# An Insight On The Use Of Employee Monitoring Software In The Workplace

Tommaso Liardo

40452307

40452307@live.napier.ac.uk

Word count: 2042

# Abstract

*The aim of this paper is to discuss some of the key arguments regarding the use of employee monitoring software by employers: productivity, employer and employee security, legality, trust, privacy. These arguments are not conclusive and each one presents an important moral consideration. Each argument is discussed with consideration to moral issues backed by previous studies, surveys, and research. It was found that despite the various legal and moral concerns, employee monitoring can turn out to be objectively beneficial to everyone involved, but only if done with the proper limitations and with careful training and explanation, otherwise it can easily become an issue that can potentially cause more financial and legal losses than the ones it is introduced to prevent.*



**Keywords:**

*Employee monitoring, Privacy, EMS, Technology, Security*

# Summary

# 1. Introduction

The increased development of technology has led organisations to implement employee monitoring software in the workplace. According to Leng (2022), 60% of employers with remote workers is already using employee monitoring software, and seventeen percent is still considering it. The reasons for monitoring employees can vary from understanding how employees spend their time in the workplace (Leng, 2022) to protecting the company from potential legal issues (Yerby, 2013), and finally to maintain and increase their productivity (Snow, Pierce, McAfee, 2014). However, despite the many arguments brought by employers in favour of said practice, there's widespread concern about whether it is legal to spy on employees (Yerby, 2013), with many arguing that improper implementation can lead to a decrease in productivity, increased turnover, and hostility in the workplace (Tomczak, Lanzo and Aguinis, 2017) and distrust (Lin, Liu and Chang, 2015). The points observed in this paper analyse the various concerns about the introduction of employee monitoring software in the workplace, however such complex discussion cannot be reduced as a simple "pros and cons" analysis, because the ethical ramifications of this practice are to be considered regardless of the benefits and risks that it can bring and should not be underestimated.

# 2. Arguments

This paper debates the implementation of EMS in the workplace with careful consideration to six main arguments: productivity, organisation security, employee security, employee privacy, employer liability, and employee distrust. Such discussions are not conclusive and do not bring solutions to the problem as there is no easy solution in these ethical issues, but they provide a careful examination of legal, objective, and moral issues and obligations regarding the monitoring of employees by employers.

## *2.1 The quality of work*

Cyberloafing, also known as cyberslacking, is a term used to describe employees accessing the internet for private use during work hours. Lim (2002) defines it as "the act of voluntarily checking personal emails and surfing websites that are not job-related by employees during stipulated work hours". A great number of organizations has decided to monitor employees in order to keep their personal computer usage to a minimum, viewing monitoring as a way to both increase productivity and contain costs. Surfing the Internet

and sending personal messages and e-mails takes up time that could (and should) be used to work, thus reducing the productivity. According to salary.com (2014) 89% of workers waste at least some time at work on a daily basis, with the biggest percentage (78%) wasting between 30 and 120 minutes. In 2017, a survey conducted by rebootonline.com showed that UK employees spend on average 37 minutes browsing social media daily, and, on top of that, they spend 33 minutes a day surfing other websites. Every minute spent booking holidays or checking the news is a minute not spent increasing revenue. This is a huge cost for companies, as it can reach about £8,000 *per employee* annually (Davies, 2017). According to Satariano (2020), there has been a surge in demand for EMS during the COVID pandemic as companies need to ensure that all of their remote workers are doing what they are paid while they're working from home unsurveiled. The researches about this topic are widely discussed. For example, data shows that employee performance increases by 13% when working from home without any form of surveillance (Bloom, Liang, Roberts, Ying, 2015). According to Ugrin and Pearson (2013) monitoring resulted effective in reducing "serious" cyberloafing activities such as pornography, but it did not reduce "minor" activities such as social networking and messaging. However, this argument rises some important questions regarding where is the line between maintaining or increasing productivity and spying on employees violating their privacy.

### *2.2 Keeping the company safe*

According to the Cybersecurity Breaches Survey conducted in 2020 by the UK government, almost half of business and one quarter of charities reported having any kind of cyber security breach or attack over a 12-months period. The top three types of attack are: Fraudulent emails or redirection to fraudulent websites (86% for business and 85% for charities), people impersonating organisations in e-mails or online (26% for business and 39% for charities), and viruses, spyware or malware attacks (16% for business, 22% for charities), which means that checking private inboxes during worktimes and especially at workplaces can statistically put the company at risk. At the same time, direct security and monitoring became harder where staff are working remotely. The data shown evidence the importance of a specific question: does the implementation of employee monitoring software lead to greater security for the companies? Organisations argue that by implementing employee monitoring software and viewing any activity done on company property or during worktime such as messages sent, installed applications, web history, they can effectively protect the organisation from insider threats such as security breaches and unauthorized access and encourage employees to comply to the other security policies, and they're not totally wrong: D'Arcy and Lowry (2017) found that computer monitoring is actually positively associated with employees' daily attitude towards policy compliance, and it can be argued that such a system would work as a deterrent, lowering the

risk just because the employees know it is implemented. However, another study (Alder, Schminke, Noel, Kuenzi, 2007) showed that the effectiveness of the monitoring system greatly depends on the characteristics of the monitoring system and how it is implemented, which means that the organisations' approach to the problem can really make a difference between reaching their true goal and creating distrust that affects both behaviour and productivity, obtaining the opposite results.

