceptions of the employer's character, which are challenged by technology-heightened levels of employee visibility that highlight power differentials and vulnerabilities in the relationship, relate to benevolence. Similar character perceptions regarding employer integrity may become strained given changes in interactions between employees and their leaders that highlight differences in accountability and interest alignment within the workplace.

Smart technology use in the employment relationship creates enormous quantities of data about employee behaviour. This process frames employees as data subjects which may hamper employee trust because it makes them more visible inside the organisation (Stanton & Stam, 2006). More precisely, it increases the overall workplace transparency by transforming the formerly unmeasurable into measurable quantities. In the words of Bernstein (2017, p. 218), increased workplace transparency can be summarised in the following four exemplary statements: "Let us all see your activity" (i.e., technology-augmented monitoring), "Watch our workflow" (i.e., technology-augmented process visibility), "We're watching everything you do" (i.e., technology-enabled workplace surveillance),

and "Let me tell you about your work" (i.e., technology-enabled disclosure of novel or hitherto unmeasurable employee information).

Smart technology allows organisations to gather and interpret employee performance data not only through log-in times, mouse pointer movements, or URL-/logfile evaluations but also through more invasive methods including recording eye movements in human-machine interaction, wearable robotics (e.g., fatigue measurement through exoskeletons), or Internet-of-Things applications, including wearable GPS devices or bio-radio frequency identity (RFID) chips. For instance, "smart chairs" and CO_2 measurements enable the collection of performance data, such as when employees are most productive (e.g., Wang & MacLellan, 2018), or "smart toilets" enable the collection of health data as a means to later evaluate promotion opportunities (e.g., Petre, 2018). Recently, Hong Kong engineers have started to analyse executive-level board members' brain activity during C-suite meetings to decipher the success formula of effective corporate governance (Copeland & Hope, 2016).

Compared to the more traditional working environment, the technology-augmented information acquisition and analysis of employee data can challenge trust in two ways. Firstly, technology can challenge employee beliefs about what they can expect from the employment relationship and how central they are in the organisation's priorities. The implementation of new technology can be framed either as intending to enable employees or as an attempt to create a foolproof organisation in a way that alienates employees and leads to feelings of coercion (Adler & Borys, 1996). Second, the change to processes that accompanies technology deployment in the workplace can negatively affect employee perceptions of situational normality and that everything is "as it should be". Technology proliferation that increases visibility, for instance, influences employees' feelings of vulnerability due to being monitored by the employer in a way that is likely to make them more alert and careful in their workplace interactions. Finally, as with many change initiatives, introducing new smart technology in the workplace can trigger suspicion in management's intention in implementing these changes. Specifically, employer collection of data sources such as feelings, relationship qualities, and other previously relatively personal information either conveys that the employer suspects bad or dishonest intentions of employees or intends to use this information as a trust substitute (Falk & Kosfeld, 2006; Lockey et al., 2021; Whitener et al., 1998). Secondly, technology functions related to decision selection and action implementation raise issues related to

accountability and interest alignment that are likely to affect perceptions of the capability of the manager and the employer. Even when the digitised decision and action process is designed to support the manager's own job (Murray et al., 2021), employees may still question the manager's control of the technology and how they will be affected by the change. Will my manager be persuaded by the recommendations or decisions of technology that might negatively affect my performance appraisal? The use of information in this way implies a change to established ways of interacting between employees and employers.

Schafheitle et al. (2021) have argued that smart technology deployment leads to the increasing automation of leadership, even for those tasks that were previously believed to remain in the "human turf". For instance, media reports of such technologies note its ability to secretly nudge other people, to emotionally trigger them (Meckel, 2018), or to tell funny jokes (Gloor et al., 2018). Schafheitle et al. (2021) outline three trust-critical scenarios: a continuous blurring of responsibilities, conflicting directives of human managers and algorithms, and the fraternisation or co-option of the human manager and the algorithm against the employee. This first scenario is trust-critical because it increases uncertainty for employees. Questions similar to "To whom am I responsible?", "Why do I always have to take the rap?", "Does my manager still envisage the 'right' goals?", or "Can I be sure that they will always act in ways to protect my interests?", are likely to emerge. The second scenario becomes tangible if one considers that the most accurate decision is not always the "best" one for the company. For instance, it might be appropriately calculated that an employee fails to meet a certain email frequency threshold for qualifying as an internal expert, but they might be offering advice and/or mentoring support face-to-face, always having an open ear or offering support via their physical and emotional presence. The third scenario is well-entitled as "human oversight" where managers "blindly rely" on algorithmic feedback and, more or less explicitly, negate to include contextual information for managerial sense-making.

