PRIVACY IN THE WORKPLACE: ARE COLLECTIVE BARGAINING AGREEMENTS A PLACE TO START FORMULATING MORE UNIFORM STANDARDS?

KARIN MIKA*

TABLE OF CONTENTS

instance, if a camera captures an employee selling drugs on company property, that employee should expect the employer to discharge her.[11] If an employee works for a company where the employee's job is to communicate with customers online, that employee should reasonably expect the employer to discipline him if monitoring discovers that he was surfing the internet rather than dealing with customers.[12] Additionally, an employee who sends threatening or sexually harassing emails through the company computer system also should expect his employer to discipline him.[13]

In each of these cases, most reasonable people would think that the employer was well within its rights to both monitor certain things electronically and discipline an employee where the monitoring discloses inappropriate work conduct. Issues arise, however, in a few major instances:

1. When the action of the employee does not occur during working hours (such as maintaining a personal blog or sending email while at home).[14]

11. *See, e.g.*, Padron v. BellSouth Telecomm., Inc., 196 F. Supp. 2d 1250, 1256 (S.D. Fl. 2002), *aff'd* 62 F. App'x 317 (11th Cir. 2003) (holding that discharge was legitimate when employee violated company policies by accessing a business account for her brother); Terwilliger v. Howard Mem'l Hosp., 770 F. Supp. 2d 980, 982 (W.D. Ark. 2011) (holding that termination was proper when employee was caught on camera stealing or attempting to steal from another employee's desk drawer).

12. *See, e.g.*, Flynn v. AT&T Yellow Pages, 780 F. Supp. 2d 886, 889 (E.D. Mo. 2011) (holding that discharge was proper when an investigation revealed that employee used his work computer for personal activities, including downloading hundreds of files of non-work-related material and surfing the internet for several hours during work time); AFSCME Council 4, Local 1565, 37 Lab. Arb. Info. Sys. 194 (June 3, 2009) (finding that termination was for just cause when an investigation showed that employee spent at least one hour of each work day surfing the internet and that he had actively searched for pornography).

13. *See, e.g.*, Alberto v. Dep't of Veterans Affairs, 98 M.S.P.R. 50, 55 (M.S.P.B. 2004), *aff'd* 05-3090, 2005 WL 1368150 (Fed. Cir. June 10, 2005) (disciplining employee for, among other acts, sending an unsolicited email over his employer's email system that was not business related and contained material of a sexual nature that the recipients found objectionable); Husen v. Dow Chem. Co., 03-10202-BC, 2006 WL 901210, at *3 (E.D. Mich. Mar. 31, 2006) (upholding Arbitrator's decision that the employer was justified in terminating employee for sending sexually explicit emails).

14. *See, e.g.*, Shelby Cnty. Sheriff's Office, FMCS # 08-00865, 2009 WL 7323374, (Dec. 8, 2009) (Fullmer, Arb.) (deputy discharged for, among other acts, blog postings even though he did not use his real name or state that he was an employee of the Sheriff's office); John S. Hong, *Can Blogging and Employment Co-Exist?*, 41 U.S.F. L. Rev. 445, 451 (2007) (programmer Mark Pilgrim fired after his manager demanded Pilgrim abandon his personal blog, which included an essay reflecting on Pilgrim's past addictions to nicotine, alcohol, and marijuana, and in response Pilgrim posted his resume on the blog); Simonetti, *supra*u Tc 0 Tw d af

2. When the employer does not have a policy that prohibits using company equipment for personal use (such as when an employer allows an email account to be used to send and receive personal communications).[15]

3. When the employer acquires the information through indirect means (such as when an email is forwarded or a co-worker "captures" otherwise private information and brings it to the attention of the employer).[16]

4. When the employer acquires information that was originally private (and not at all related to the employer's job duties), happened at some point in the past, but somehow still can be gleaned through an internet search engine (such as when an employer is still able to discover a lewd photo from an employee's college days).[17]

her blog); Kathryn S. Wenner, *Scribe's Secret*, AM. JOURNALISM REV. (Sep. 1, 2002), http://www.ajr.org/article.asp?id=2612 (Houston Chronicle reporter Steve Olafson terminated as a result of postings on his personal blog); Liz Wolgemuth, *Five Ways Your Computer Use Can Get You Fired*, U.S. N

