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

KARIN MIKA*

TABLE OF CONTENTS

INTRODUCTION

With the explosion of technology has come the opportunity for nearly every aspect of a person's life to be monitored.[1] A phone GPS can detect a person's whereabouts at any time; keystroke monitors can record anything a person types on a keyboard; cameras can and do monitor movements in schools, stores, parking lots, homes, and many other places; software can capture real-time chats; email can be accessed by the provider of the service; and internet access points can be pinpointed, even if a person is not using his/her own computer.

* Professor of Legal Writing, Cleveland-Marshall College of Law. I would like to thank my research assistant Monica Giangardella for all of her help. I would also like to thank Ariana Levinson of the University of Louisville Law School, who is, as far as I'm concerned, the expert in the field of electronic privacy law.

1. *See generally* Daniel Solove, *The Digital Person: Privacy and Technology in the Information Age* (2004) (exploring how public-and private-sector databases create "digital dossiers"—a perpetual series of records detailing nearly every aspect of a person's life).

None of these technologies even consider the voluntary nature of disclosed personal activities—Facebook, internet blogs, listserv discussions, twitter posts, and even forwarded emails.[2] For all intents and purposes, our lives are open books, even if we take great strides to limit our disclosures.

One area where this becomes especially problematic is in the workplace.[3] Although most people would agree that employers have many rights when it comes to scrutinizing arguably "personal" activities—sending threatening or harassing communications to co-workers, using work time to engage in personal social networking, or disclosing company secrets[4]—many employees have run into situations where employers may have crossed the line when disciplining or discharging an employee for personal activities that seem unrelated to the job.[5] These activities include those that occur outside of work, such as the posting comments on a personal (or even anonymous public) blog,[6] or posting pictures and/or comments on a quasi-private Facebook page.[7] The activities may also include those

---

2. *See* Tonn Petersen, *Redefining "Privacy" in the Era of Social-Networking,* 53 ADVOC. 27 (2010) (discussing the "exploding popularity of social networking" sites).

3. *See generally* Ariana R. Levinson, *What Hath the Twenty First Century Wrought? Issues in the Workplace Arising from New Technologies and How Arbitrators are Dealing with Them,* 11 TRANSACTIONS: TENN. J. BUS. L. 9 (2010).

4. *See, e.g.*, Neal Buethe & Sally Scoggin, *Doocing the Blogzilla: Managing Workplace E-Communications,* BENCH & B. MINN. (June 1, 2007*), available at* http://mnbenchbar.com/2007/06/e-communications/ (employee fired after "reportedly post[ing] satirical accounts of life at work" on her personal blog); *see also* Doe v. XYC Corp.*,* 887 A.2d 1156, 1158 (N.J. Super. Ct. App. Div. 2005) (holding that an employer having "notice that one of its employees is using a workplace computer to access [child] pornography . . . has a duty to . . . take prompt and effective action to stop the unauthorized activity").

5. *See, e.g.*, City of Ontario v. Quon, 130 S. Ct. 2619 (2010) (holding that employer had a right to review lewd text messages sent on Company issued Blackberry); *see also* Bob E. Lype, *Employment Law and New Technologies: Emerging Trends Affecting Employers*, 47 TENN. B.J. 20 (2011); Robert Sprague, *Orwell was an Optimist: The Evolution of Privacy in the United States and its De-Evolution for American Employees*, 42 J. MARSHALL L. REV. 83 (2008).

6. *See* Robert Sprague, Fired for Blogging: Are There Legal Protections for Employees Who Blog?, 9 U. PA. J. LAB. & EMP. L. 355 (2007); *see also* Marshall v. Mayor of Savannah, 366 F. App'x 91 (11th Cir. 2010) (discharge for posting "inappropriate" photos on MySpace); Shelby Cnty. Sheriff's Office, FMCS # 08-00865, 2009 WL 7323374 (Dec. 8, 2009) (Fullmer, Arb.) (discharge even though employee blogged with a pseudonym); Ellen Simonetti, *I was fired for blogging*, CNET NEWS (Dec. 16, 2004, 4:00 AM), http://news.cnet.com/I-was-fired-for-blogging/2010-1030_3-5490836.html.

