Employee Surveillance: A Fight Against Undue Workplace Monitoring

A Research Paper submitted to the Department of Engineering and Society

Presented to the Faculty of the School of Engineering and Applied Science

University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree

Bachelor of Science, School of Engineering

Matthew Walsh

Spring 2020

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Advisor

Sean M. Ferguson, Department of Engineering and Society

Employee Surveillance: A Fight Against Undue Workplace Monitoring

How do employers and employees negotiate the line between justified employee surveillance and unwarranted invasions of privacy?

According to Statista (2020), there are 4.66 billion active internet users globally. Companies collect online user data to study their customer base and to develop targeted advertising campaigns (Clement 2020). Among American internet users, most report they "have very little or no control over the data that government (84%) or companies (81%) collect about them" (Auxier et al., 2019). To thwart cyberattacks, companies and government agencies collect the online data of their customers and employees, but most Americans report that the risks of such data collection outweigh the benefits (Auxier et al., 2019). Employers use key stroke tracking, web activity tracking, and other surveillance methods to ensure that employees are not doing anything that they shouldn't be doing. Employers and employees compete to draw the line between necessary and invasive data collection.

Origins of a Surveilled Workplace

Workplace Surveillance has been around far longer than computers and the age of the internet. Managers in offices have always been able to easily watch their employees and ensure that work was being done correctly and efficiently. While the law varies by state, most offices have clearly defined laws regarding an employees' rights to privacy while in the workplace. As many workplaces are private companies, employers often have the legal right to enforce any type of surveillance. Before email, social media, and other internet related technologies, the extent of an employer's surveillance was mostly limited to the physical workplace. In rare cases, this surveillance may have reached into the personal lives of employees, but any extra surveillance

measures that occurred outside the workplace required hiring private investigators or other economically taxing procedures. Ajunwa, Crawford, and Schultz (2017) describe the surveillance used by Henry Ford in his factories: "[Ford] stalked the factory floor with a stopwatch, timing his workers' motions in a push for higher efficiency" and "hired private investigators to spy on his employees' lives away from the factory to discover personal problems that could interfere with their work." Clearly, these techniques would not be sustainable or possible with thousands of employees in large companies but employers have always wanted to ensure that their employees are always acting in the best interest of the company. As computers became widely used in the workplace, surveillance became easier. Currently, employers are legally entitled to have security cameras, monitor an employee's usage of computers or the internet, search an employee's belongings, test for substances, and more. In most cases, however, it is required by law that these policies are well defined and that employees are fully aware of any surveillance measures (UpCounsel, 2020).

As companies started using electronic filesystems and most work was done electronically, many tasks became more efficiently done. At the same time, employees had access to many more distractions in the workplace. With access to social media accounts, personal emails, and other private and social aspects of the internet from work computers, the distinct separation between an employee's private life and their personal life grew smaller. Employers use internet history, keystroke logging, and email history to monitor employee's use of computers. Employers now have the ability to see much further into the personal lives of their employees than ever before.

Among employees, about 70 percent suspect their employers "routinely monitor their behavior at work" (Wronski, 2019). To many employers, however, surveillance is necessary to

prevent data breaches, which cost companies an average of 3.86 million dollars at each occurrence (IBM, 2020). About 57 percent of these employees perceive monitoring as more harmful than beneficial (SHRM, 2020). Vendors of workplace surveillance systems, however, contend that employers must determine whether employees are "working hard or hardly working," and "who is accessing sensitive files or participating in risky activities" (InterGuard, 2020). Such companies promise their clients that with such systems, they can "monitor and control user activity to ensure compliance with internal security policies and regulatory requirements" (Teramind, 2020).

