Shared without the student's name, with permission.

CS 4001, Fall 2014

Term Paper

Ethics of Workplace Surveillance

Introduction

According to Marx (1999) we are "increasingly measuring everything that moves." It is true that rate of data collection in the world is growing exponentially, which is a cause of concern among privacy advocates (King, 2011). In this paper I will specifically discuss ethical concerns surrounding data collection for the use of surveillance on employees in the workplace, which has been a growing trend over the past thirty years. This trend has been supported by the increase of computers and various other technologies that make surveillance easy and cheap (Lasprogata, 2004).

For the purposes of this analysis I will use the term workplace surveillance to mean going beyond the typical surveillance necessary to protect the safety of employees and prevent theft of company equipment. Specifically, it is surveillance carried out by employers on employees to monitor their productivity. Introna (2002) defines it as "the multiplicity of formal and informal practices of monitoring and recording aspects of an individual or groups' behavior 'at work' for the purposes of judging these as appropriate or inappropriate; as productive or unproductive; as desirable or undesirable; and so forth".

According to the 2007 American Management Association's survey of 526 companies, 66 percent monitor Internet connections and websites visited, 45 percent monitor keystrokes and time spent at the keyboard, 43 percent store and review files saved to the computer, and 43 percent monitor employee email. Of the companies that monitor email, 40 percent assign an individual to manually read it. These percentages are astoundingly high and stimulate an intriguing ethical debate over the rights of employees in the workplace. In this paper I will discuss the controversy surrounding workplace surveillance from both sides of the argument and provide my own thoughts and on the matter.

Common Methods of Surveillance Used

There are many ways in which workplace surveillance limits and potentially infringes upon the privacy of employees. Bustard (2013) identifies three categories of workplace surveillance: monitoring of non-work use of technology, monitoring and tracking employees while they work, and out-of-work hours monitoring. These distinctions are useful in the language of workplace surveillance because each has a different reason for why it is carried out and has different ethical concerns associated with it.

Monitoring the use of technology for non-work-related purposes is the most common form of workplace surveillance (American Management Association, 2007). Its purpose it to ensure company property is not being misused for purposes such as slacking off or conducting personal business. Examples of this type of monitoring include video surveillance, scanning or reading e-mails, eavesdropping on or recording phone calls, monitoring keystrokes, recording web sites visited, and monitoring files accessed. The major ethical concern when conducting surveillance of this type is the privacy of the employee. The potential for revelation of sensitive employee information, most notably, information that may revealed in a personal phone call or email, is very high in this form of surveillance (Bustard, 2013).

Monitoring and tracking employees while they work is the second most common of Bustard's three workplace surveillance distinctions (American Management Association, 2007). This form of monitoring is intended to make sure employees are on task when they should be. Examples include recording how long tasks take or how many were completed, monitoring how much time is spent working versus on break, and location tracking (Bustard, 2013). Many of the concerns raised over this form of monitoring address the physical and mental health of the employee. Some privacy advocates argue that employees' knowledge of the relentless surveillance that judges their performance leads to extreme stress which can cause mental or physical harm (Fazekas, 2004).

A less common and highly controversial form of workplace surveillance is the monitoring of employees during out-of-work hours. The intent behind this practice is to ensure employees are representing the company's ideals and standards in their everyday lives. A common example of this type of surveillance is monitoring employees' social media accounts. Some companies even go as far as requesting the passwords to social media accounts before interviewees are eligible for hire (Knowledge Center 2012, Yahoo 2012). This form of surveillance is the most controversial because it involves monitoring employees' personal lives and using this information to judge their performance or worth in the workplace. Privacy supporters find this practice unnecessarily invasive and would argue an employee's personal life should not reflect on their professional life (Knowledge Center, 2012).

Arguments for Workplace Surveillance

Although workplace surveillance can certainly become too invasive and infringe on the rights of employees, to some extent employers have the right to ensure their employees are on task and not misusing company property. In this section I will discuss the most common arguments in favor of workplace surveillance.

Since employers pay employees either hourly or based on a workweek with a set number of hours, it is acceptable for them to expect full and undivided attention during business hours. After all, if an employee is using large amounts of company time for personal business or doing unproductive tasks like surfing the web, are they not indirectly stealing money from their employer? Just as we use CCTV cameras to protect against theft of physical items, a company can use surveillance to protect against employee theft of paid time.

