iS
CHANNEL

Workplace Surveillance Outside the Workplace: An Analysis of E-Monitoring Remote Employees

Amy Vatcha

MSc Management of Information Systems and Digital Innovation
Department of Management
London School of Economics and Political Science

KEYWORDS

Workplace Surveillance
E-Monitoring
Remote Employees
Privacy
Security

ABSTRACT

In the time of Covid-19, working from home has suddenly become the norm. This thematic literature review explores the workplace surveillance landscape for remote workers from an employee perspective. The literature considered includes information systems journals, management journals, regulation whitepapers, and technological solutions. This paper discusses the excessive surveillance that occurs, the technologies that facilitate it, why it erodes trust with employers, and what tools and frameworks employees can use to demand privacy. Employee surveillance is no longer confined to the office space, it is holistic, constant, round the clock monitoring, enabled by new technologies and lowering costs of existing technologies. I argue that remote employee acceptance of workplace monitoring solutions depends on the transparency on data collection from employers, and the exclusive use of the data for security rather than hiring and firing decisions.

I. Introduction

The presence of workplace surveillance is not a surprise to employees in white collar roles. In the context of remote working, the dynamic is unique because there are no physical boundaries between work and leisure hours. In this essay, I explore the specific context of remote working from an employee perspective, where the living room doubles as an office. Some employers offer flexible working accommodations such as working from home, or working from anywhere including co-working spaces such as WeWork, or an island in the Mediterranean. There are blurred boundaries between the home and office, which is problematic because employee surveillance extends beyond in-office monitoring to 24/7 surveillance. The surveillance technology is "unblinking" and "ever-present" (Nord, 2006). Employee surveillance is no longer confined to the office space, it is holistic, constant, round the clock monitoring, enabled by new technologies and lowering costs of existing technologies. The flexibility comes at a price, being the boss of one's own schedule literally means that one's boss can monitor employees anytime. The goal of employers offering flexibility is to improve employee-employer relationships, so excess surveillance would undermine these efforts.

Rather than broadly defining the concept of privacy, in the context of this paper it would be more appropriate to define the importance of privacy as "privacy thus possesses intrinsic value: it is essential for thinking and acting freely" (Stone-Romero & Stone, 2007). The Computer Security Institute (CSI) found that over 75% of companies faced issues with employees using illegitimate software, online shopping during work, accessing pornographic material, using work hours for childcare or napping, and using their work emails inappropriately (Nord, 2006; Bloomberg, 2020). To detect employees who are shirking their responsibilities during work hours, surveillance technology is employed. There is "large scale systematic monitoring" using software such as Spectorsoft, DynaComm, Investigator 2.0, and Silent Watch (Introna, 2002; Nord, 2006; Nockleby, 2002). These software solutions solve "an old puzzle made more complex with new software" (Nord, 2006). Investigator 2.0 is available for under $100 and sends summaries of all activities on a given PC, while Silent Watch even provides the exact typing patterns, so the technologies are already available at a lower cost than ever before (Nockleby, 2002). The root of the problem is the use of intrusive technologies without consent in private places such as the home of a remote worker. I argue that in the era of technology, flexible working, and fluid boundaries between the home and office, workplace monitoring for business reasons often extends into one's personal life leading to all round employee monitoring. Remote employee acceptance of workplace monitoring solutions depends on these factors - transparency on data collection from employers, clarification of data usage for system security or for hiring and firing decisions, and the avenues available for employee privacy concerns to be heard.

II. Why Excess Employee Surveillance Erodes Trust

What forms of surveillance are used? Which are considered "excessive"?

