New York Law Journal

NEW YORK LAW JOURNAL SPECIAL REPORT

An ALM Publication

Cybersecurity

WWW.NYLJ.COM

VOLUME 261—NO. 105

MONDAY, JUNE 3, 2019

Striking a **Balance** Between Cybersecurity and **Employee Privacy**

BY AVI GESSER MATTHEW KELLY, WILL SCHILDKNECHT AND ANNA MARIENKO

SHUTTERSTOCK

Various regulatory regimes require companies to implement reasonable cybersecurity measures, which generally seek to protect company systems and confidential data. As a result, companies are increasingly expending resources to mitigate the risks to their sensitive information posed by external threats, including organized criminals, hacktivists and hostile nation states.

At the same time, insider cyber threats, such as deliberate theft or destruction of sensitive information, as well as innocent mistakes that result in lost control over confidential data, are primary risk factors for most businesses. To protect sensitive information and meet their regulatory obligations, many companies feel compelled to closely monitor the activities of their employees.

Determining how far a company should go in tracking its employees, however, requires a delicate balance between (1) reasonable efforts to detect and prevent wrongdoing or carelessness that could harm the company, and (2) respecting employees' reasonable expectation of privacy. Although the appropriate measures should be determined on a case-by-case basis, over time, a few principles have emerged that provide guidance on where to draw lines. As summarized below, most successful approaches for striking the proper balance involve having clear policies.

Principles From Established Data Privacy Challenges

Work Emails and Internet Use. Generally, a company can monitor employees' work emails and other activity on work applications hosted

AVI GESSER *is a partner in the litigation department of Davis Polk & Wardwell, representing clients in a wide range of cybersecurity issues.* MATTHEW KELLY, WILL SCHILDKNECHT *and* ANNA MARIENKO *are associates in the firm's litigation department.*

on a company network. See, e.g., *United States v. Finazzo*, 682 F. App'x 6, 16 (2d Cir. 2017). For example, employers may implement software that looks for employees who may be (1) using their work email to send confidential company data to their personal email accounts, (2) downloading large amounts of sensitive company data to a portable device, or (3) using phrases in their work email that may be associated with fraud (such as "let's not discuss this by email, please give me a call, we don't want to get in trouble"). Similarly, monitoring and limiting employees' Internet use is usually an acceptable way for companies to reduce the risk of hacking and other data leaks.

Personal Emails. By contrast, absent a compelling reason or express policy, employers generally should not monitor the personal email accounts of employees, even if such emails are being accessed using company-owned devices, because employees have a reasonable expectation of privacy over their personal email accounts. See *Pure Power Boot Camp v. Warrior Fitness Boot Camp*, 587 F. Supp. 2d 548, 559-60 (S.D.N.Y. 2008).

Phone calls. Employers can generally monitor an employee's phone calls, as long as the employee is aware of this. See *United States v. Rittweger*, 258 F. Supp. 2d 345, 354 (S.D.N.Y. 2003), although some states, like California, require consent of both parties on a call before the call can be recorded. Cal. Penal Code §632.

Video surveillance. An employer may generally film employees at their desks during working hours as part of an investigation. See *Clark v. Elam Sand & Gravel*, 4 Misc.3d 294, 295 (Sup. Ct. 2004). But, if the cameras are hidden, the employer needs to demonstrate a legitimate business reason for the surveillance and it should not place cameras in areas where the employees have a reasonable expectation of privacy, such as bathrooms. See *Mendez v. Starwood Hotels & Resorts Worldwide*, 746 F. Supp. 2d 575, 598 (S.D.N.Y. 2010); N.Y. Labor Law §203-c(1). In some states, such as New York, video recordings are subject to state wiretap laws, and the audio function on the video cannot be turned on unless an employer has the employees' consent. N.Y. Penal Law §250.00; see also *DeVittorio v. Hall*, 589 F. Supp. 2d 247, 258 (S.D.N.Y. 2008), aff'd, 347 F. App'x 650 (2d Cir. 2009).