Employers must comply with the EPCA, the Electronic Communications Privacy Act of 1986, which limits workplace surveillance. Many state laws require employers to inform their employees of any monitoring policies (Mehl, 2020). The EPCA is largely outdated and has not been successful in keeping up with emerging technologies. Government surveillance laws exist in the constitution and apply to government employees, but private corporate entities are not required to abide by these laws. These private companies can employ any surveillance measure that they can defend in court. Most legislation comes from state governments, and these vary greatly across the United States (Ajunwa et al., 2017). Delaware and Connecticut, for example, require employers to inform workers when their email accounts are monitored but other states do not explicitly require this (Laird, 2020). Additionally, employees generally lose such rights, when they use employer's devices or accounts (PRC, 2019). For example, in *U.S. v. Hamilton* (2012), the court found that because an employee "did not take any steps" to protect his email on a company computer, he had abandoned his right to privacy (EPIC, 2012). U.S. courts are still determining the legal limits of employer surveillance of personal devices that employees use for work (Laird, 2020).

The United States Supreme Court heard two cases in 2010 and 2011 regarding employer surveillance. In 2010 in the case of City of Ontario v. Quon, the City of Ontario Police Department went before the Supreme Court to defend their auditing of text messages of Sergeant Quon. Quon had been sending messages from a Department issued pager to his wife and mistress, and had been audited when he surpassed the character limit set by the Department. The mistress sued the Department for a violation of privacy. The court ruled that the City of Ontario was within its rights to audit and read the messages sent, given that the pager was Department property and that the Department had informed all employees that they could be audited at any time (ASAP, 2010). The 2011 case, NASA v. Nelson, revolved around background checks that employees deemed as unconstitutional. The Supreme Court sided with NASA, but did say that NASA must keep all employee information private as part of the Privacy Act (EPIC, 2011).

Modern Surveillance in Action

A unique facet of modern workplace surveillance comes from wellness programs. Many companies award employees for being healthy, whether with better health insurance benefits, access to health and fitness programs, or other financial incentives. To track the perceived wellness of employees, some companies provide fitness trackers and other health-related technologies. While these types of programs encourage a healthier balance between work and private lives of employees, they are often invasive and quite subjective. Health data collected by wearable technologies such as Fitbits or Apple Watches is fully accessible by employers if the devices are property of the company. This leads to the potential for discrimination based on health related issues. Obesity and smoking are not classified as disabilities, and therefore are not protected by the Americans with Disabilities act of 1990 (Ajunwa et al., 2017). This means that

employees may feel pressured into participating in wellness programs or may fear losing their jobs if they are a smoker or are obese. Employees have very little legal backing to fight against such discrimination.

Many large companies such as Amazon, Walmart, and Google have been accused of using surveillance measures to monitor union activity among employees. While many of the threats have not been confirmed, unionization efforts have only increased in recent years. Amazon claims that unions would slow down communications between managers and employees, thus slowing down business operations. Employees, however, feel that they are helpless when negotiating for better wages and work conditions and more than 40% of Amazon employees support unionizing (Business Insider, 2021). In 2019, Bloomberg reported that Google introduced a software that would automatically flag any employees who scheduled meetings with "more than 10 rooms or 100 participants," which many suspect to be a way to identify any employees hoping to organize unionization efforts. At the same time, Google fired four employees who were active in organizing and subsequently hired a law firm known to handle anti-union cases.

As unionization remains out of reach at large corporations, many advocacy groups have gotten involved to fight for employee privacy and ensure that workers are aware of their rights. The American Civil Liberties Union (ACLU) contends that employer surveillance "often goes well beyond proper management concerns and becomes a tool for spying on employees in furtherance of no legitimate business interest" (ACLU, 2018). The ACLU resists such excesses, in part by ensuring that employees have access to legal counsel. The ePolicy Institute consults with companies to "maximize compliance, manage behavior, and minimize risks—including

litigation and regulatory investigations—through best-practices-based policies and employee training programs" (ePolicy Institute, 2020).

In March 2020, quarantines and lockdowns to prevent coronavirus transmission contributed to the biggest single-month increase in unemployment in the U.S. since 1975 (BLS, 2020). Many workers who kept their jobs shifted to remote work. According to the U.S. Bureau of Labor Statistics, 22.7 percent of laborers were working from home in September 2020; 37 percent of jobs may eventually shift to fully remote work (BLS, 2020). To monitor employees working from home, many employers now require access to workers' keystrokes, screens, and electronic communications, even on personal computers. To many employees, however, such practices are invasions of privacy.