Corresponding Author
Email Address: vatcha.amy@berkeley.edu

Employers justify carrying out surveillance to protect company secrets and sensitive confidential information, protect themselves in case of liability issues such as discrimination or harassment, prevent "time theft" where employees lie about their hours, discourage employees from carrying out non work-related tasks at work, or "careless communication" which can expose the company's systems to phishing (Smith & Tabak, 2009). In an organization, there are various threats to data privacy such as phishing attacks, system security vulnerabilities, hackers gaining unauthorized access to the network, but employees are known to be the weakest link in organizational data privacy (Pigni et al., 2018; Culnan et al., 2009). For example, in the Target data breach in 2013, the initial access to the system was granted by an unsuspecting employee, the aftermath of which cost the company upwards of $18 million and a lifetime of irreparable public relations damage (Pigni et al., 2018). Moreover, today's labor market is evolving for the gig economy, with new employee categories such as independent contractors and outsourcing becoming increasingly common. Contractors are not bound by the same non-disclosure agreements as full-time employees are, which adds another layer of vulnerability to data privacy initiatives. Besides cybersecurity concerns stemming from employee negligence, employees can also tarnish the reputation of their employer if they engage with inappropriate social media posts even when they are not at work (Hyman, 2017). Social media posts are monitored because personal views of an employee can be tied to the company's public image. The public connotation of the data on the platform merges with the private aspect that is usually hidden from coworkers. Employers use workplace surveillance to monitor employee honesty while using it as a tool to prevent employees from engaging in unproductive and illegal acts at work including extra breaks, and safety shortcuts (Stone-Romero & Stone, 2007). The monitoring techniques include using contemporary technologies such as artificial intelligence, advanced analytics, mobility data, keystroke logging software, and social media, but the monitoring is considered excessive because it occurs round the clock including in an employee's personal time.

Why is employee trust necessary for employers?

Employee buy-in is necessary with any investment in workplace technology because employees would react negatively if their freedom is threatened or if the privacy invasion is unfair (Horton, 2020; Parks et al., 2017). According to an executive at Simply Communicate workplace consultancy, "tracking technology without clear well-communicated mutual benefit for both business and employee always struggles to get adoption or, worse, may be inadvertently or deliberately sabotaged by employees" (Horton, 2020). The necessity of employee surveillance has been compared to using security cameras at a bank, "not because of lack of trust...it's because it's imprudent not to do it" (Bloomberg, 2020). If employees comply with all of their duties, and companies are transparent with how they are tracking their employees, the hostility and pushback against surreptitious surveillance can give way to a solid trust relationship. As a Bloomberg article for managers suggested, "if you hired them, you should trust them" (Bloomberg, 2020). Value-driven companies aim to protect the interests of their stakeholders, and employee monitoring is inconsistent with this message to the company's most valuable asset: their staff.

Why does excess surveillance erode trust?

The power dynamic between employers and employees is incredibly asymmetrical. Employers are in a position of power through the contracts that employees sign, the paychecks they are in charge of, and the terms and conditions of being on the job. Employees can be constantly monitored, i.e. "passive surveillance", rather than actively surveilled where particular employee's actions have sparked the suspicions of the system (TUC, 2017). Passive surveillance is the prevalent form of employee monitoring today, involving "blanket" monitoring of all employees regardless of individual justification (TUC, 2017). Active surveillance focuses on depth rather than breadth of surveillance, with particular individuals being closely monitored (TUC, 2017). Active surveillance is problematic because it is more susceptible to human bias. Executives have access to more confidential information and information systems than junior employees do. Yet, active surveillance mechanisms scrutinize junior entry-level employees at a higher rate than executives are monitored (TUC, 2017). An e-monitoring solution called Hubstaff conducts dynamic surveillance according to job title (Bloomberg, 2020). Companies need to calculate if the loss of employee morale created due to surveillance is worth the value that surveillance brings (Horton, 2020). If employers trusted their employees, they would measure their performance output instead of effort input (TUC, 2017). E-monitoring erodes psychological trust where the perceived risks of the monitoring system cannot be controlled by the employee so they lack control over their personal information (Ozdemir et al., 2017).