Focusing on the needs of the organisation but overlooking the concerns of the employee, smart technology designed either for decision support or implementation via various individual channels can be perceived by employees to be particularly threatening. Further, for employees, if smart technology interferes with human decision-making and implementation, it is likely to be perceived as contrasting the existing pattern of work, which tends to lower trust in the manager and the employee's subsequent

willingness to accept the change proposed. For organisations, balancing between the needs for more detailed information about employees and the complex functioning of smart technology and anticipated employee resistance is key to the success of maintaining trust and introducing these changes in the workplace. Therefore, the question remains: how can effective smart technology implementation be achieved without threatening employment relationships?

5.4 Opportunities for Building Trust in the Organisation

Examining this issue from a trust perspective, we look to opportunities for organisations to implement smart technology in ways that are more protective and supportive of trust. In particular, theory suggests that careful attention to issues of data privacy, situational normality, structural assurance, and employee participation are likely to be vital. We provide some exploration of these protective measures below though further research is necessary to determine the efficacy and boundary conditions of these measures for protecting employee trust during the proliferation of smart technology in our workplaces.

Protecting data privacy by minimising the visibility of an individual footprint in the process of smart technology deployment is crucial for retaining employee trust while implementing the change (Stanton & Stam, 2006). The anonymisation of employee data starting from the earlier stages (e.g., data collection) and covering more stages of the overall technology deployment process can help to address employees' concerns. If anonymity cannot be guaranteed, organisations are particularly prone to the loss of trust.

Further, as members of the same organisation, employees' interpretation of managers' and colleagues' trustworthiness can be enhanced by giving a sense of situational normality (McKnight et al., 1998). If the way work is carried out appears to be "normal" and "in proper order" even after smart technology deployment (Baer et al., 2018; Lewis & Weigert, 1985), employees may reasonably rely on their past positive experience to infer that managers will continue to behave in a similarly normal and predictable manner. For organisations, with the adoption of smart technology becoming the new norm, the restoration of a sense of normality is crucial for trust to grow and flourish within the organisation. Employees who are

comfortable with their own role and the purpose of smart technology, knowing the latter's introduction will support rather than replace their job, are more likely to maintain trust in the employer.

Providing structural assurance, such as regulatory or social safeguards, that reinforces any claims made by management is a useful channel for enhancing trust, especially at the initial introduction of the new technology rather than later (McKnight et al., 1998). Structural assurance that focuses on stipulating the actions of management, for instance, professional membership or organisational policies that prescribe adherence to a clear set of ethical norms, is powerful for encouraging acceptance of new technology (Long & Sitkin, 2018). Employees feel more assured about the intentions of managers when the potential cost of any untrustworthy behaviour such as misconduct or exploitation is higher than its reward. On the other hand, positive structural reinforcement, such as rewards for successful utilisation of new technology in the workplace, provides another incentive for employees to experience and verify the authenticity of their manager's words.

Lastly, highlighting the employer's control over decision selection and action implementation processes is crucial for maintaining an overall sense of normality within the organisation. Even when smart technology automates decision and action implementation, managers may emphasise and clarify "human logic" as the foundation of automation. For instance, a group understanding or consensus in relation to automation must be achieved for it to be enacted (Murray et al., 2021). Alternatively, any decision or action taken via automation may be approved and announced by managers instead of being implemented without scrutiny. To be perceived as a supporting function rather than the actual agent of decisions is crucial for the acceptance of automation by employees, before the change becomes the new norm within the organisation. Similar to Feldman's assertions that organisational theory holds "so long as human agents perform them" (2000, p. 627), an employee's trust holds when they perceive human, not smart technology, to be the true leader who ultimately determines the process and outcome in the workplace (Schafheitle et al., 2021).

The potential for smart technology to make work easier and more efficient through greater transparency, efficient knowledge management, and learning has been repeatedly demonstrated. Yet, its initial success in socio-technological materialisations hinges on whether the technology builds an employee's confidence in the character and capability of the organisation rather than, or at least as well as, the technology itself. For

management, clarifying intentions and providing assurance in relation to the purpose of the new technology may be even more crucial for protecting and building trust than advocating its technological strengths and benefits. Besides the various pay-offs associated with successful tango of smart technology and trust in the workplace, companies might also consider trust protection as a normative principle, since trust, personal growth, and flourishing have been established as virtues of modern work.