Most employees would not think that their jobs could be at stake

THE FEDERAL WIRETAP ACT AND THE ELECTRONIC COMMUNICATIONS PRIVACY ACT

The primary federal statutes that cover acquiring electronic information are part of what was originally called the Omnibus Crime Control and Safe Streets Act.[23] The original Wiretap Act was enacted in 1968,[24] and the Electronic Communications Privacy Act, which amended the Wiretap Act, was enacted in 1986.[25] The internet did not exist in 1968, and the primary focus of the original Wiretap Act was prohibiting inappropriate interception of telephone communications.[26]

According to the Act it is unlawful for an individual to "intercept or endeavor to intercept, any wire, oral, or electronic communication."[27] A few exceptions were made for providers of the service, employers, and when there was consent for the interception.[28]

responding firms acknowledged doing so. In addition, the Privacy Foundation's Workplace Surveillance Project found that fourteen million American workers are under continuous online surveillance, and that employee-

The use of the word "interception" created such ambiguity that made it difficult to apply this statute to electronic communications that are "acquired" by an employer.[29] Originally, an *interception* was de

one of the major issues related to consent was whether the monitoring went beyond the scope of consent given by the employee.[34]

The Stored Electronic Communications Act, which is part of Title II of the Electronic Communications Privacy Act (ECPA) prohibits the unauthorized "retrieval" of electronic communications and was enacted to close some of the loopholes related to email and other types of stored electronic communication.[35] With respect to employers, courts have interpreted the statute to mean that similar exceptions that apply to intercepted communications, also apply to stored communications.[36] Thus, where an employer retrieved a communication in the ordinary course of business, many courts have held that the statute has not been violated.[37] Moreover, where an employee consented to the monitoring of retrieved information, courts have also concluded that there has been no violation of the statute.[38]

ECPA as they apply to the monitoring of employees' electronic communications).

34. *See, e.g.*, Pure Power Boot Camp v. Warrior Fitness Boot Camp, 587 F. Supp. 2d 548 (S.D.N.Y. 2008); Rassoull v. Maximus, Inc., 93 F. App'x. 495 (4th Cir. 2004); In re Pharmatrak, Inc., 329 F.3d 9 (1st Cir. 2003); Shefts v. Petrakis, 758 F. Supp. 2d 620 (C.D. Ill. 2010); Bohach v. City of Reno, 932 F. Supp. 1232 (D. Nev. 1996).

35. 18 U.S.C. §§ 2701–2712 (2012); *see also* Theofel v. Farey Jones, 341 F.3d 978, 982 (9th Cir. 2003) *opinion amended and superseded on denial of reh'g sub nom.* Theofel v. Farey-Jones, 359 F.3d 1066 (9th Cir. 2004) (noting that the SCA "reflects Congress's judgment that users have a legitimate interest in the confidentiality of communications in electronic storage at a communications facility"). *See generally* Alexander Scolnik, *Protections for Electronic Communications: The Stored Communications Act and the Fourth Amendment*, 78 FORDHAM L. REV. 349, 375 (2009) (describing the Stored Communications Act and its protection of e-mails, text messages, and other forms of electronic communications).

36. The Act exempts conduct "authorized . . . by the person or entity providing a wire or electronic communications service," 18 U.S.C § 2701(c)(1), or "by a user of that service with respect to a communication of or intended for that user,"18 U.S.C § 2701(c)(2).

37. *See, e.g.*, Bohach v. City of Reno, 932 F. Supp. 1232, 1236 (D. Nev. 1996) (holding that messages between employees over City intranet could lawfully be accessed by employer). "§ 2701(c)(1) allows service providers to do as they wish when it comes to accessing communications in electronic storage. Because the City is the provider of the 'service,' neither it nor its employees can be liable under § 2701." *Id.*

38. 18 U.S.C. § 2701(c)(2) (2012); *see also, e.g.*, *Pure Power Boot Camp*, 587 F. Supp. 2d at 599 (holding that accessing and obtaining e-mails directly from an electronic communication service provider is a violation of the SCA if done without authorization).

Note that one of the major issues that arises regarding the authorization exception is to what exactly the employee has consented. For instance, in *City of Ontario v. Quon,* 130 S. Ct. 2619, 2629 (2011), the employee consented to the monitoring of text messaging minutes and destinations, but incorrectly believed that the content of his messages would remain private. The authorization exception may also work in favor of the employee in circumstances where the employer's policy is not specific enough to include the activity that brought about the alleged invasion of privacy. For example, in *Pure Power Boot Camp,* 587 F.NSup-10.7p 2619-10.7d t bri

Courts typically predicate the application of both of these rules on the form and scope of the consent that the employer has obtained. In practice however, most courts have interpreted the provisions of the ECPA broadly in favor of employers.