III. Why Employee Monitoring is Holistically Intrusive

Surveillance starts before an employee is even onboarded! The background check is the starting point for workplace surveillance, before a candidate has even signed their employment contract. Background checks previously provided a one-time snapshot of past crimes, but now in the USA, the FBI's RAP BACK program allows employers to receive continuous information about their employees, and their involvement with petty crime or police (Kofman, 2017). New technologies enable new kinds of holistic surveillance techniques, but also bring down the cost of monitoring. For example, the FBI's RAP BACK program only costs an employer $13/person monitored (Kofman, 2017). Opt-in or opt-out is not feasible because this kind of surveillance is mandatory in employment contracts (D'Acquisto et al., 2015). Candidates in the pipeline also have their social media accounts parsed.

Employee monitoring is holistically intrusive because it extends beyond the boundaries of work-

related surveillance. In the case of remote working, the forms of surveillance include computer log on and off times, location tracking of work phones and laptops, search history typing speed, keystrokes (including passwords), call logs, instant messenger chat response speed, and emails scanned for financial crime such as insider trading (Jeske et al., 2015; TUC, 2017; Bloomberg, 2020). Arguably, tracking computer logon and logoff times is parallel to in-office workers who are tracked by how much time they spend at work via badge scans (Horton, 2020). Barclays uses heat sensors and motion detection to track employee presence, but claims that this information is collected to optimize office space and floor layout (Horton, 2020). Office desktop monitoring is not a new phenomenon, but it "seems a violation of privacy to a lot of workers when they're required to have software on their computers that tracks their every move in their own homes'' (Bloomberg, 2020). According to Gartner, employee monitoring will occur in 80% of companies by 2021 (Horton, 2020). Covid-19 has made e-monitoring software solutions popular such as InterGuard, Time Doctor, Teramind, VeriClock, innerActive, ActivTrak, and Hubstaff (Bloomberg, 2020). A software called Sneek takes pictures of an employee every five minutes via webcam to check if they are at work, and companies have access to a "wall of faces'' to monitor them at a glance (Holmes, 2020). These technological solutions can be used outside of standard working hours (Horton, 2020). The judgements from after-hour monitoring can leak into workplace compensation decisions (TUC, 2017).

Lack of Transparency around Data Collection Methods

Remote employees are monitored by their internet use, social media posts, audio from their work laptops, phone calls, mobility data from their work phone, every email that flows through their work email account, every file saved on a work computer, and every keystroke typed (Ball, 2010; Bowcott & Rawlinson, 2017). If an employee turns off their company issued mobile phone to disconnect from work on the weekend, their offline status can be detected. New technologies are enabling e-surveillance and employers are "harnessing the emergence of Big Data, the Internet of Things, and artificial intelligence in the workplace" (A. K. Agarwal, Gans, & Goldfarb, 2017). This data is being used, however employees have no insight into what data is being collected, how it is used, whether the data is used in promotions or terminations, whether the data can lead to discrimination, and what happens to one's data after termination. Employers do not disclose these details because they do not want employees to beat the system. An innovative solution to drive transparency in data collection can be achieved with visual models showing where the data goes and what automated decision making is used for (D'Acquisto et al., 2015).

Functional Creep in Employee Data Usage

"Functional creep" occurs when more information than the necessary minimum is being monitored (Ball, 2010; Kofman, 2017). Storing and harnessing data from many sources is cheaper and easier than it ever has been. Although employee data can be used in firing decisions, it is unclear whether the data is deleted and erased if an employee voluntarily terminates their job. Employees tend not to be told what information is monitored so they cannot tailor their actions and do not know if they are on the "watchlist" or not (Jeske et al., 2015). Employers claim that employees are monitored to ensure the security of the company's systems, but "functional creep" occurs when these same data points are used to measure performance through speed and correctness of work (Jeske et al., 2015; TUC, 2017; Kofman, 2017; Ball, 2010). E-monitoring warps the incentive of employees to complete their work with full accuracy and "doesn't take into account the realities of the job" (TUC, 2017). E-monitoring is a "blunt tool" for performance measurement because tracking time needed to complete a task might not reward the employee for doing a thorough job (TUC, 2017).