References

Adler, P. S., & Borys, B. (1996). Two types of bureaucracy: Enabling and coercive. *Administrative Science Quarterly, 41*(1), 61–89.

Alloghani, M., Al-Jumeily, D., Mustafina, J., Hussain, A., & Aljaaf, A. J. (2020). A systematic review on supervised and unsupervised machine learning algorithms for data science. In *Supervised and unsupervised learning for data science*, 3–21. Springer.

Baer, M. D., Van Der Werff, L., Colquitt, J. A., Rodell, J. B., Zipay, K. P., & Buckley, F. (2018). Trusting the "look and feel": Situational normality, situational aesthetics, and the perceived trustworthiness of organizations. *Academy of Management Journal, 61*(5), 1718–1740.

Bain, P., & Taylor, P. (2000). Entrapped by the 'electronic panopticon'? Worker resistance in the call centre. *New Technology, Work and Employment, 15*(1), 2–18.

Bernstein, E. S. (2017). Making transparency transparent: The evolution of observation in management theory. *Academy of Management Annals, 11*(1), 217–266.

Buck, B., & Morrow, J. (2018). AI, performance management and engagement: Keeping your best their best. *Strategic HR Review, 17*(5), 261–262.

Cardinal, L. B., Sitkin, S. B., & Long, C. P. (2010). A configurational theory of control. In S. B. Sitkin, L. B. Cardinal, & K. Bijlsma-Frankema (Eds.), *Organizational control* (pp. 51–79). Cambridge University Press.

Chakraborty, S., Tomsett, R., Raghavendra, R., Harborne, D., Alzantot, M., Cerutti, F., … Rao, R. M. (2017). *Interpretability of deep learning models: A survey of results.* Paper presented at the 2017 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computed, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI).

Copeland, R., & Hope, B. (2016). The world's largest hedge fund is building an algorithmic model from its employees' brains. *The Wall Street Journal.*

Falk, A., & Kosfeld, M. (2006). The hidden costs of control. *American Economic Review, 96*(5), 1611–1630.

Feldman, M. S. (2000). Organizational routines as a source of continuous change. *Organization Science, 11*(6), 611–629.

Fulmer, C. A., & Gelfand, M. J. (2012). At what level (and in whom) we trust: Trust across multiple organizational levels. *Journal of Management, 38*(4), 1167–1230.

Gillespie, N., Fulmer, C. A., & Lewicki, R. J. (Eds.). (2021). *Understanding trust in organizations: A multilevel perspective.* Routledge.

Gloor, P., Fischbach, K., Gluesing, J., Riopelle, K., & Schoder, D. (2018). Creating the collective mind through virtual mirroring based learning. *Development and Learning in Organizations: An International Journal, 32*(3), 4–7.

Hunkenschroer, A. L., & Luetge, C. (2022). Ethics of AI-enabled recruiting and selection: A review and research agenda. *Journal of Business Ethics*, 1–31.

Jordan, M. I., & Mitchell, T. M. (2015). Machine learning: Trends, perspectives, and prospects. *Science, 349*(6245), 255–260.

Lewis, J. D., & Weigert, A. (1985). Trust as a social reality. *Social Forces, 63*(4), 967–985.

Lewis, J. D., & Weigert, A. J. (2012). The social dynamics of trust: Theoretical and empirical research, 1985–2012. *Social Forces, 91*(1), 25–31.

Lockey, S., Gillespie, N., Holm, D., & Someh, I. A. (2021, January). A review of trust in AL: Challenges, vulnerabilities and future directions. In *Proceedings of the 54th Hawaii International Conference on System Sciences* (p. 5463).

Long, C. P., & Sitkin, S. B. (2018). Control–trust dynamics in organizations: Identifying shared perspectives and charting conceptual fault lines. *Academy of Management Annals, 12*(2), 725–751.

Love, E. G., & Kraatz, M. (2009). Character, conformity, or the bottom line? How and why downsizing affected corporate reputation. *Academy of Management Journal, 52*(2), 314–335.

Lynn, T., van der Werff, L., & Fox, G. (2021). Understanding trust and cloud computing: An integrated framework for assurance and accountability in the cloud. In *Data privacy and trust in cloud computing* (pp. 1–20). Palgrave Macmillan.

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. *Academy of Management Review, 20*(3), 709–734.

McKnight, D. H., Cummings, L. L., & Chervany, N. L. (1998). Initial trust formation in new organizational relationships. *Academy of Management Review, 23*(3), 473–490.