The Harmful Effects of Surveillance

McParland and Conolly (2020) note that Jeremy Bentham's 1791 prison design, the panopticon, featuring "an observation unit" from which a warden could "observe any inmate in the unit at any time," mirrors remote workplace monitoring. In the same way that the prisoners could not tell when or if the warden was watching, remote workers may be unaware that companies "observe their employees and collate data on them" (McParland and Conolly, 2020). As the pandemic forced millions to shift from working in an office to working from home, employers scrambled put procedures in place that would help ensure employees weren't slacking at home. With strictly virtual interactions, managers could no longer simply walk around to ensure work was being done productively.

The decline in productivity caused by working in remote environments has been colloquially named Zoom fatigue. Throughout the pandemic almost all social and professional

environments semi-permanently moved to virtual settings. Many workers and students reported feeling far more exhausted when spending the day in front of their computer rather than in the office or at school. A Stanford report details the causes of Zoom fatigue, listing prolonged face-to-face encounters, more complex social cues, a decrease in mobility, and “an all day mirror” (Bailenson, 2021). By spending much more of the day in front of a camera speaking directly with coworkers, not only are the attendees of a virtual meeting looking at far more people at once than in a regular meeting, they are also much closer to each other than they would be in person. This amount of eye contact and lessening of personal distances can be psychologically taxing and may lead to fatigue. Additionally, small things such as conversation flow and reading of social cues become much more difficult in a remote environment. Humans are trained throughout their lives to learn the flow and progression of conversational interactions and many of the social cues that are easy to identify in person become much harder to recognize in a virtual environment. These modified social interactions, in addition to the potential stress caused by virtually looking into a mirror all day while confined to one solitary place, can lead to added fatigue and a possibility of reduced productivity.

A Voiter report from May of 2020 reports that employees who worked remotely reported a 1% decrease in overall productivity. A following report from the same source, however, showed that remote workers had overcome this reduction and in April of 2021, workers reported a 2% increase since the previous year, equaling a 1% net increase from in-person employment (Voiter, 2021). The sample sizes for these reports were rather small and the ratings of productivity were self-reported, meaning the data may not be statistically significant. However, these reports do show that after a year of working from home, many employees feel as though

they may no longer face the same impairments to productivity as they did at the beginning of the pandemic.

The perceived decline in productivity and motivation at the beginning of the pandemic led to a 55% increase in remote employment surveillance software, as managers feared that distractions at home would make it harder to stay focused. Internet searches related to remote employee surveillance surged by 1705% in April of 2020 (ZDNet, 2020). Currently, 45 percent of employees who work remotely believe that their employers monitor them (SHRM, 2020). Microsoft issued a patent for a software that would monitor virtual meetings and track things such as facial expressions and participant contributions to rate each employee on the productivity in the meetings. In response to public backlash, Microsoft removed any individualized assessments from the software (EPIC, 2020).

In the office, contact tracing has become ubiquitous to prevent the spread of the virus. Shoebridge (2020) contended that until a COVID-19 vaccine was widely available, employers would need to track and trace employees' locations to limit workers' exposure to the virus in the office. Contact tracing often comes in the form of GPS tracking to ensure that employees are not within close proximity to each other. An employee at State Street Bank in Boston says that employees working in the office must wear tracking lanyards at all times. These lanyards attach a tracking device that beeps loudly if any two employees are within 10 feet of each other and alert a compliance team about any violations of social distancing. A London Deloitte office uses PointGrab tracking software, which monitors which desks in offices are occupied and notifies managers when too many desks are full (CNN, 2020). In the case of an infection, these systems would allow employers to notify those who may have been in contact with that employee and may need to quarantine.

