Workplace Surveillance: Employee fired from his job, not by his manager but by a machine

Author: Tapiwa Gomo . October 2019

Tawanda is successful for a front desk position. The benefits will enable him to buy his dream car in 8 months' time from time to inception. He beat out hundreds of other applicants for the opportunity to be with this corporation. However, his enthusiasm for his first day begins to diminish. The more he learns about the internal affairs and procedures from the induction process, the more concerned he becomes.

Before Tawanda can even set foot in the on his office chair, he must undergo an extensive physical examination, which also includes the insertion of an implant in the back of his right hand. Any devices—such as smartphones or tablets—must be checked in at the security desk and have Wi-Fi enabled. ID badges with credit card chips, personal data, and GPS trackers must wear from the neck and the information scanned must match the data on the implant. He is also equipped with a company-issued earpiece and microphone to monitor everything he says and hears.

Tawanda must also sign a waiver permitting the company access to his automobile at all times and allow the company to install an additional GPS tracking unit to monitor its location at all times. Reluctantly, he accepts the terms. He hopes he made the correct decision to give up every aspect of his privacy. He hopes the company does not use all the collected data against him. Is this just a singular company's attempt to control and monitor every single one of its employees? Is this their way to prevent dishonesty, frivolous lawsuits, and stealing? Is this something darker? What happens when surveillance goes beyond opening postal mail and shooting video? Is this the new reality in the workplace?

Monitoring employees is nothing new in the workforce. Telephone monitoring has been around for decades. Even toll-free phone calls often start with the disclaimer: "This call may be recorded for quality assurance." Today's workplace surveillance began with email and phone monitoring but now includes keeping track of web-browsing patterns, text messages, screenshots, keystrokes, social media posts, private messaging apps like WhatsApp and even face-to-face interactions with co-workers.

Employer's perspective

In order to increase efficiency, measure productivity, decrease risk, and generally maximize profits, many private enterprises monitor their employees. Monitoring prevents workers from slowing or sabotaging the modes of production, both in factories and in offices. In an aim to find out what structures and technologies can ensure efficiency and integrity in the organization of business and labour, Frederick Winslow Taylor, a measurement-obsessed mechanical engineer, developed a theory that he names after himself. His mission was to map out the knowledge of how a task is by identifying, fragmenting and regimenting workflows and to deploy methods of "performance monitoring" to reach production targets (Sewell, 2005). The worker's knowledge of and control over the work is thus

removed from the worker and its execution is rationalized into discrete piecework that is organized and overseen by the manager in an increasingly scientific process (Braverman, 1998). This implies the probability that a worker can sabotage production without the manager realising tends to be close to zero.

The rule of the Taylor system is that **the unobserved worker is an inefficient one** (Saval, 2014). This is the principle used by majority of monitoring systems at workplaces. To monitor productivity, software can measure proxies such as the number of emails sent, websites visited, documents and apps opened and keystrokes. Over time, it can model a picture of typical user behaviour and then alert when an individual deviates.

If it is normal for you to send out 13 emails, type 6,500 keystrokes and be active on a computer for three hours a day, if all of a sudden, you are only active for one hour or typing 1,000 keystrokes, there seems to be a dip in productivity. If you usually touch 10 documents a day and print two and suddenly you are touching 500 and printing 200 that may mean you're stealing documents in preparation of leaving the company.

Employee's perspective

Surveillance technologies can be used in many ways to create a sense of security for workers, and the public. "Sousveillance" is the term that describes how those who are typically watched by a more dominant power from above can turn the surveillance gaze on their overseer from below. For example, British police installed CCTV cameras into the area where the "Yorkshire Ripper" murders of prostitutes occurred in the 1970s and '80s, hoping to scare prostitutes from their place of work (Sewell, 2014). Instead, prostitutes gathered in front of the cameras so that their departures from the street and into a vehicle would be time-stamped, and the license number or other details of the driver would be recorded in case anything bad happened to them.

Can we trust the accuracy of this technology?

Using smartphones, fitness bracelets and a custom app, researchers at Dartmouth have created a mobile-sensing system that evaluates employee performance. The system works by monitoring the physical, emotional and behavioural well-being of workers to classify high and low performers. They found that the system could correctly distinguish the difference between low- and high-performing employees only 80% of the time. What about the other 20%? Are those workers misjudged and targeted erroneously? It seems possible.

In 2018 there was an incidence that proved that surveillance technologies have flaws. A worker was fired after an AI system flagged his profile after the manager forgot to renew the employee's contract (BBC News, June 2018). Ibrahim Diallo was fired from his job, not by his manager but by a machine. The news has many such reports over firings due to AI-based interferences. This is not simply a matter of employee privacy, but also a matter of deferred responsibility. If HR departments are willing to forgo some amount of paperwork and allow potentially flawed programming to make decisions, then the whole process becomes easier but also more susceptible to error.

Do both parties agree?

There is an unchallenged assumption that employers monitor their employees simply because they can, and that they do so more intrusively for the same reason— especially as technologies evolve to enable more and more methods of surveillance. As it stands, the literature indicates that there is not a point of give and take consent amongst all parties involved; instead, there is a mutual understanding in acknowledging what is happening as the boundaries of what is possible to what is permissible and what is a violation. What are the privacy anxieties that workers have about the surveillance data that is collected on them? How could it sway their future job prospects?

Numerous other questions emerge as well: to what level are these new tools aggravating a power differential between employers and employees? What constitutes “labour” and what divides it from home life? When the spatial constraints of a physical location can no longer demarcate labour, what are the new frameworks we have to consider when thinking about labour and its protections? In addition, what should we be measuring to understand what is happening? These questions represent significant gaps in the literature on workplace surveillance that justify attention and thoughtful consideration.

https://thehumancapitalhub.com/articles/Workplace-SurveillanceEmployee-Fired-From-His-Job-Not-By-His-Manager-But-By-A-Machine