As previously indicated, there are a great many "retrievals" and "interceptions" that one should not expect an employee to object to. If working for a package delivery company, an employee might expect an employer to object if GPS monitoring demonstrated that the employee made numerous personal detours during the work day. An employee who works for a company that issued him oD 1 >rer a PM

employees might cause to members of the general public if there was a means to discover that the employee was inappropriately dealing with members of the public.[41]

Few people would disagree that it is both the right and responsibility of an employer to have the means to prevent sexual harassment, threats of violence, disclosure of company secrets, or committing crimes on the job. However, few people agree as to the proper boundaries of the employer in accomplishing this goal.

It is rare that any straightforward prerogative of a responsible employer becomes subject to litigation (e.g., checking whether an employee has threatened another employee by using company email). What tends to be litigated, however, are situations when the employer is perceived to have overstepped its bounds. For instance, if an employer, rather than merely monitoring internet usage for efficiency purposes, uses personal information, which could uncover an affair or some other kind of prohibited relationship, for disciplinary purposes. Or if an employer, rather than monitoring whether a phone is being used mostly for work, listens in on conversations to see who is being called and for what. Or when an employer reads the content of personal emails rather than merely determining the identity of the recipient.

Those become difficult matters for courts, especially if an employee has given an employer carte blanche authority to monitor internet usage, phone usage, and email. In those situations, courts tend to look at matters on a case-

an employee that an employer believes reflects badly on the employer. In neither of these cases would the electronic information have been retrieved from an employee's work files or equipment, nor could the information be considered "intercepted." Yet an employee might still be subject to discipline or discharge depending on existing work rules (e.g., "an employee may be discharged for engaging in any activity that, in any way, reflects badly on the employer or is disparaging of the employer"), or even on a mere whim of the employer in the abs

cho (s)3.6(c)-3.9 (ons)3.6(pi)-.4(t)-3.3(oye)6.

COLLECTIVE BARGAINING AND REASONABLE WORK RULES

About the only arena where a workforce has any type of power to negotiate at least some work rules is in collective bargaining.[46] Although union contracts must integrate some aspects of federal law (such as anti-discrimination laws, and adherence to both the Americans with Disabilities Act and the Family Medical Leave Act),[47] union negotiation affords workers the opportunity to craft certain rules unique to an employer or a particular set of workers. With respect to privacy matters, (absent statutory proscriptions) unions might be one of the only groups that have the ability to set out in writing what would be the restrictions of using acquired electronic communications for purposes of making adverse employment decisions.

Currently, discipline and discharges related to electronically acquired information are go-pn4(d)1010.2(i1(by-3.9(re)10.2(i)-)-3.2(ons)3-3.9(m)7.12(p)10.4(l)-3.3(

are encompassed in a collec

CAN UNIONS REALLY NEGOTIATE SUCH A PROVISION?

Currently, only about 11% of the workforce is unionized and many would suggest that unions are not in any type of position of power to be negotiating provisions that give employees more power over their destinies than less. Several states—most noteworthy Ohio and Wisconsin—have enacted legislation that has limited the power of collective bargaining representatives to bargain over wages and benefits for government employees. Economics also play a role related to the power of unions. With much work being outsourced to foreign countries that can perform the work cheaper, unions are rarely in a position of power to be making demands of an employer.

The lack of power of collective bargaining representatives has onsons irc( )10.85()10.,-3.2(oye).9(rnny(h)10.4(e)-3 e)-3.hop repr.3(e)-3.(h3(e)-3.gun EMC /Po

related to the reality of the work environment and situation.[60] This is a power that non-

CONCLUSION

Legislation relating to employee monitoring is a hodge-podge of statutes that do not directly apply to the technologically advanced way that most communications are made today. In addition, statutes, where they exist, neither address situations related to employer scrutiny of communications that an employee might regard as personal (such as posting on a blog or on Facebook), nor those where the employee communicates on his or her own personal device during non-working hours. Because many employees now work on the go on either employer-issued equipment or on personal equipment, the lines between non-working hours and working hours have become blurred, as have become the lines between work and non-work activities. Employees have a right to know what behaviors are considered impermissible. Moreover, it is to the benefit of employers to have clear, enforceable policies that set the guidelines for what is expected from employees.

It is this author's position that although a federal statute could provide some of the guidelines necessary for a 21st century workforce, passing an all-encompassing statute that covers various unique workplace situations will be difficult. Moreover, although various proposed statutes deal with restrictions on monitoring, they do not necessarily encompass situations where disciplines from communications are made known to an employer although not "monitored" in the traditional sense. The author believes that it would be beneficial to both employers and employees to define what