E&MLF

CITE AS
32 *Energy & Min. L. Inst.* 3 (2011)

Chapter 3

Employee Privacy Rights: Employer Monitoring and Investigating Employees' Electronic Activities and Communications

C. David Morrison
Steptoe & Johnson PLLC
Bridgeport, West Virginia

Robert L. Bailey
Steptoe & Johnson PLLC
Charleston, West Virginia

Synopsis

§ 3.01. Introduction.

Technology pervades every corner of our lives, and nowhere is this more apparent than the workplace. Much of what companies and their employees do — in and out of the office — constitutes an electronic activity of one kind or another. The fact that these activities (and the devices and systems that they use) are electronic is often overt, as in the case of computers and telephones. But some facets of technology can be more covert — or, perhaps due to their omnipresence, at least easily ignored or forgotten.[1] Because of this ubiquity

[1] A recent United States Court of Appeals decision dispelled any doubt as to the broad scope that courts are willing to give laws related to technology and how blurry technological lines have become. In *United States v. Kramer*, 631 F.3d 900 (8th Cir. 2011), the defendant

and stealth, technology offers employers new and enhanced opportunities to monitor their employees' (and applicants') electronic activities to accomplish important business objectives.[2] This monitoring, however, is subject to a collage of regulation that inevitably trails behind — and changes almost as quickly — as the technology itself.

Because of this complexity, analysis of an employer's potential liability for monitoring its employees' electronic activities defies a single, efficient, top-down taxonomy. First, there are far too many relevant cross-cutting factors to prefer elevating any one to the top of the hierarchy: What kind of technology is being monitored? Who paid to acquire and operate it? How technically difficult is it to monitor? What was the person doing with the technology at the time it was being monitored? Was it purely work, purely personal, or a hybrid? What data or metadata was monitored? Does the employer want to intercept the electronic activity in real time or access previously stored data? Filter it? Block it? Alter it? What did the employer learn? How is the employer using the information? Is the context pre-, during, or post-employment? What steps must employers take pre-, during, and post-monitoring? What if the acquired information is released, inadvertently or intentionally?

"pleaded guilty to transporting a minor in interstate commerce with the intent to engage in criminal sexual activity with her, a violation of 18 U.S.C. § 2423(a). He also admitted that he used his cellular telephone — a Motorola Motorazr V3 — to make voice calls and send text messages to the victim for a six-month period leading up to the offense." *Id.* at 901-02. Based on that admission, the district court gave Kramer more than two additional years in prison under a sentencing guideline that provided: "If the offense involved the use of a computer . . . increase by 2 levels." U.S.S.G. § 2G1.3(b)(3). "Computer" in the guidelines was defined as "an electronic . . . or other high speed data processing device performing logical, arithmetic, or storage functions . . . but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device[.]" 18 U.S.C. § 1030(e)(1). Because of the computing power of Kramer's Motorazr, the Eighth Circuit affirmed the enhancement.

[2] Unless the context indicates otherwise, in this discussion, candidates for employment are considered to fall within the rubric of "employees."

Second, analysis is complicated by the fact that restrictions on employers monitoring their employees' electronic activities form as crazy a quilt as has ever been quilted, coming from just about every source of law imaginable: federal, state, local, and private; legislative, administrative, and judicial; civil and criminal. The analysis presented here employs functional categories to introduce the technology, a temporal context (pre-, mid-, or post-employment) for discussing the activities an employer might monitor and why, and jurisdictional divisions for presenting the kinds of restrictions with which every employer should be familiar.

In light of the scope of the topic, there will necessarily be *many* specific issues not mentioned, such as most wage and hour issues;[3] the intellectual property implications of monitoring (or failing to monitor);[4] the effect of employees' electronic activities on the attorney/client privilege, the work product doctrine, and the marital privilege;[5] electronic discovery or

---

3 *See, e.g.*, Thomas Kleeh, "You've Got Mail (and a Lawsuit): Mobile Communication Devices and the Wage and Hour Pitfalls They Present," *Nat'l L. Rev.*, available at http://www.natlawreview.com.

4 *See, e.g.*, Jeffrey D. Neuburger, "New Media, Technology and the Law: A Summary of Key Legal Developments Affecting Technology and Emerging Business Issues," 996 *PLI/Patent* 33 (Feb.-Apr. 2010).

5 *See, e.g.*, Adam C. Losey, Note, "Clicking Away Confidentiality: Workplace Waiver of Attorney-Client Privilege," 60 *Fla. L. Rev.* 1179 (Dec. 2008); in re: "Oil Spill by the Oil Rig 'Deepwater Horizon' in the Gulf of Mex.," on Apr. 20, 2010, No. 2:10-MD-2179, at *1 (*E.D. La.* Mar. 28, 2011)(order denying assertion of marital privilege and granting access to email communications); Alamar Ranch, LLC v. County of Boise, No. CV-09-004-S-BLW, 2009 WL 3669741, at *4 (D. Idaho Nov. 2, 2009)("It is unreasonable for any employee in this technological age — and particularly an employee receiving the notice Kirkpatrick received — to believe that her e-mails, sent directly from her company's e-mail address over its computers, would not be stored by the company and made available for retrieval. Accordingly, the court finds that Kirkpatrick waived the privilege for those messages she sent from her work computer. With regard to the e-mails Charney [her attorney] sent to her, there is no question that her address . . . clearly put Charney on notice that he was using her work e-mail address. Employer monitoring of work-based e-mails is so ubiquitous that Charney should have been aware that the IHFA would be monitoring, accessing, and retrieving e-mails sent to that address. Given that, the court finds that Charney's e-mails sent to Kirkpatrick's work e-mail are likewise unprotected by any privilege.").