### *2.3 Keeping the employees safe*

One of the main point brought to light by the advocators of EMS in the workplace is that it does not only help protecting the organisation, but the employees as well. According to AllVoices.co (2021) 44% of employees have experienced harassment in some form at work, and 38% still experienced harassment remotely through e-mail, chat and video conferencing. Each and every one of these forms of harassment impact productivity negatively which means it is in the companies' best interest to engage proactively and fight any type of harassment in the workplace. Companies argue that EMS would help recording interpersonal communications such as chat, calls and social media activities between employees, which can then be used as both as deterrent to prevent any form of harassment, and as evidence that can reduce time and financial expenses during the control process. Alan (2021) describes how EMS can help companies reduce episodes of harassment, as well as identify false allegations and address third party harassment such as abusive customers by recording audio and video, monitoring chats and social media activity. However, it could be argued that there should be better ways to fight harassment in the workplace other than bugging your employees, as there's a risk that allowing such invasive control can backfire when the manager/employee uses whatever information they've acquired to harass employees, or in case of security breaches.

### *2.4 What about my privacy?*

This is one of the main concerns regarding the implementation of EMS in the workplace. Despite the many possible advantages, should employers be able to monitor employees at all? Do the employees have the right to know if their employers are monitoring them and why? Should there be any restriction on what can be monitored?

According to many groups such as unions and organisations that fight for workplace fairness and rights, secret monitoring would violate workplace rights, but following this logic there should not be *any* kind of monitoring in the workplace (Yerby, 2013). However, in Frayer's (2002) opinion, it would be "ridiculous" to *never* allow

an employer to monitor their employee's activities, mostly for the reasons that were explained in the above sections. So, assuming that both parts are right in their demands, where's the line between the employees' right to privacy and the organisations' right to protect their assets and ensure the productivity of their company? To find such a line, one should first analyse how people address ethical situations. The two most common types of ethical reasoning are deontologism and consequentialism. Deontologists believe that an action is right or wrong if its motives are *universally* right or wrong, regardless of their consequences. Opposingly, consequentialists say the consequences of the action define the basis for its rightness or wrongness. Alder, Schminke, Noel and Kuenzi (2007) found in their study that employee's acceptance and compliance to the implementation of EMS in the workplace largely depends on their ethical reasoning and perspective: employees that believe in deontologist ethics tended to perceive employee monitoring as invasive and as a threat to their privacy. On the other hand, consequentialist employees mostly believed that monitoring could potentially represent a useful tool. In either case, the advent of technology has forced people to reconsider their concept of privacy.

### *2.5 Legal considerations*

The legal aspects of employee monitoring differ in each country as it depends on the presence of laws that regulate if monitoring is allowed and to what extent. Generally speaking, most country require employees to be notified before the monitoring activity can begin. Yerby (2013) explains how employers that refuse to monitor their employees' activities in the workplace are more likely to suffer financial losses and can even potentially be considered liable for the employees' hostility in the workplace or for their misbehaviour. If an employee opens a private e-mail while at work and downloads a virus that allows a hacker to steal the private data of thousands of customers causing enormous financial loss and potential lawsuits from said customers, are they liable or is the organisation liable? Could it have been prevented? Yerby (2013) suggests how the introduction of monitoring could be appropriate if employees are trained in resource usage and are warned about the possibility of monitoring. However, even when reasonable and accepted, monitoring should be done with limitations. For example, if an employer requires the installation of a software to monitor work phone/video calls, it would be best to provide a work phone and number for the employee rather than asking them to install it on their private phone and record their private calls as well, that will let them understand the reason behind the monitoring and possibly make them more willing to accept such condition. In the end, employers have both legal and moral obligations to control their workers' actions and behaviour in order to protect themselves, the employees and potentially the customers as well, but it's up to them to do it properly.

### *2.6 Trust*

When implementing employee monitoring software in the workplace, disagreement between employers and workers may arise, especially when debating about the ownership of employee information. Unclear information about monitoring, leakage of private information to third parties and excess monitoring can lead to employees' distrust towards the organisation. According to Tomczak, Lanzo and Aguinis (2017), inappropriate implementation of employee monitoring can lead to various negative reactions that can eventually lead to decreased performance and counter-productive work behaviours which will outweigh any potential benefit brought by the EMS. A study conducted by Lin, Liu and Chang (2015) shows how excessive monitoring, insecure design of policies and privacy transgression by other coworkers and managers negatively affects trust in EMS, policies, and management. The same study revealed how sufficient monitoring, clear and well-defined policies and careful compliance from every member can increase employees' trust in said system, developing even further their long-term commitment to the organisation and facilitating compliance to the policies.