Mission Creep

"Mission creep" is where employee data can be used for alternate uses than the existing data was collected for, for example used in a discriminatory manner (Kofman, 2017; Ball, 2010). The justification is that data has already been collected and is readily available, even if not used for its original intended purpose (Kofman, 2017; Ball, 2010). If data is already collected and stored, it can easily be put to other uses and abused. Given that the employee has no visibility into the surveillance process, the employee does not know if their employer has crossed the boundary of acceptable use. Ideally, organizations should control who has access to employee data, the form of access controls, what access an immediate manager has, and whether HR can access one's information for hiring and firing decisions (D'Acquisto et al., 2015). In reality, these information points are not shared and employees fear retaliation if they were to ask. Another example of "mission creep" is that managers are notified if one of their employees seems to be looking for their next job based on their search history or documents downloaded (Kofman, 2017; Ball, 2010, Bloomberg, 2020). The dark side of "mission creep" occurs when employers sift through employee data to find a reason to fire an employee and "find the one mistake you made if they wanted" (Kofman, 2017; Ball, 2010; TUC, 2017). This is a departure from the primary purpose of workplace data collection for the goal of systems security and performance monitoring.

IV. How Employees Demand Privacy

What aspects of surveillance need to be transparent?

Employers do not share insight into what data is collected because that can give employees the information needed to work around the system. Consequently, employees have no idea what the collected data is being used for. Employment agreements require employees to waive their right to workplace privacy by allowing routine collection of information. Routine information collection is more invasive than circumstantial investigation, because the latter would require a special justification as to why a particular employee was singled out to be

closely monitored, whereas routine data collection involves all employees at all times (Wicker, 2011). Wicker (2011) studied the effects of active versus passive surveillance, also termed as comprehensive versus random monitoring (Wicker, 2011; Chen et al., 2007). Active surveillance profiles certain categories of people through a pre-selection where the user is unaware and cannot explain their side of the story, while passive surveillance limits employees from experimenting for fear of triggering the suspicion of the system (Wicker, 2011). The cost of data collection and storage is exponentially reducing over time. Therefore, employers are easily able to collect more information than ever before. Employee data mining is problematic because it represents the power that the organization has over each employee, furthering the existing "asymmetry of power" (Introna, 2002). Traditional principles such as anonymization cannot solve this problem because the very premise of employee monitoring is to track which employees do not cover their fair share of work. Decentralized repositories for data from disparate sources is recommended (D'Acquisto et al., 2015). If employees were given insight into how the surveillance is carried out, they could use that information to endorse their current capabilities as high-performing employees.

Trade Unions

According to the Trades Union Congress (TUC), new forms of surveillance should be implemented in the workplace only after informing trade unions who have a fundamental right to be involved in the decision-making process (TUC, 2017). Long-Bailey from the Labor Party in the UK strives to minimize the always-on working habits by allowing employees to pause from their work emails after hours (Topping, 2020). She supports a short-term and long-term plan for up to 5 years which was outlined in a manifesto to drive collective bargaining and protect mental health (Topping, 2020). Some middle managers are tempted to embrace surveillance to monitor their employees, but then realize that their senior leadership is using the same technology to scrutinize them, so both front line employees and middle level managers are supportive of trade unions solving this problem. Hosting regular catch-up meetings for employees and their managers is a low-tech solution suggested by trade union representatives to solve the problem of assessing productivity, but makes it harder for managers to complete their own daily workload if they are constantly checking in with large teams (Bloomberg, 2020). Trade union reps also suggest a more regimented structure of work hours to be applied to surveillance such as only monitoring from 9-5pm, but that does not completely solve the problem of Orwellian surveillance and ignores the flexibility that remote workers possess. Introna (2000) argues for "organizational justice" in the era of a "pervasive net of surveillance" (Introna, 2000). Similarly, Chen et. al (2007) argue for "procedural" and "distributive justice" for employees (Chen et al., 2007). Justice includes the right for employees to use their personal social media sites to campaign about a union-supported cause (TUC, 2017). Trade unions approach justice by searching for solutions that allow remote employees to help their managers understand their ability to work independently without excessive monitoring (Bloomberg, 2020).

