Questions—And Answers

Electronic Monitoring in the Workplace

Kevin J. Smith and Rachel J. Tischler

Employers and employment attorneys alike have been concerned about the legal limits of electronic monitoring since before many of us had personal e-mail accounts.[1] And since that time, the amount of work done "online"—through the Internet, intranet, e-mail, remote computing, and personal devices—has increased exponentially. This shift has been accompanied by an equal increase in the availability of monitoring technology, making employer surveillance of employees cheaper and more accessible. In the past decade, this has been further complicated by the proliferation of employees' use of personal electronic devices to conduct business. Accordingly, there are widespread concerns about employee efficiency, focus, and information, as well as product security. Employees' telephone, computer, mobile device, e-mail, voice mail, and social media accounts, in addition to all of the files and data stored therein, have all found themselves under employer scrutiny at one time or another, and often the results of that surveillance have been used in termination decisions or employment litigation. One form of conflict emerges when trying to balance the safety and integrity of an employer's data and computer systems with employees' expectations of and rights to privacy. Another conflict can arise when an employer's enforcement of its policies on personal electronic devices, computer and Internet usage, and employees' use of the devices for nonbusiness purposes—however innocent—leads to disciplinary action.

Although employer monitoring practices would seem to be barred by the federal Electronic Communications Privacy Act of 1986 (ECPA),[2] exceptions exist that permit monitoring in many circumstances. The ECPA governs, among other things, workplace electronic monitoring and applies to e-mail, telephone conversations, and electronically stored data. The ECPA

Published online in Wiley Online Library (wileyonlinelibrary.com). DOI 10.1002/ert.21491

prohibits the "intentional intercept[tion] ... [of] any wire, oral, or electronic communication,"[3] as well as intentionally accessing stored electronic communications.[4] Exceptions under the ECPA permit employers to (1) monitor business-related communications; (2) monitor communications over which the employee has given consent; and (3) access employee e-mail messages stored by the employer.[5] This Q&A addresses questions to help clarify what types of electronic monitoring employers can conduct and the limits of what employers can supervise in the workplace.

CAN EMPLOYERS LISTEN IN ON EMPLOYEE PHONE CALLS?

Federal law does not prohibit employers from monitoring an employee's *business-related* phone calls,[6] although laws may vary by state.[7] Employers are not permitted, however, to monitor calls it knows to be personal in nature.[8] The ECPA protects the privacy of personal telephone calls by limiting the exceptions to the general prohibition on intentional interception of electronic or wire communications. In addition to the *business-related* exception, there is an exception for consent, but courts have clearly stated that consent is not an all-or-nothing proposition.[9] For instance, in workplaces with policies prohibiting the use of company telephones for personal calls, there is a risk to employees that calls they place on company phones—personal or otherwise—may be monitored. No consent would be required under those policies in order for an employer to monitor even personal phone calls. Under more permissive employer policies, however, where infrequent personal calls are permitted, employees have not necessarily consented to the monitoring of their personal calls; if the monitoring is automatic, once the employer determines the call is personal, the monitoring should cease.[10] This rule does not apply to calls made from an employee's personal mobile phone or device because this device is not within the employer's control.

CAN EMPLOYERS READ EMPLOYEE E-MAILS?

Under federal law, employers are permitted to conduct computer monitoring and supervision that captures a record of certain employee activity. For employer-provided computers, there are a number of methods by which an employer may monitor employee usage. Employers may use programs that allow them to (1) see what is on an employee's screen at any given time, (2) review the keystrokes or frequency of keystrokes of their employees, (3) track when a computer is being used and when it is idle, and (4) monitor Internet usage and search history (among others). These different surveillance capabilities are useful for various purposes, but they mean that an

employer can see the purpose for which an employee is using the company computer at any moment.

When it comes to reading employee e-mails, an employer handbook may state that any e-mail sent using a company-provided e-mail address is the property of the employer, and thus subject to monitoring without consent of the employee. Further, because keystroke monitoring may allow an employer to see what an employee is typing, the content of any web searching or web-based e-mail may be available to an employer as well. Again, state laws may do more to protect employee privacy, but federal law does not prohibit this type of monitoring.

ARE EMPLOYEE PERSONAL E-MAILS OFF-LIMITS TO EMPLOYERS?