Bustard (2013) notes a common argument of workplace surveillance supporters, which states that employees chose their employers and can leave at any time. Similar to the free market approach to consumer privacy, a subscriber to this theory would argue that if an employee does not like the surveillance practices of a particular company, he or she could choose not to work there. The problem with this argument is that employees often have a very limited choice of where they can work. If given the choice between a job with policies they do not agree with or being jobless, most people would reluctantly choose the job. Not everyone is in a financial position to turn down a salary if no other options exist.

Desprochers (2001) highlights the argument that employee knowledge of workplace monitoring may increase motivation in the workplace. While this may be true to some extent, it is important to look at the psychological effects of workplace monitoring on employees. I would argue that motivation through fear is not the best approach to inspire employees to perform at their best.

Mitrou (2006) brings up the issue of employer liability as a justification for workplace surveillance. He claims that an employee may use Internet access and email to disclose company trade secrets or private information, perform fraud, or complete other illegal tasks. These actions could have a significant impact on the well-being and reputation of the company. While being generally opposed to workplace surveillance, Mitrou (2006) concedes “undoubtedly, an employer has a legitimate right and interest to run his/her business efficiently and the right to protect his/her property and himself from the liability or the harm that employees’ actions may cause.” I would agree that this is a fair argument in support of surveillance because of the irreparable damage a single disgruntled employee could cause an organization.

In his attempt to find a balance between workplace monitoring and privacy, Sewell (2012) discusses the issue in two different grammars, one of which he calls “Care” which has a more favorable view of workplace surveillance. From this viewpoint, he explains workplace surveillance as a means to create a fairer environment between employees. Surveillance could expose underperforming workers who may be harming the reputations of fellow coworkers. It could also expose unfair practices like favoritism and nepotism. In this way the employer would be using “surveillance as a means of policing the contractual arrangement between principal and agent to minimize opportunistic behavior” (Sewell, 2012). I believe this to be an interesting analysis of workplace monitoring, but believe Sewell’s “Coercive” model of monitoring, which is discussed in the next section, is more applicable.

Arguments Against Workplace Surveillance

In opposition to the model of “Care” for discussing workplace surveillance, Sewell (2012) also discusses a language he refers to as the “Coercive” model of surveillance. In this description, he expresses surveillance as a means of control and manipulation. He suggests that the monitored employee will almost always be against forms of workplace surveillance because it has the effect of “intensifying work, reducing autonomy, increasing stress, and undermining solidarity by pitting worker against worker” (Sewell, 2012).

Bustard (2013) points out that the level of workplace surveillance is often much higher than the level of surveillance carried out by the Unites States government. He questions why workplace surveillance is not held to the same standards. I think this is particularly interesting when you consider that government surveillance exists primarily to prevent disasters that could claim many lives. It is unusual that there are stricter regulations on this form of monitoring than those imposed on employees of a private company.

Probably the most common argument against workplace surveillance is that it reveals the potential for employers to find sensitive information on their employees (Bustard, 2013). By reading employees' emails or listening in on phone calls, employers may be reading or eavesdropping on sensitive data. While employees should use reason before discussing personal information on company time or while using company equipment, it does not seem fair that an employer could access potentially sensitive information that employees would wish to keep private. Some people may have no choice but to get certain personal business done, such as scheduling medical appointments, during work hours.

Another common argument against employee monitoring is what is known as the "panoptic effect." This name of this phenomenon comes from the concept of the Panopticon which was a prison designed to allow a guard to watch all inmates without their knowledge (Botan, 1996). The "panoptic effect" refers to an imbalance of power that allows several people to spy on a large group that cannot have any expectation of privacy (Botan, 1996). Allen (2007) also discusses this effect and suggests that the pressure of being constantly under surveillance ultimately leads to stress and break of trust. This is discussed more in the following section where I examine several studies on the effects of workplace monitoring.

Research Conducted

Because of the growing concern over the increase of workplace surveillance, many studies have been conducted to monitor its effect on employee behavior, mentality, and physical health. The results of many of these studies show that excessive employee monitoring can have detrimental effects on the health of employees under surveillance.

People tend to change their behavior when they know they are being watched. Ball (2011) discusses a study conducted on a call center with results that suggest the surveillance program did not improve employee motivation, but actually led to the opposite. Researchers found that knowledge of monitoring led employees to exploit the system in order to appear more productive (Ball, 2011). Additionally, employees tended to oppose surveillance either by sabotage or by ‘effort bargaining,’ which is rationalization of slacking off due to perceived infractions (Ball, 2007). Allen (2007) discusses a similar phenomenon in a related study, which he refers to as the “chilling effect” where employees changed their behavior in response to being monitored.