Regulations

Companies have been encouraged to consider ethical data collection to maintain trust with their employees, but they have continued implementing excessive e-monitoring. Regulations are needed to enforce a baseline status quo. Over 65% of workers are concerned about discrimination stemming from unregulated surveillance (TUC, 2017). Surveillance for legitimate reasons such as system security is necessary (TUC, 2017). Regulations can enforce that only necessary data points are being collected, so employees can be assured that their interests are safeguarded by institutional means (TUC, 2017). Successful regulations are timeless to account for the dynamic technology environment, which is why they aim to be neutral to the particular technologies (Whitley, 2020). However, the Employment Practices Code can and should be up to date with emerging surveillance technologies (TUC, 2017). Budd and Colvin (2008) propose three indicators that allow employees to resolve trust issues around e-monitoring (Budd et al., 2008). These include efficiency of company resources, equality and anti-discrimination, and democratic decision-making processes (Budd et al., 2008). Regulations can serve as a vehicle to educate employees about their rights. Employee data only represents a part of their whole context, but employees need not justify their lives outside work, termed the "right to a private life" (TUC, 2017). Empowered remote employees prefer regulation that mandates information about e-monitoring initiatives before they are introduced, with a justification for their introduction, and a mandate that after-hours monitoring is illegal (TUC, 2017).

V. Framework to Access if Surveillance is Excessive

This paper has established that although employees resent and resist employee monitoring, employers do have justified business needs for a certain spectrum of surveillance. Now I explore a framework to ensure that reasonable employee privacy is considered. The notion of contextual integrity is key to making this distinction (Brey, 2005). Work meetings over video conferencing software are not usually considered private from an employer but "sustained intense surveillance" of personal phone calls without a justified business need and without prior consent can be considered "prima facie violations of privacy" (Brey, 2005). To determine if surveillance is excessive, both the context and the level of accountability need to be considered (Brey, 2005). The contents of personal phone calls should not be monitored, even on work hours, because these moments are generally considered private outside the office environment, and thus should remain private even inside the remote office environment (Brey, 2005). The hallmark of excessive surveillance is lack of control over one's personal situation. Control can be violated physically by monitoring movements, psychologically by a software snooping through confidential conversations, or if the employees cannot control the level of surveillance (Brey, 2005). These findings can

be classified into an overall "operationalized notion of privacy" (Brey, 2005).

The current state of affairs in the regulatory landscape at the US state level includes a California law that aims to "protect its citizens against privacy infringement of any nature...employers digging into employees' privacy after working hours violate these rights and might be accused in a court of law for privacy infringement" (Genova, 2009). Connecticut requires sharing info about e-monitoring, but that is the only state with such a law (Nockleby, 2002). At a federal level, the Fourth Amendment is only for the government as an employer, so corporations have no obligation (Nockleby, 2002). For non-government employers, the Electronic Communications Privacy Act (ECPA) still does not cover employees because they accept the terms and conditions of using their employer's system (Nockleby, 2002). In the EU, GDPR covers employee data and requires Data Protection Impact Assessments (DPIAs) (ICO, 2018).

The Information Commissioner's Office has a Code for Employment Practices that recommends including the justification for surveillance, understanding its psychological reactions on workers, finding the least privacy invasive mechanism for monitoring, providing transparency on how data will be applied in decisions, and not using surveillance data for other undisclosed reasons such as performance bonuses (TUC, 2017). As the European Court of Human Rights rightly says "private life is a broad concept that does not stop at the door of the workplace" (TUC, 2017). Therefore, invasive monitoring of private social media data or personal email accounts would need to be adequately justified, and business intelligence systems should not be permitted to make automated hiring and firing decisions based on employee data points (TUC, 2017).