Although the appropriate measures should be determined on a case-by-case basis, over time, a few principles have emerged that provide guidance on where to draw lines.

The Importance of Having Clear Policies

Applying these general principles to new technologies and current data threats can be tricky. Perhaps the most important step employers can take to reduce the risk of inadvertently infringing on employees' privacy rights is to have clear policies.

To see how this works in practice, consider the challenge that companies face in determining when they can demand access to employees' personal phones that are used for both work and personal communications. Some companies allow their employees to have confidential work emails on their personal smartphones. Those companies may want to have policies that allow them to monitor those devices to ensure that they are updated with the latest security patches and software updates, and that no malicious apps are downloaded that could access sensitive company data.

Many companies are also adopting policies on what kind of communications can and cannot take place on personal apps. So if, for example, an employee uses iMessage to communicate about a substantive work issue that becomes important for a regulatory investigation, the policy could make clear that failing to copy that message to the company's system within a reasonable time is a violation of policy, and the employer has a right to access those messages and to discipline employees who refuse such access.

Another example where having clear policies can avoid problems is social media. Companies may have a legitimate interest in monitoring their employees' use of social media to ensure that employees are not (1) saying things that are defamatory to the company, individual supervisors, or clients, (2) improperly disclosing confidential company or client information, or (3) making statements on behalf of the company without authorization. But such monitoring should not be done to investigate employees' political or social positions. Moreover, §7 of the National

Labor Relations Act provides some protection for employees who are discussing the terms and conditions of their employment or their working conditions, so long as their statements are not false. Accordingly, employers would be well-served by having clear policies on the proper use of social media so that any monitoring can be clearly justified as an expected effort to ensure compliance.

Departing Employees

Insider threat risks do not end when employees leave the company. Sensitive company data in the hands of a disgruntled former employee is a serious potential risk, as is unauthorized access to confidential company information by a former employee who may be acting in good faith.

Some companies require departing employees to identify all the locations where they may have confidential company data, including old company computers and phones, personal computers where company data has been saved, and personal email accounts or messaging applications. They also ask departing employees to identify all of their employment-related accounts, such as a sharepoint, FTP sites, and extranets, to make sure the accounts are properly closed. Other measures that reduce the risk of former employees leaking confidential company information include:

- Prohibiting and disabling the use of portable electronic data storage devices, such as thumb drives, on work-issued electronic devices.
- Employing software that can isolate and remotely wipe work-related apps and data from employees' personal devices.
- Monitoring the web, including sites like GitHub and LinkedIn, for sensitive company information.

The Coming Challenges

As more employees work from outside the office using their personal devices, finding the right balance between cybersecurity and employee privacy will be even harder to maintain, especially as the increasing number of high-profile data leaks make employees more concerned about their privacy, and companies more focused on protecting data from various threats, including insiders. In addition, new privacy laws are coming into effect (such as the California Consumer Privacy Act) that require companies to protect confidential data, but also place constraints on what data employers can collect about their employees, which may limit companies' ability to engage in certain kinds of monitoring.

To further complicate these issues, recent advances in technology allow employers to easily monitor every keystroke and every step that employees make. And the combination of location tracking of phones and widely available facial recognition technology will introduce a host of new privacy challenges. There is little doubt that companies gain substantial security benefits from knowing where all of their employees are located at any given moment. Such data can greatly reduce the risks of unauthorized physical access, and can be extremely valuable in determining whether a suspicious remote login, or phone call to the technology help desk, is legitimate or not. But location tracking can also be used to see who is meeting with whom outside of the office, who is coming to work late or leaving early, and what employees are doing on days they report in sick.

These are only a handful of the dozens of new monitoring options that will become available to employers for which the proper lines between protecting legitimate company interests and unreasonably infringing on employee privacy will not be easy to draw. Previous experience with technological developments shows that having clear policies and training for employees on the proper use of company information and devices, and what they should and should not expect to be private, can go a long way in gaining employee trust and avoiding legal and reputational problems.