document retention issues;[6] law outside the jurisdictions examined;[7] private and industry guidelines that lack the force of law (although plaintiffs will undoubtedly argue that such guidelines establish reasonableness);[8] and concerns affecting special industries (like government employers, who are bound by the extra considerations required by the First,[9] Fourth, Fifth, and Sixth Amendments to the United States Constitution,[10] and health care providers[11]). Nonetheless, many of the cases related to those issues still will

---

Compare this, however, with the result in *Stengart v. Loving Care Agency, Inc.*, 990 A.2d 650 (N.J. 2010). *See also* Convertino v. United States Dept. of Justice, 674 F. Supp. 2d 97, 110 (D.D.C. 2009)("Mr. Tukel reasonably expected his e-mails with his personal attorney [sent through the DOJ's computer system] to remain confidential.").

6 *See* Evan E. North, Note, "Facebook Isn't Your Space Anymore: Discovery of Social Networking Websites," 58 *U. Kan. L. Rev.* 1279 (June 2010).

7 Although sufficiently intriguing or important cases from all jurisdictions are considered, this chapter focuses on Alabama, Illinois, Indiana, Kentucky, New York, Ohio, Pennsylvania, Tennessee, Virginia, West Virginia, and Wyoming.

8 *See, e.g.*, Fin. Indus. Regulatory Auth., Reg. Notice 10-06, *Guidance on Blogs and Social Networking Web Sites* (Jan. 2010), available at http://www.finra.org/industry/regulation/notices/2010/p120760 (requiring companies to monitor and store certain social media use and communications records).

9 *See, e.g.,* San Diego v. Roe, 543 U.S. 77 (2004).

10 *See, e.g.*, Ontario v. Quon, 130 S. Ct. 2619 (2010); United States v. Bailey, 272 F. Supp. 2d 822, 824 (D. Neb. 2003)("Bailey, a reasonably well educated person, had no expectation of privacy in the work computer owned by someone else because every time he accessed the work computer he physically acknowledged that he was giving consent to search the computer. Such repeated warnings about consent to search, followed by such repeated acknowledgments, categorically and without more defeat Bailey's claim of privacy."); Smyth v. Pillsbury Co., 914 F. Supp. 97, 101 (E.D. Pa. 1996)("In the first instance, . . . we do not find a reasonable expectation of privacy in e-mail communications voluntarily made by an employee to his supervisor over the company e-mail system notwithstanding any assurances that such communications would not be intercepted by management. Once plaintiff communicated the alleged unprofessional comments to a second person (his supervisor) over an e-mail system which was apparently utilized by the entire company, any reasonable expectation of privacy was lost. . . ."); Matthew Tokson, "Automation and the Fourth Amendment," 96 *Iowa L. Rev.* 581 (Jan. 2011); Andrew William Bagley, "Don't Be Evil: The Fourth Amendment in the Age of Google, National Security, and Digital Papers and Effects," 21 *Albany L.J. of Sci. & Tech.* 153 (2011).

11 *See, e.g.*, David Gevertz and Gina Greenwood, "Crafting an Effective Social Media Policy for Healthcare Employees," 22 (No. 6) *Health Lawyer* 28 (Aug. 2010); Lauren B.

warrant investigation because the analyses that courts use to decide them (in particular, whether an objectively reasonable expectation of privacy exists, and whether the monitoring or use of the data gathered was reasonable) translate well to the issues covered here.[12]

Finally, the issues' dynamicity — both legal and factual — means that employers must remain vigilant to frequent changes in both the technological context and the governing legal restrictions. Just like that shiny new smart phone, tablet, or e-reader that you finally got around to buying, legal analysis — especially of technology — quickly becomes outdated.[13] Realistically, an exhaustive analysis of all workplace privacy issues implicated by an employer's monitoring of its workforce's electronic activities would occupy volumes and require constant factual and legal upkeep. The practical goal of this chapter is instead to encourage deliberate reflection about the pervasiveness of technology in the workplace and its role in monitoring employee conduct; to provide enough examples of governing law so that employers are aware of the kinds of potential liability to avoid; and to inspire dialog about solutions.

§ 3.02. Technology that Can Be Used for Monitoring Purposes.

Analysis of the propriety of an employer monitoring its employees' electronic activities first requires spotting the technology, and then understanding which activities are candidates for monitoring and which are not. This section addresses the first issue; later sections will address the others.

Companies communicate using both wired and wireless systems. The two wired technologies most important to most companies are the various flavors of landline voice telephone service and wired data connectivity

---

Solberg, "Data Mining on Facebook: A Free Space for Researchers or an IRB Nightmare?," 2010 *U. Ill. J. L. Tech. & Pol'y* 311 (Fall 2010).

12 *See* Lisa Smith-Butler, "Workplace Privacy: We'll Be Watching You," 35 *Ohio N. U. L. Rev.* 53, 60-63 (2009).

13 The recency of many of the stories noted here is indicative of how frequently new fact patterns present themselves for analysis by legislatures, courts, agencies, and private parties.