VI. Conclusion

The current Covid-19 global pandemic demonstrates that remote working has gained a lot of traction and is here to stay. Workplace surveillance is another layer atop the already delicate relationship between a manager and an employee. Flexible working is a gray area without any hard and fast boundaries between home and work. Remote working is highly desirable for employees who would otherwise have a long commute, need to relocate, or have other parallel priorities such as caring for a dependent or child at home. Remote working is extremely desirable but involves sacrificing personal privacy to endure 24/7 employee monitoring as the cost of this freedom. The dark side of remote working is that employees are excessively monitored in the name of security of company-confidential information, but the data collected can be repurposed for electronic performance monitoring (EPM) (Jeske et al., 2015). The system is imbalanced in terms of power because employees are punished from their monitored data, but not rewarded. A recommended solution is using performance rewards as an incentive mechanism to drive employee acceptance of monitoring technology so both employers and employees can reap the benefits of surveillance data together (Jeske et al., 2015).

Bhave et al. (2020) term this "emerging entanglement of privacy contexts" where data privacy and physical privacy in the office are intertwined (Bhave, D. P., Teo, L. H., & Dalal, R. S., 2020). The double-edged sword of remote working is that the same technological solutions that allow remote working also enable employee monitoring. The literature suggests possible solutions from the employer's end such as blocking access to inappropriate websites on work laptops, co-creating employee monitoring systems with the perspective of employees designed into the system, and from the employee's end by encouraging end-to-end email encryption (Nockleby, 2002). I argue that remote employee acceptance of surveillance depends on the following factors - transparency on data collection from employers, clarification of data usage for system security or for hiring and firing decisions, and the avenues available for employee privacy concerns to be heard.

References

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

Allen, M., Coopman, S., Hart, J., Walker, K. (2007) "Workplace surveillance and managing privacy boundaries" Management Communication Quarterly (21) pp. 172-200.

Ball, K. (2010) "Workplace Surveillance: an overview" Labor History (51:1) pp. 87-106.

Bhave, D. P., Teo, L. H., Dalal, R. S. (2020) "Privacy at Work: A Review and a Research Agenda for a Contested Terrain" Journal of Management (46:1) pp. 127–164. https://doi.org/10.1177/0149206319878254

Bloomberg.com (2020) "Bosses Panic-Buy Spy Software To Keep Tabs On Remote Workers" [online] Available at: <https://www.bloomberg.com/news/features/2020-03-27/bosses-panic-buy-spy-software-to-keep-tabs-on-remote-workers> [Accessed 29 March 2020].

Bowcott, O., Rawlinson, K. (2017) "Romanian whose messages were read by employer had privacy breached" Guardian September 5. Retrieved from https://www.theguardian.com/law/2017/sep/05/romanian-chat-messages-read-by-employer-had-privacy-breached-court-rules.

Brey, P. (2005) "The Importance of Privacy in the Workplace" Privacy in the Workplace (eds. S. O. Hansson and E. Palm), Fritz Lang, pp. 97-118.

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

Chen, J., Ross, W. (2007) "Individual differences and electronic monitoring at work" Information, Community and Society (10:4) pp. 488-505, DOI: 10.1080/13691180701560002

Culnan, M.J. & Williams, C.C. (2009) "How Ethics Can Enhance Organizational Privacy: Lessons from the Choicepoint and TJX Data Breaches" MIS Quarterly (33:4) pp. 673- 687

D'Acquisto, G., Domingo-Ferrer, J., Kikiras, P., Torra, V., Montjoye, Y., Bourka, A. (2015) "Privacy by design in big data: An overview of privacy enhancing technologies in the era of big data analytics" 10.2824/641480.

Genova, G. (2009) "No Place to play: Current employee privacy Rights in Social Networking Sites" Business Communication Quarterly pp. 97-103.

Holmes, A. (2020) "Employees At Home Are Being Photographed Every 5 Minutes By An Always-On Video

Service To Ensure They're Actually Working — And The Service Is Seeing A Rapid Expansion Since The Coronavirus Outbreak" [online] Business Insider Available at: <https://www.businessinsider.com/work-from-home-sneek-webcam-picture-5-minutes-monitor-video-2020-3?r=US&IR=T> [Accessed 29 March 2020].