A somber example of workplace surveillance during the pandemic comes from Amazon warehouses. A 2020 lawsuit details Amazon's lack of responsibility in contact tracing COVID-19 infections. The lawsuit claims that Amazon discourages employees from taking any breaks from work stations to properly sanitize themselves or their environments, denies paid leave for mandatory quarantine, and accuses Amazon of "purposefully concealing information about who has contracted the virus from the coworkers who may have come into contact with it" (Public Justice, 2020). Amazon has been the center of many controversies regarding workplace monitoring. Workers in Amazon factories are monitored using scanners that track how many packages each employee processes in a given amount of time. These scanners also record how much break time the employees take and penalizes those that do not meet certain quotas.

As reported by Hanley and Hubbard for Open Markets, the rate of severe injuries in Amazon warehouses is up to five times greater than the average of the industry. This worrying statistic can be attributed to warehouse employees feeling "forced to work through the pain and injuries they incur on the job". Amazon's system will automatically warn employees if they fall below a certain rate of processing packages, though they do not inform employees as to the exact value of the expected rate. Many employees believe that the rate constantly changes. Additionally, the system may automatically terminate employees. The pressure of keeping up with an unknown rate and feeling compelled to skip breaks has been documented to lead to a decline in mental health, as Amazon warehouses made 189 emergency calls related to mental health emergencies from 2013 to 2018 (Hanley and Hubbard 2020).

Surveillance measures such as those implemented at Amazon warehouses can compromise employees' trust of their employers. Accenture (2019) found that monitoring diminishes trust among 52 percent of employees, estimating the consequences may cost

companies 3.1 trillion dollars globally. Zhang and Bock (2006) found that strict policies may limit job satisfaction as well. Berfstrøm and Svare (2017) use the definition from Lau et al. of "felt trust" to be "the trusted other's own perception of whether he or she is trusted by others". They state that while this is similar to trust, it is not the same. By trusting someone, you are willing to be vulnerable and expect them to act in a way that aligns with your own desires, but felt trust is to what extent you believe others would put trust in you. Berfstrøm and Svare continue to detail how electronic monitoring systems can impair the felt trust of employees, making them less likely to believe that their management deems them as trustworthy. A lack of felt trust can lead to a lack of "mastery" and "intrinsic motivation." In other words, employees who feel as though their employers do not believe they can successfully perform their job without supervision are less likely to excel in their fields or even be motivated to do so. Fichtner, Strader and Scullen (2013) argue that policies relating to the surveillance of electronic activities must be well defined and explicitly enforced via a "comprehensive written policy" to ensure that employees are held accountable for inappropriate use of company technology without a loss of trust.

Employers must grapple with the pros and cons of employee surveillance. On one hand, they are vulnerable to data breaches, scandals, or loss of productivity caused by unsupervised employees using work time to check social media or surf the internet. But on the other hand, employing surveillance measures could cause workers to lose trust and motivation, losing the companies not only money but loyalty from employees. It is clear that any form of surveillance policy must be clearly defined and well publicized. Though lawsuits are piling up against large corporations, no changes have been made to legislation regarding the protection of employees rights. The law seems to side with private companies rather than workers and Amazon is a great

example of how employers have taken advantage of this. Employees are put in a difficult situation, especially during crises such as the COVID-19 pandemic, where they are forced to choose between measures that may infringe upon their personal privacy and quitting or losing their job. This struggle helps nobody. If employees are consulted before surveillance measures are put in place, they will be more understanding of the causes and motivations behind such measures and can inform their managers to any discomforts. For employers, not only does this help retain trust, but it also places a safe legal barrier if employees violate these guidelines. Modern legislature must be put in place to develop a distinct boundary between the personal lives of employees, cyber or otherwise, and the employer's surveillance. With clear laws and regulations from both employers and governing bodies that constantly change to account for social and technological changes, workers will have more space to advocate for and maintain privacy. Without these changes, the divide between employees and employers will only continue to grow and both parties will suffer.