If an employee is using a company-provided e-mail system to send personal messages, those messages are generally accessible and reviewable by the employer because the content is part of a system that the employer owns, thus making it employer property. Company policy permitting monitoring may also cover personal e-mail sent from a password-protected web-based e-mail account when sent using the employer's computer. For example, e-mails from a Gmail or Hotmail account that an employee sends from an employer's computer terminal may be lawfully monitored by the employer. That being said, recent case law in New Jersey has drawn a line between personal e-mail that employers may monitor and that which they may not—even when a company computer is being used.[11] In *Stengart v. Loving Care Agency*, the court found that attorney-client privileged e-mails that an employee sent using a personal e-mail account—on an employer-provided laptop—were excluded from e-mails that the employer could permissibly monitor.[12] The court noted that the employer's policy about use of the company computer did not contemplate personal e-mail accounts at all, and even if it had, the privileged nature of the messages would have given the employee a reasonable expectation of privacy.[13]

Employees should also be aware that data they delete from a work computer may not be "gone forever," as they had intended. Often, employers back up all system data on a daily (or even more frequent) basis. In this manner, all messages sent, received, or deleted may be retained in redundant storage and can be accessed by an employer—even after an employee deletes the message or file.

WHAT HAPPENS IF EMPLOYEES USE THEIR OWN DEVICES FOR BUSINESS PURPOSES?

Many employers now have in place policies that specifically address the privacy of data and content saved or viewed on *employee*-owned devices

used for business purposes. These "bring-your-own-device," or BYOD, policies can be included in a handbook, employment agreement, intranet policies, or as a stand-alone document. Often, these policies affect the employees' privacy in ways they might not realize. Because of the employer's concern for the security of its data—including trade secrets, proprietary information, contact or marketing lists, and other potentially privileged information, as well as potential information loss caused by malicious software present on the employees' devices—employer BYOD policies can limit the types of devices and software it permits, require employees to install certain support and monitoring software on their personal devices, and, among other things, mandate employee consent to employer access to personal data, remote employer access and data management, and restrictions on deletion of certain data. In more concrete terms, this means employers may be able to access employees' phone records and text messages, view the web and streaming history on those devices, monitor GPS information, and access social media and other accounts—all on phones *not* owned by the employer.

Employers who implement these policies must balance the strength of the security protocols they are implementing with legitimate privacy concerns of their employees. Under the ECPA discussed above, if an employee brings a suit for a perceived privacy violation, an employer may still be required to meet the requirements for accessing stored electronic data mandated by the ECPA, regardless of employer security concerns.

CAN EMPLOYERS DEMAND ACCESS TO EMPLOYEE SOCIAL MEDIA ACCOUNTS OR PASSWORDS?

There are presently no federal protections for employees seeking to avoid disclosing their personal social media account information to their employer or prospective employer. As of November 2014, however, legislation limiting employer access to employee social media passwords has been passed in 6 states, and was introduced or is pending in close to 30 others.[14] State by state, this question is being analyzed and argued, and the vast majority of the states that have addressed it have limited employer access to this personal material. The National Labor Relations Board has joined the chorus in protecting employees' use of social media as a labor-organizing tool.[15] (See the State Regulations Update in this issue of *Employment Relations Today*.) As a result, employers in many states cannot demand employee social media account information, nor can they retaliate or discriminate against an employee or prospective employee for refusal to provide such information.

There are exceptions to this general rule, however, and where the social media accounts are being used for business purposes, access to those

user names or passwords may be permissible.[16] Similarly, soliciting a user name or password may be permissible for investigations aimed at "ensuring compliance with applicable laws, regulatory requirements, or prohibitions against work-related employee misconduct" when the investigation is spurred by an employer's receipt of specific information about activity on an employee's personal account.[17] These are not bright-line rules, and there may be many scenarios for which the question of whether an employer has permissible access to employee social media accounts cannot easily be answered. The best course would be for employers to have clear social media policies, and to ensure that the policies comply with the most current law in their state.

ARE EMPLOYEE PERSONAL FILES SAVED ON AN EMPLOYER'S COMPUTER CONSIDERED PRIVATE?

The short answer is no. An employer-owned computer and all data stored on that computer belong to the employer, including any files that an employee saves to that computer. An employer's computer-usage policy should be clear in this regard. Employees should be discouraged from using the computers for their personal use in the first place, and so the presence of their personal files on an employer-provided device could be grounds for a disciplinary action. The safety of an employer's data and computer systems overrides the employee's desire to use the equipment for personal purposes.