Horton, C. (2020) "Employee Tracking: Why Workplace Tech Demands Trust" [online] Raconteur. Available at: <https://www.raconteur.net/business-innovation/employee-tracking-workplace-tech> [Accessed 28 March 2020].

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

Ico.org.uk. (2018) "Data Protection Impact Assessments (Dpias) Guidance" [online] Available at: <https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/data-protection-impact-assessments-dpias-guidance/> [Accessed 10 April 2020].

Jeske, D., Santuzzi, A. (2015) "Monitoring what and how: Psychological implications of electronic performance monitoring" New Technology, Work and Employment (30) pp. 62-78. 10.1111/ntwe.12039.

Klopfer, P., Rubenstein, D. (1977) "The concept privacy and its biological basis" Journal of Social Issues (33) pp. 52-65.

Kofman, A., (2017) "The FBI Is Building A National Watchlist That Gives Companies Real-Time Updates On Employees" [online] The Intercept. Available at: <https://theintercept.com/2017/02/04/the-fbi-is-building-a-national-watchlist-that-gives-companies-real-time-updates-on-employees/> [Accessed 10 April 2020].

Nockleby, J., (2002) "Privacy In The Workplace" [online] Cyber.harvard.edu. Available at: <https://cyber.harvard.edu/privacy/Module3_Intronew.html> [Accessed 10 April 2020].

Nord, G., McCubbins, T., Nord, J. (2006) "E-Monitoring in the Workplace: Privacy, legislation, and surveillance software" Commun. ACM. (49) pp. 72-77. 10.1145/1145290.

Introna, L. (2000) "Workplace surveillance, privacy, and distributive justice" ACM SIGCAS Computers and Society (30) 10.1145/572260.572267.

Ozdemir, Z., Smith, H., Benamati, J. (2017) "Antecedents and outcomes of information privacy concerns in a peer context: An exploratory study" European Journal of Information Systems (26) 10.1057/s41303-017-0056-z.

Parks, R., Xu, H., Chu., C., Lowry, P. (2017) "Examining the intended and unintended consequences of organisational privacy safeguards" European Journal of Information Systems (26:1) pp. 37-65.

Pigni, F., Bartosiak, M., Piccoli, G., Ives, B. (2018) "Targeting Target with a 100 million dollar data breach" Journal of Information Technology Teaching Cases (8) pp. 9-23

Smith, W., Tabak, F. (2009) "Monitoring Employee E-mails: Is there Any Room for Privacy?" Academy of Management pp. 33-48.

Wicker, S. (2011) "Cellular telephony and the question of privacy" Commun. ACM (54:7) pp. 88–98. DOI:https://doi.org/10.1145/1965724.1965745

Stone-Romero, E., Stone, D., Hyatt, D. (2003) "Personnel selection procedures and invasion of privacy" Journal of Social Issues (59) pp. 343-368.

Topping, A. (2020) "Give People Right To Ignore Work Emails At Home, Says Long-Bailey" [online] The Guardian. Available at: <https://www.theguardian.com/politics/2020/feb/07/rebecca-long-bailey-labour-leadership-workers-rights-phones> [Accessed 29 March 2020].

Tuc.org.uk. (2017) "I'll Be Watching You" [online] Available at: <https://www.tuc.org.uk/research-analysis/reports/ill-be-watching-you> [Accessed 29 March 2020].

Vatcha, A. (2020) "Amy Vatcha: Employee Monitoring" [online] Available at: <https://apps.lse.ac.uk/mahara/view/view.php?id=2517> [Accessed 10 April 2020].

Whitley, E. (2020) "Week 5 Lecture: A Role for Technology? Approaches: How can we research Data Governance?" [online] LSE. Available at: <https://moodle.lse.ac.uk/course/view.php?id=3548> [Accessed 10 April 2020].