References

Accenture. (2019, January 21). More Responsible Use of Workforce Data Required to Strengthen Employee Trust and Unlock Growth, According to Accenture Report. https://newsroom.accenture.com/news/more-responsible-use-of-workforce-data-required-to-strengthen-employee-trust-and-unlock-growth-according-to-accenture-report.html

ACLU (n.d.). American Civil Liberties Union. The Rise of Platform Authoritarianism. https://www.aclu.org/issues/privacy-technology/surveillance-technologies/rise-platform-authoritarianism

Ajunwa, I., Crawford, K., & Schultz, J. (2017). Limitless Worker Surveillance. *California Law Review, 105*(3), 735-776. Retrieved April 14, 2021, from http://www.jstor.org/stable/44630759

Auxier, B., Rainie, L., Anderson, M., Perrin, A., Kumar, M., & Turner, E. (2020, August 17). Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information. https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/

Bailenson, J. (2021, February 23). Nonverbal overload: A theoretical argument for the causes of ZOOM Fatigue · Volume 2, Issue 1. https://tmb.apaopen.org/pub/nonverbal-overload/release/1

BLS (2020, June 1). U.S. Bureau of Labor Statistics. Ability to work from home: Evidence from two surveys and implications for the labor market in the COVID-19 pandemic : Monthly Labor Review. (2020, June 01). https://www.bls.gov/opub/mlr/2020/article/ability-to-work-from-home.html

Brown, E. (2020, November 16). Employee surveillance software demand increased as workers transitioned to home working. https://www.zdnet.com/article/employee-surveillance-software-demand-increased-as-workers-transitioned-to-home-working/

Clement, J. (2020, October 29). Internet users in the world 2020. https://www.statista.com/statistics/617136/digital-population-worldwide/

Durkee, A., Lutz, E., & Bilton, N. (n.d.). Google's alleged union busting is now under federal investigation. https://www.vanityfair.com/news/2019/12/google-investigation-national-labor-relations-board-union-firings

Electronic Communications Privacy Act of 1986 (ECPA). (2019, April 23). https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1285

Employee privacy rights: Everything you need to know. (n.d.). https://www.upcounsel.com/employee-privacy-rights

EPIC (2012, Dec. 13). Electronic Privacy Information Center. United States v. Hamilton. https://epic.org/amicus/hamilton/

ePolicy Institute. (n.d.). Welcome to The ePolicy Institute. http://www.epolicyinstitute.com/

Fichtner, J., Strader, T. J., & Scullen, S. E. (2013). *Creating, Clarifying, and Enforcing an Effective Non-work Related Computing Policy: A Legal Perspective* (Rep.). Penn State University Press. JSTOR

Gordon, P., Drake, D. (2010). U.S. Supreme Court Ruling Provides Guidance on Monitoring Employee Texts and E-Mails. (2010, June 10). ASAP. https://www.littler.com/files/press/pdf/2010_06_ASAP_USSupremeCourt_GuidanceEmployeeEmailTexts.pdf

Hanley, D. A., & Hubbard, S. (2020, September). Eyes Everywhere: Amazon's Surveillance Infrastructure and Revitalizing Worker Power. https://static1.squarespace.com/static/5e449c8c3ef68d752f3e70dc/t/5f4cffea23958d79eae1ab23/1598881772432/Amazon_Report_Final.pdf

Hartmans, A. (2021, March 29). Amazon workers in Alabama have a few hours left to vote on whether to join a union. Here's how unions work and why many companies oppose labor organizers. https://www.businessinsider.com/union-definition-why-companies-amazon-oppose-labor-organizing-workers-rights-2021-3

IBM. (2020). Cost of a Data Breach Study. https://www.ibm.com/security/data-breach

Interguard. (2020) Remote Employee Monitoring & Productivity Tracking Software. (2020, October 06). https://www.interguardsoftware.com/?utm_campaign=brand

Kampmark, B. (2020). The pandemic surveillance state: An enduring legacy of COVID-19. *Journal of Global Faultlines, 7*(1), 59-70. doi:10.13169/jglobfaul.7.1.0059

Kneese, T. (2014, October 8). Workplace Surveillance. https://www.researchgate.net/publication/326121856_Workplace_Surveillance

Laird, L. (2020, June 23). What Are Your Privacy Rights When You Work From Home? https://www.legalzoom.com/articles/what-are-your-privacy-rights-when-you-work-from-home

McParland, C., & Connolly, R. (2020). *Dataveillance in the Workplace: Managing the Impact of Innovation* (Rep.). Dublin, Ireland: Dublin City University Business School.