Meckel, M. (2018). *Mein Kopf gehört mir: Eine Reise durch die schöne neue Welt des Brainhacking.* Piper.

Mishina, Y., Block, E. S., & Mannor, M. J. (2012). The path dependence of organizational reputation: How social judgment influences assessments of capability and character. *Strategic Management Journal, 33*(5), 459–477.

Murray, A., Rhymer, J., & Sirmon, D. G. (2021). Humans and technology: Forms of conjoined agency in organizations. *Academy of Management Review, 46*(3), 552–571.

Nilsson, N. J. (2014). *Principles of AL*. Morgan Kaufmann Publishers.

Orlikowski, W. J., & Scott, S. V. (2014). What happens when evaluation goes online? Exploring apparatuses of valuation in the travel sector. *Organization Science, 25*, 868–891.

Petre, J. (2018). Big Brother is watching loo: Fears over 'smart' lavatory that can test users for drugs, pregnancy and urine problems. *Daily Mail on Sunday*. Retrieved September 1, 2022, from https://www.dailymail.co.uk/news/article-5905047/Fears-smart-lavatory-test-users-drugs-pregnancyurine-problems.html

Ravid, D. M., Tomczak, D. L., White, J. C., & Behrend, T. S. (2020). EPM 20/20: A review, framework, and research agenda for electronic performance monitoring. *Journal of Management, 46*(1), 100–126.

Schafheitle, S., Weibel, A., Ebert, I., Kasper, G., Schank, C., & Leicht-Deobald, U. (2020). No stone left unturned? Towards a framework for the impact of datafication technologies on organizational control. *Academy of Management Discoveries, 6*(3), 455–487.

Schafheitle, S., Weibel, A., & Rickert, A. (2021). The Bermuda Triangle of leadership in the AI era? Emerging trust implications from "two-leader-situations" in the eyes of employees. In *Proceedings of the 54th Hawaii International Conference on System Sciences* (pp. 5473–5482).

Schneider, P., & Sting, F. J. (2020). Employees' perspectives on digitalization-induced change: Exploring frames of industry 4.0. *Academy of Management Discoveries, 6*(3), 406–435.

Simpson, J. A. (2007). Psychological foundations of trust. *Current Directions in Psychological Science, 16*(5), 264–268.

Stanton, J. M., & Stam, K. R. (2006). *The visible employee: Using workplace monitoring and surveillance to protect information assets—Without compromising employee privacy or trust*. Information Today, Inc.

Stieglitz, S., Mirbabaie, M., Möllmann, N. R., & Rzyski, J. (2021). Collaborating with virtual assistants in organizations: Analyzing social loafing tendencies and responsibility attribution. *Information Systems Frontiers*.

Stone, M., Knapper, J., Evans, G., & Aravopoulou, E. (2018). Information management in the smart city. *The Bottom Line*.

Van den Heuvel, S., & Bondarouk, T. (2017). The rise (and fall?) of HR analytics: A study into the future application, value, structure, and system support. *Journal of Organizational Effectiveness: People and Performance, 4*(2), 157–178.

van der Werff, L., Blomqvist, K., & Koskinen, S. (2021). Trust cues in Artificial Intelligence. In *Understanding trust in organizations: A multilevel perspective*. Routledge.

von Krogh, G. (2018). Artificial Intelligence in organizations: New opportunities for phenomenon-based theorizing. *Academy of Management Discoveries, 4*(4), 404–409.

Wang, A. X., & MacLellan, L. (2018). Herman Miller's new Aeron chair is an office spy, collecting data on your every move. *Quartz Work*. Retrieved September 1, 2022, from https://qz.com/work/1218346/herman-millers-new-aeron-chair-isan-office-spy-collecting-data-on-your-every-move/

Weibel, A., den Hartog, D. N., Gillespie, N., Searle, R., Six, F., & Skinner, D. (2016). How do controls impact employee trust in the employer? *Human Resource Management, 55*(3), 437–462.

Whitener, E. M., Brodt, S. E., Korsgaard, M. A., & Werner, J. M. (1998). Managers as initiators of trust: An exchange relationship framework for understanding managerial trustworthy behavior. *Academy of Management Review, 23*(3), 513–530.

Zirkle, B., & Staples, W. (2005). Negotiating workplace surveillance. In J. Weckert (Ed.), *Electronic monitoring in the workplace: Controversies and solutions* (pp. 79–100). Idea Group Publishing.