Excessive monitoring in the workplace seems to cause harm to employee health. Fazekas (2004) discusses a study in which workers whose communications were monitored were at greater risk for mental health problems. The employees involved suffered from higher rates of depression, anxiety, and fatigue than those who were not monitored. Marmot (1991) suggests that excessive surveillance can affect not only mental health, but also physical health as well. He references a study that shows a lack of control within the workplace influenced relative life expectancy, which usually presented itself as an increased risk of heart disease. He suggests that a close supportive relationship with a manger is healthier and less stressful than judging an employee’s work remotely and secretly.

Extreme surveillance practices can also have adverse effects on the parties conducting the surveillance. Lammers (2010) shows that as individuals feel more powerful, they are motivated to judge others more harshly and are also more likely to engage in practices they would describe as immoral. This can lead to a scenario where the people carrying out the surveillance eventually escalate to more immoral and invasive monitoring which can lead to the aforementioned health problems for employees.

Current Legislation and Court Cases

In general, legislation in the United States has few restrictions on employer surveillance and court cases tend to side with the employer. It is important to note that the United States Constitution outlines some privacy considerations that limit surveillance, but that these limitations only apply to surveillance carried out by the government (Mitrou, 2006). There are not many concrete laws that limit what forms of surveillance are acceptable in the workplace. In many cases an employer simply must inform employees of any monitoring policies (Mitrou, 2006).

A critical case in the United States that set many legal standards for workplace surveillance was the case of McLaren v. Microsoft. In this case McLaren sued Microsoft for violation of privacy after the company read his personal emails, which he stored in a password-protected folder in his inbox. The Texas Court of appeals ruled that Microsoft did not violate McLaren's privacy by reading these messages because he used company time and equipment to send and store them (Mitrou, 2006). According to the ruling, the messages "were not McLaren's personal property, but were merely an inherent part of the office environment" (Desprochers and Roussos, 2001). There are a number of similar cases in the United States that suggest employees have little to no right to privacy while in the workplace.

Compared to the Unites States, the European Union has much stricter and more concrete regulations that limit workplace surveillance. Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms explicitly states “everyone has the right to respect for his private and family life, his home and his correspondence”. Unlike the privacy mentions in the US Constitution, these laws apply to the employer and employee relationship (Mitrou, 2006). The Charter of Fundamental Rights of the European Union adds “protection of personal data” as a right. In the European Union, employers must explicitly state the data being collected, the purpose for its use and collection, as well as obtain consent from all employees involved (Mitrou, 2006).

The case Onof v.Nikon France, stands in direct contrast to the ruling of McLaren v. Microsoft. In a similar situation, Nikon read Onof’s personal emails that were sent on company time using company equipment. In this scenario, the French court decided that the interception of personal email was a violation of Article 8, even though those emails were sent and received by misusing company equipment. (Mitrou, 2006) Halford v. United Kingdom resulted in a similar ruling, but in regard to listening in on telephone calls (Mitrou, 2006). Together these two cases made it clear that Article 8 applies to employees while at work in the European Union.

How much Surveillance is Acceptable?

It is clear that due to its prevalence, workplace surveillance is not going to be discontinued any time soon. Surely though, it should be restricted to an amount that allows employers some level of protection but does not dehumanize its employees.

Introna (2002) uses the philosophies of Levinas to argue that workplace surveillance is unethical but he then provides several suggestions for its practice. He insists that workplace surveillance is not a solvable ethical problem and that its practice must start by accepting the fact that it is unethical and unfair. After accepting this fact, every judgment made from the data must be treated as suspicious and that the monitored must be allowed to explain themselves (Introna, 2002). While this is a useful starting point, I believe some additional considerations would be more useful.

Bustard (2013) notes the unfair and asymmetrical nature of workplace surveillance but poses several suggestions to help balance the privacy of the employee with the security of the employer. First, he suggests monitoring should be obvious, as secret monitoring is undoubtedly morally wrong. Second, he suggests that monitoring should only be used to examine commercial factors and never aspects of an employee's personal life. I believe following these rules would be a good starting point for maintaining some level of employee privacy in the workplace.

In his theory of justice, Rawls (1971) notes that in order to maintain fairness, judgment must be administered by "disinterested parties who are subject the normal checks and balances of the democratic state." Ideally only third parties would only administer workplace surveillance, but for obvious security reasons, this is not always possible. Certainly though, managers should attempt to remain impartial in their monitoring. For this reason, I would add this point to the rules proposed by Bustard to form three workable rules for workplace surveillance.