CAN AN EMPLOYER USE EMPLOYER-PROVIDED DEVICES TO MONITOR EMPLOYEES OFF-SITE?

Even in states where consent is required for GPS tracking of a personal vehicle, no similar federal restrictions are required on employer-provided vehicles.[18] This means that employers are theoretically permitted to track an employee using a GPS or some similar geolocation device if it is employer provided. Similarly, "apps" on smartphones can monitor a user's activity anywhere the device is being used, and if the employer provides the device, it can install and run any programs or monitoring software it wants. The presence of this software need not be disclosed to employees, but a BYOD policy should disclose that monitoring is a possibility.

CAN AN EMPLOYER USE VIDEO SURVEILLANCE TO MONITOR ITS EMPLOYEES ON- OR OFF-SITE?

Video surveillance is still limited insofar as it cannot be a "physical invasion" of employee privacy, such as placing a camera in a locker room or

bathroom. State laws may also limit how and why an employer may use video surveillance on its employees. Federal law, however, does not require employee consent or knowledge prior to an employer's using video surveillance. And, of course, employer surveillance of an employee in the privacy of his or her own home should be avoided unless that employer wants to open the door to invasion-of-privacy tort lawsuits. This does not mean, however, that an employer may not monitor the location of its devices or monitor the activity on its devices when they are in an employee's home—but they should not be used to monitor the private, nonwork activity of the employee when there.

NOTES

1. See, e.g., Julie A. Flanagan, Note, Restricting Electronic Monitoring in the Private Workplace, 43 Duke L.J. 1256 (1994).
2. Codified at 18 U.S.C. §§ 2510–22, §§ 2701–12.
3. Id. § 2516(1)(a).
4. Id. § 2701(a).
5. Id. § 2511(2)(a) & (c), § 2701(c).
6. See id. § 2511(2)(a).
7. For example, California requires a tone or recorded message to be played notifying the parties when a telephone call is being recorded. See Cal. Pub. Util. Comm'n, Gen. Order 107-B, available at http://www.cpuc.ca.gov/Published/Graphics/567.pdf. Also see the State Regulations Update in this issue of Employment Relations Today.
8. See Watkins v. L. M. Berry & Co., 704 F.2d 577, 583 (11th Cir. 1983).
9. Id. at 582.
10. See id.
11. See Stengart v. Loving Care Agency, Inc., 201 N.J. 300, 323–24 (N.J. 2010) (finding employee privacy rights violated when an employer was reading e-mails sent to employee's counsel through her personal e-mail account while using a company-provided laptop).
12. Id.
13. Id. at 322–23.
14. See Nat'l Conf. of State Legislatures, Employer Access to Social Media Usernames and Passwords, http://www.ncsl.org/research/telecommunications-and-information-technology/employer-access-to-social-media-passwords-2013.aspx#2014 (last updated Nov. 18, 2014).
15. See NLRB, The NLRB and Social Media, http://www.nlrb.gov/news-outreach/fact-sheets/nlrb-and-social-media (last visited Dec. 29, 2014).
16. See, e.g., N.Y. Assembly Bill No. A00443-B; N.Y. Senate Bill No. S02434-B.
17. See 2013 N.J. Sess. Law Serv. Ch. 155 (West) (Assembly 2878).

18. In a recent decision, the New York Court of Appeals held that warrantless GPS tracking of a government employee in his own car during working hours was permissible. See Cunningham v. N.Y.S. Dep't of Labor, 21 N.Y.3d 515 (N.Y. 2013) (permitting the search but prohibiting surveillance outside of working hours).

Kevin J. Smith *is special counsel at Sheppard, Mullin, Richter & Hampton LLP in the firm's Labor and Employment group. He has extensive experience in employment litigation, including trials and appeals in federal and state courts, and conducting arbitrations and administrative hearings. His employment law practice also includes counseling Fortune 500 companies in all types of employment and labor-law matters. He may be contacted at kjsmith@sheppardmullin.com.* ***Rachel J. Tischler*** *is a labor and employment attorney at Sheppard, Mullin, Richter & Hampton LLP. She has a broad range of experience in labor and employment matters, including wage-and-hour class-action lawsuits, wrongful-termination and discrimination lawsuits, and counseling. Her practice also includes experience in international employment concerns, wage-and-hour compliance, and personnel handbooks, with particular experience in I-9 and E-Verify compliance. She may be contacted at rtischler@sheppardmullin.com.*