## 3. Conclusion

This document discussed the main concerns about the introduction of EMS in the workplace. It was considered that even though monitoring employees can benefit every part involved by ensuring productivity, reducing wastage, and protecting employees from liabilities and harassment, the data clearly shows that inappropriate and inefficient implementation of a monitoring system, can lead to the opposite results and therefore reduce productivity, generate hostile environments in the workplace, favour harassment and abuse. It should be empathized that the real question regarding monitoring should not be "is it right or wrong?", but "is it done properly or not?", as the discussed data clearly evidences that while the perception of a monitoring system can depend on the ethical views of the monitored, it is vastly influenced by how the system is implemented, and if the employees are correctly trained and informed about their monitoring.

# References


2014 wasting time at work survey. (2014, March 19). Retrieved April 3, 2022, from https://www.salary.com/chronicles/2014-wasting-time-at-work/

Alan, C. (2021, November 29). Employee monitoring can prevent and resolve workplace. Retrieved April 3, 2022, from https://speakrights.com/employee-monitoring-can-prevent-and-resolve-workplace-harassment/

Alder, G. S., Schminke, M., Noel, T. W., & Kuenzi, M. (2007). Employee reactions to internet monitoring: The moderating role of ethical orientation. *Journal of Business Ethics, 80*(3), 481-498. doi:10.1007/s10551-007-9432-2

Bloom, N., Liang, J., Roberts, J., & Ying, Z. J. (2015, March 3). *Does working from home work? Evidence from a chinese experiment*. Retrieved April 2, 2022, from https://nbloom.people.stanford.edu/sites/g/files/sbiybj4746/f/wfh.pdf

Chang, S. E., Liu, A. Y., & Lin, S. (2015). Exploring privacy and trust for employee monitoring. *Industrial Management & Data Systems, 115*(1), 88-106. doi:10.1108/imds-07-2014-0197

Cyber security breaches survey 2020. (2020). Retrieved March 27, 2022, from https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2020/cyber-security-breaches-survey-2020

D'Arcy, J., & Lowry, P. B. (2017). Cognitive-affective drivers of employees' daily compliance with information security policies: A multilevel, Longitudinal Study. *Information Systems Journal, 29*(1), 43-69. doi:10.1111/isj.12173

Davies, T. (2017, August 17). 27% of the Working Day is wasted. Retrieved April 3, 2022, from https://www.rebootonline.com/blog/survey-reveals-how-much-time-we-really-waste-in-the-working-day/

Frayer, C. E. (2022). Employee Privacy and Internet Monitoring: Balancing Workers' Rights and Dignity with Legitimate Management Interests. *The Business Lawyer, 57*(2), 857-878.

Leng, A. (2022, January 31). 6 in 10 employers require monitoring software for remote workers. Retrieved April 1, 2022, from https://digital.com/6-in-10-employers-require-monitoring-software-for-remote-workers/

Lim, V. K. (2002). The it way of loafing on the job: Cyberloafing, neutralizing and organizational justice. *Journal of Organizational Behavior, 23*(5), 675-694. doi:10.1002/job.161

Pierce, L., Snow, D. C., & McAfee, A. (2015). Cleaning House: The Impact of Information Technology Monitoring on Employee Theft and Productivity. *Management Science*, *61(10),* 2299–2319. http://www.jstor.org/stable/24551528

Satariano, A. (2020, May 6). How My Boss Monitors Me While I Work From Home. *The New York Times*.

The State of Workplace Harassment 2021. (2021, September 1). Retrieved April 8, 2022, from https://www.allvoices.co/blog/the-state-of-workplace-harassment-2021#:~:text=44%25%20have%20experienced%20harassment%20at%20work,-

To%20start%20with&text=43.8%25%20report%20that%20they%20have,likely%20to%20have%20experienced%20harassment.

Tomczak, D. L., Lanzo, L. A., & Anguinis, H. (2018). Evidence-based recommendations for employee performance monitoringDF. *Business Horizons, 61*(2), 251-259. doi:10.1016/j.bushor.2017.11.006

Ugrin, J. C., & Michael Pearson, J. (2013). The effects of sanctions and stigmas on cyberloafing. *Computers in Human Behavior, 29*(3), 812-820. doi:10.1016/j.chb.2012.11.005

Yerby, J. (2013). Legal and ethical issues of employee monitoring. *Online Journal of Applied Knowledge Management.* 1. 44-55 Retrieved March 16, 2022.