Like many ethical problems, there is no clear distinction between right and wrong in the case of workplace surveillance. For this reason, we cannot simply propose a set of rules that will solve the problem. Sewell (2012) proposes ten questions that we should keep in mind when designing an employee surveillance system. These are useful questions that should be asked and answered by an employer before implementing a monitoring policy and can help evaluate its worth and invasiveness. In my opinion, the three aforementioned rules in conjunction with Sewell's following ten questions pose a workable model for analyzing the fairness of a workplace surveillance system.

i. Do we really need to measure this aspect of performance?
ii. Are we measuring the right things?
iii. Does performance measurement really lead individuals to modify their behavior in desirable ways?
iv. Is it focused on the right people?
v. Is it accurate?
vi. Have we got the balance right between intrusiveness and protection?
vii. Do we believe that we will get useful feedback from the system of surveillance?
viii. Will such feedback be used to improve our performance and give fair rewards or will it be used to discipline and punish?
ix. Has management forced the alleged benefits of performance measurement upon the employees or were they consulted in the process?
x. How much choice do employees have about the extent to which they are monitored?

Concluding Remarks

As jobs are becoming more computer-based and technology intertwined, workplace surveillance to determine employee productivity is becoming increasingly easier. I certainly do not agree with excessive workplace surveillance, but I recognize that employers should be afforded some rights to ensure employees are on task and protect themselves against sabotage. Because the United States provides little legislation about what forms of surveillance are acceptable, it is often hard to discern when a company is crossing a line with its level of surveillance.

I have discussed the ethical controversy of workplace surveillance from both sides of the argument and have suggested a set of guidelines that help to judge the morality of a particular surveillance system. The guidelines inspired by Rawls, Ball, and Sewell are not hard-set rules but can open a dialog to help to determine if a system is too invasive or if it is more invasive than useful.

References

Allen, M. W., Coopman, S. J., Hart, J. L., & Walker, K. L. (2007). Workplace surveillance and managing privacy boundaries. *Management Communication Quarterly*, *21*(2), 172-200.

American Management Association. (2007). 2007 Electronic Monitoring and Surveillance Survey. Available from www.amanet.org

Ball, K. S., & Margulis, S. T. (2011). Electronic monitoring and surveillance in call centres: a framework for investigation. *New Technology, Work and Employment*, *26*(2), 113-126.

Botan, C. (1996). Communication work and electronic surveillance: A model for predicting panoptic effects. *Communications Monographs*, *63*(4), 293-313.

Bustard, J.D. (2013). Ethical Issues Surrounding the Asymmetric Nature of Workplace Monitoring. In *Human Aspects of Information Security, Privacy, and Trust* (pp. 226-235). Springer Berlin Heidelberg.

Dickerson, N. (2012). Employers Continue to Ask for Facebook Passwords – States Take Action. *Knowledge Center*. Retrieved from http://knowledgecenter.csg.org/kc/content/employers-continue-ask-facebook-passwords-states-take-action

Desprochers, S., Roussos, A., 2001. The jurisprudence of surveillance: a critical look at the laws of intimacy. Working Paper*, Lex Electronica* 6(2).

Fazekas, C. P. (2004). 1984 is still fiction: Electronic monitoring in the workplace and US privacy law. *Duke L. & Tech. Rev.*, *2004*, 15-15.

Introna, L. D. (2002). Workplace surveillance 'is' unethical and unfair. *Surveillance & Society*, *1*(2), 210-216.

King, B. (2011). Too Much Content: A World of Exponential Information Growth. *The Huffington Post*. Retrieved from http://www.huffingtonpost.com/brett-king/too-much-content-a-world-_b_809677.html

Lasprogata, G., King, N. J., & Pillay, S. (2004). Regulation of electronic employee monitoring: Identifying fundamental principles of employee privacy through a comparative study of data privacy legislation in the European Union, United States and Canada. *Stan. Tech. L. Rev.*, *2004*, 4-4.

Marx, G. T. (1999). Ethics for the new surveillance. In C. J. Bennett & R. A. Grant (Eds.), Visions of privacy: Policy choices for the digital age (pp. 39–67). Toronto, Ontario, Canada: University of Toronto Press.

Mitrou, L., & Karyda, M. (2006). Employees' privacy vs. employer's security" Can they be balanced?. Telematics and Informatic, 23(3), 164-178.

Rawls, J. (1971). *A Theory of Justice*. Harvard University Press.

Sewell, G., Barker, J. R., & Nyberg, D. (2012). Working under intensive surveillance: When does 'measuring everything that moves' become intolerable?. *human relations*, *65*(2), 189-215.

Valdes, M. (2012). Job seekers getting asked for Facebook passwords. *Yahoo Finance*. Retrieved from http://finance.yahoo.com/news/job-seekers-getting-asked-facebook-080920368.html