JacksonLewis

Monitoring Remote Employees and Privacy Concerns

Issue:
How can employers monitor employees working from home while ensuring compliance with a growing number of legal mandates related to employee privacy?

Historical Context:
Record numbers of employees have been working from home since the onset of the COVID-19 pandemic. As we settle into a post-pandemic “new normal,” remote work will remain a permanent fixture of life for many. Technological advancements have made it easier to monitor remote employees through audio and video monitoring, spyware, keystroke monitoring, and tracking network activity to see how active employees are throughout the day.

Employers monitor off-site employees for numerous reasons—not simply to ensure productivity, but to protect trade secrets, avoid data breaches, track an employee’s physical location, and generally discourage or identify misconduct. Most recently, monitoring has been used for COVID-19-related contact tracing purposes. However, privacy-related legal pitfalls abound.

Critical Factors:
Employers must contend with a growing number of privacy and confidentiality requirements at the local, state, federal, and international levels. Myriad obligations and compliance considerations can be triggered by employee monitoring and/or data collection, each imposing varying obligations for employers.

State privacy laws (*e.g.*, the California Consumer Protection Act (CCPA)) may require that employees be provided notice describing the categories of personal information (including network activity) that a company collects and the purposes for which that information is used. Also, more than 25 states have enacted social media password protection laws that prohibit employers from requesting or requiring employees to provide credentials to their personal social media or other online accounts. Accessing these communications can also violate the federal Stored Communications Act. In addition, an employer may inadvertently discover medical information about an employee through spyware, implicating the Americans with Disabilities Act (ADA) and state medical privacy protections, or information about an employee's family member suffering from a debilitating health condition, which may raise concerns under the Genetic Information Nondiscrimination Act (GINA). Additional privacy and security regulations also may apply based on the industry in which the organization operates (*e.g.*, healthcare, finance, government contractors); heightened professional responsibilities (applicable to attorneys or accountants, for example); and contractual obligations governing the collection, storage, and destruction of data, which apply when using certain platforms and vendors.

Steps to Take:

Employers must strike the proper balance between the use of technology to monitor remote employees and the protection of employees' privacy or security expectations. Adopt these best practices to ensure the highest levels of privacy are met while simultaneously protecting your business and employees.

- **Understand the technology.** Deploy these technologies only after a careful review, with input from HR and the Legal Department to minimize legal risk and maintain good employee relations and trust.

- **Draft an acceptable use and electronic communication policy** that informs employees about what they can expect when using the organization's systems, both at the workplace and when working remotely. This includes addressing employees' expectation of privacy and makes clear which information systems and activity are subject to the policy.

- **Revisit the organization's policies and protocols** and conduct user training to minimize the risk of violations resulting from device usage, network access, data security and document retention.

- **Safeguard the information collected.** Under certain statutes, the mere act of collecting sensitive information can be problematic. A growing number of states have stringent requirements to maintain reasonable safeguards to protect

personal information. The definition of personal information is not limited to Social Security numbers. Medical information, online account credentials, credit card numbers, and birth dates all can be captured and stored using spyware, keylogging, and other tools.

- **Exercise caution when taking adverse action.** When making personnel decisions based on information obtained though surveillance, heed federal and state laws prohibiting discrimination on the basis of genetic information, disability, or poor credit or payment histories. The use of such information for a discriminatory purpose could result in statutory violations.

- **Be prepared to investigate.** Surveillance may uncover nonperformance, irregular activity, malicious insiders, and other conduct that will need to be promptly addressed. Be prepared to respond to such findings with a comprehensive investigation protocol that involves the appropriate persons at the earliest time. The time to lay out that process is *before* evidence of improper activity is discovered.

- **Know your rights.** Numerous states restrict employer access to employees' personal social media or other online accounts. However, these laws generally permit employers to follow up on specific information obtained on an employee's personal online account for purposes of investigating potential violations of the law and ensuring compliance with prohibitions against work-related misconduct. Employers also may monitor, review, access or block electronic data stored on an electronic communications device paid for, in whole or in part, by the employer, or data that is stored on the company network.

- **Monitor the monitors.** If your organization assigns individuals to monitor remote employees, provide guidance to ensure they don't go too far in their surveillance, and routinely review monitors' compliance with those guidelines. Set clear boundaries that the organization has determined, with guidance of counsel, to be appropriate. Ensure that monitors know what to do if they inadvertently discover information about an employee's religion, disability, or genetic information.

- **Stay on top of emerging privacy laws.** A growing list of states are curtailing the use of employer-driven devices, radio frequency identification devices (RFIDs), and microchip implantation, which some experts view as the next battleground over privacy rights. Employers using such technology, or considering adopting these tools, must keep a watchful eye on the ever-changing legal landscape.

JacksonLewis

More information on this topic can be found at www.jacksonlewis.com**.**