TechTank

BROOKINGS

# How employers use technology to surveil employees

Darrell M. West Tuesday, January 5, 2021

Lisa Rene worked at an Indianapolis store operated by G. F. Fishers. Without informing company employees, the firm installed keylogger software on the store's computers which recorded characters typed on the business machines and periodically emailed that information to supervisors. While at work, Rene used the store computer to check her personal email and bank account. Through the installed software, a company employee discovered her personal passwords and used that information to look at her private emails and financial account. When she learned what had happened, she confronted her fellow employees and was fired for poor performance.

This is just one example of what has become an onslaught of intrusive workplace surveillance practices in the United States. Companies have the legal ability to use keylogger software on business computers, deploy video surveillance cameras, monitor worker attentiveness, track physical movements through geolocation software, compile lists of visited websites and applications, monitor emails, social media posts, and collaboration tools, and compile productivity data on how workers are spending their time and how long it takes them to finish particular tasks.

With more people working remotely at home due to the COVID-19 pandemic, the boundary between business and personal activities has blurred because people are spending considerable time on company equipment and business video calls, including in the evenings and on weekends. As I discuss below, these developments raise important concerns for company workers and highlight the need for stronger protections of employees at the state and national levels.

*Keylogger software*

Work on firm equipment and over company digital networks generally is subject to monitoring as long as the activity takes place during the "ordinary course of business". Both the Electronic Communications Privacy Act and the Stored Communications Act allow firms to track employee activities without prior notification, although the scope of the allowable oversight varies quite a bit from state-to-state. Many of the rules governing workplace surveillance are at the state level and there is wide variation in what jurisdictions allow and the legal precedents that govern such actions.

In a number of places, firms are able to use keylogger software on company equipment. If workers intermingle personal and business activities on the company device, that can expose private information to supervisors. According to Matt Pinsker, an adjunct professor of homeland security and criminal justice at Virginia Commonwealth University, "as a general rule, employees have little expectation of privacy while on company grounds or using company equipment".

*Video surveillance*

Firms are allowed to engage in video surveillance in common areas, but not private spaces such as bathrooms or locker rooms. They can use closed circuit television to safeguard security, monitor movements, and track worker performance. According to an American Bar Association report, "an employer may photograph employees in plain view, at their workstations and during working hours, for time and motion studies or as part of an investigative process." But the camera or recording equipment should be clearly visible and not a hidden device.

*Attention tracking*

In some places, organizations are using webcams to track worker attentiveness. Using biometric data such as eye movements, body shifts, and facial expressions, webcam software can evaluate whether people are paying attention to the tasks at hand and being properly attentive in workplace activities and on video calls. Those who are inattentive can be reprimanded or subject to disciplinary action.

*Geolocation tracking*

Company-issued smart phones have geolocation features that allow for the tracking of physical movements and location. They can show equipment locations within a few feet and track the time spent there. The combination of timelines and physical location is powerful because it shows where individuals are as well as when and how long they are at that location.

*Web browsing and app utilization*

Many firms use software which show the websites employees have visited and the apps they have used. That allows companies to keep track of browsing behavior and see if employees are wasting time or visiting inappropriate sites. Furthermore, businesses can monitor app usage as a way to gauge productivity and policy compliance.

*Email and social media monitoring*

In nearly every jurisdiction, emails are subject to company oversight in order to make sure employees are complying with company policies, not engaging in illegal activities, not leaking information, or not using company equipment for abusive or harassing actions. Firms can use keyword searches to spot suspicious or unethical activities and monitor attachment downloads. A 2018 Gartner survey found that "half of large companies use some type of monitoring techniques to keep tabs on their employees, including methods like analyzing texts of emails and social media messages and gathering biometric data".

*Collaboration tools*

An increasing number of organizations are utilizing collaboration tools like Slack for internal communications. These platforms allow workers to send private messages to one another, comment on one another's work products, and share memos, papers, reports, and videos. If done on company equipment, these activities are subject to firm monitoring since they are considered part of ordinary business.

*Productivity data*

Business leaders are using software to track what employees are doing, how quickly they are doing it, and how productive they are. This includes activities such as number and length of emails, how long it takes to compose particular messages, how long it takes to perform specific tasks, how much of one's day is devoted to meetings and phone calls, and how much quiet or unoccupied time people have.

## Ways to Protect Worker Privacy

When taken together, it is clear organizations have a wide range of tools at their disposal to monitor worker performance and keep track of their activities. As long as the monitoring takes place in office workplaces, on company devices, or over firm networks, there aren't many limits on what organizations can do in most states.

In this situation, there is a need to clarify workplace rules, and improve worker understanding of how they are being monitored, especially during remote work from home. There needs to be stronger protections of worker privacy, greater transparency about current practices, and better notification of what tools are being used. Many of these changes need to take place at the state level because current federal privacy proposals generally have set aside stricter regulation of workplace monitoring due to its complexity and a desire not to preempt existing state laws.

*Better worker notifications*

With the ubiquity of monitoring software on company devices, it is important to develop new laws, regulations, and policies that notify workers about surveillance practices. Some states such as Connecticut and Delaware have adopted mandatory worker notification rules, while others such as California have enacted new privacy protections (the California Consumer Protection Act) which say employees must be informed about network activities such as "browsing history, search history, and information regarding an internet website, application, or advertisement". One laudable practice in the U.S. national government is to show a warning that federal email is government property and there is no right to privacy in electronic communications. That message reminds government employees their emails are not private and are subject to freedom of information requests.

*Clarification of workplace rules when employees are working from home*

One of the areas in greatest need of reform concerns the rules governing workplace monitoring in regard to remote work. Working from home either full-time or part-time likely is to become the new normal even after COVID-19 recedes. Many workers like the convenience of remote work and the flexibility provided for childcare and elder care. But in this situation, workers need guarantees that their privacy is protected when even when using company laptops or phones. The blurring of the lines between work and non-work has increased during the pandemic because many people are working at night or on the weekends, and mixing personal and professional tasks. It behooves companies to respect worker privacy as people shift quickly from personal to employment-related activities and back during the course of the day. It would not be fair to fire or penalize employees for breaking workplace rules while they are working from home.

*Clearer rules on internal data sharing and external disclosures*

Companies should be clear on their rules for data sharing. Under what circumstances is data available to immediate, mid-level, and top-level supervisors and what are they allowed to do with this information? There needs to be policies on whether worker consent is required for these kinds of disclosures. There also should be clear policies on when and under what circumstances the compiled data is made available to law enforcement, government officials, and legislative oversight bodies and when disclosures are made to employees.

*Limits on storage time*

There should be limits on the storage time for data collected for purposes of worker surveillance. The exact length should depend on the sensitivity of the information and possible employee harms. Employee information should not be held for indefinite periods by employers, but rather only as long as it serves a clear and discernible purpose.

*Learning from the European Union*

The General Data Protection Regulation of the European Union goes further than American policies in covering employees and providing privacy protections. The EU explicitly notes that worker notification and consent is limited in practice due to the significant power imbalances between employees and employers. In most cases, workers have no choice but to grant consent because it is a requirement of the job and withholding consent means they cannot perform their job duties.

*Stronger norms against workplace surveillance*

Irrespective of the legal situation, companies should develop best practices that limit their surveillance. Even if they have the legal right to monitor employees does not mean they actually should utilize the full range of monitoring tools. They should recognize that employees have expectations of privacy in the workplace and they need practices that respect those expectations. If companies allow incidental personal use of business email and devices, employers should be respectful of messages and activities that are personal in nature.

**Acknowledgments:**

*The author would like to thank Mishaela Robison for helpful research assistance on this blog post.*