Mehl, B. (2020, August 13). The State of Employee Privacy and Surveillance in 2020. https://www.getkisi.com/blog/state-employee-privacy-surveillance

Moore, A. (2000). Employee Monitoring and Computer Technology: Evaluative Surveillance v. Privacy. *Business Ethics Quarterly, 10*(3), 697-709. doi:10.2307/3857899

Palmer, A. (2020, October 24). How Amazon keeps a close eye on employee activism to head Off unions. https://www.cnbc.com/2020/10/24/how-amazon-prevents-unions-by-surveilling-employee-activism.html

PRC (2019, June 27.) Privacy Rights Clearinghouse. Somebody's Watching Me: Employee Surveillance. https://privacyrights.org/resources/somebodys-watching-me-employee-monitoring

Provision Living. (2020, June 25). Smartphone Screen Time: Baby Boomers and Millennials. https://www.provisionliving.com/news/smartphone-screen-time-baby-boomers-and-millennials

Scott, K. (2020, October 23). Smart sensors could track social distancing in the office. https://www.cnn.com/2020/10/23/tech/pointgrab-sensors-social-distancing-office-spc-intl/index.html

Shoebridge, M. (2020). *Returning to work during the pandemic: Testing, surveillance, apps and data as our near term future* (Rep.). Australian Strategic Policy Institute. JSTOR

Spiggle, T. (2020, May 21). Can employers monitor employees who work from home due to the coronavirus? https://www.forbes.com/sites/tomspiggle/2020/05/21/can-employers-monitor-employees-who-work-from-home-due-to-the-coronavirus/?sh=14ed39ae2fb7

Turner, J. (2020, June 3). Amazon Workers and Their Family Members File Suit for Workplace Policy Changes to Stop Community Spread of COVID-19. https://www.publicjustice.net/wp-content/uploads/2020/06/Amazon-JFK8-Lawsuit-Press-Release-FINAL.pdf

Teramind. (2020, November 01). https://www.teramind.co/?utm_source=Google

United States Patent & Trademark Office (2020). *Meeting Insight and Computing System. http://appft.uspto.gov/netacgi/nph-Parser?Sect1=PTO1&Sect2=HITOFF&d=PG01&p=1&u=/netahtml/PTO/srchnum.html&r=1&f=G&l=50&s1=%2220200358627%22.PGNR.&OS=DN/20200358627&RS=DN/20200358627*

Vincent, J. (2021, March 24). Amazon delivery drivers have to consent to AI surveillance in their vans or lose their jobs. https://www.theverge.com/2021/3/24/22347945/amazon-delivery-drivers-ai-surveillance-cameras-vans-consent-form

Wettemann, R. (2020, May 25). Working at home is working. https://valoir.com/blog-1/working-at-home-is-working

Wettemann, R. (2021, April 06). Work from home: One year in. https://valoir.com/blog-1/work-from-home-one-year-in

Wronski, L. (2019, October 25). Axios poll: Workplace surveillance. https://www.surveymonkey.com/curiosity/axios-poll-workplace-surveillance/

Zhang, C., & Bock, G. (2006). *Why Employees Do Non-Work-Related Computing: An Investigation of Factors Affecting NWRC in a Workplace* (Rep.). Pacific Asia Conference on Information Systems. JSTOR

Zielinski, D. (2020, August 08). Monitoring Remote Workers. https://www.shrm.org/hr-today/news/all-things-work/pages/monitoring-remote-workers.aspx