7. *See, e.g.*, Don McIntosh, *Workers Fired for Facebook Posts; NLRB Investigates,* NORTHWEST LABOR PRESS (May 6, 2011), http://www.nwlaborpress.org/2011/0506/5-6-11FB.html (employee filed complaint with NLRB after she was fired for venting about her job to friends via Facebook posts); *Auto Club Fires 27 in Message Board Crackdown*, USA

that occur during the work day, such as forwarding a seemingly innocuous email, or making a personal comment in an email when there is no general prohibition on this activity.

In most instances, neither the employer nor the employee is truly of certain of his or her rights or obligations. However, in most cases, it is usually the employee who suffers the consequences when the employer decides that an activity discovered through electronic monitoring is something that should be subject to discipline or discharge.

This article will examine the issues regarding employee privacy created by a world where nearly everything can be discovered by some form of electronic monitoring. It will posit that most laws today do little to apprise either the employer or the employee of the legality of electronic monitoring of personal communications. It will further posit that most employer policies related to scrutinizing employee electronic communications are vague and unsuitable. The article will moreover assert that, given the (often justifiable) leeway that employers tend to have in monitoring employees, there is little chance that we will soon see any standardization of laws regarding what can be done with electronically obtained information.

The author concludes that vague privacy laws and policies are bad for both employers and employees, and result in unnecessary litigation. In doing so, the author demonstrates that the only real standardization we might expect to see regarding any limitation employers may have in using electronically obtained personal information would have to come from the unions and union negotiation. Given that the current laws regarding obtaining and using electronic communications are inconsistent at best, it may only be strong unions that are be able to negotiate clauses that provide the definitive limitations for when an employer may use electronically obtained personal communications for purposes of discipline or discharge. Standardized policies would be beneficial for both employers and employees, and if these policies begin to exist in the unionized sector, we may see more of them adopted in the private sector.

TODAY (Aug. 6, 2005, 12:42 AM), http://www.usatoday.com/tech/news/2005-08-06-posters-fired_x.htm (auto club workers fired for posting work-related messages on a social networking site).

EXACTLY WHAT CAN AN EMPLOYER MONITOR AND WHAT CAN BE DONE WITH IT?

Both employers and employees often ask (1) what is allowed to be monitored and (2) what can be done with the resulting information. The answers to both questions are an employer can monitor virtually anything, and almost anything can be done with the monitored communication.[8] Limitations are few and far between, especially if the employer has posted a monitoring policy.[9] Additionally, courts are generally willing to uphold discipline and discharges of employees as long as the action resulted from the discovery of an activity that had some relationship to work duties.[10]

In terms of employee monitoring, the truth is that there are some things every employee knows he or she should not be doing over the employer's internet or email system, and that person should not be surprised when there are consequences for such actions. Most situations are matters of common sense and have nothing to do with whether the information was discovered by electronic means. For

---

8. *See, e.g.*, Mindy C. Calisti, *You Are Being Watched: The Need for Notice in Employer Electronic Monitoring*, 96 KY. L.J. 649, 662 (2008) (noting that "very few states regulate employers' monitoring of e-mail and Internet activity").

9. *See, e.g.*, Smyth v. Pillsbury Co., 914 F. Supp. 97, 101 (E.D. Pa. 1996) (upholding employee discharge for the inappropriate content of an e-mail, despite the fact that the company had stated that it would not monitor e-mail messages); Cicero H. Brabham, Jr., *Curiouser and Curiouser: Are Employers the Modern Day Alice in Wonderland? Closing the Ambiguity in Federal Privacy Law As Employers Cyber-Snoop Beyond the Workplace*, 62 RUTGERS L. REV. 993, 1018 (2010) (discussing how employers now reference their monitoring policies to claim legitimate access to employees' cyber activities). In a *Wired* magazine article, one author suggests that notice of monitoring is the central consideration:

> [I]f an employee is led to expect something is private, such as e-mail communications, then that privacy cannot be violated. But, if the company informs its employees that, for example, e-mail sent over the company's network is monitored, then the employee can no longer claim an "expectation of privacy." In short, once the company stakes its claim over its cyber-dominion, its employees have no right to privacy there.

Jeffrey Benner, *Privacy at Work? Be Serious,* WIRED NEWS (Mar. 1, 2001), http://www.wired.com/techbiz/media/news/2001/03/42029.

10. *See* Richerson v. Beckon, 337 F. App'x 637, 638–39 (9th Cir. 2009), as amended (Aug. 27, 2009) (holding that transfer of employee to a different position was proper on grounds that her internet blog included highly personal and offensive comments about her employers, union representatives, and fellow teachers). *But see* Donald Carrington Davis, *Myspace Isn't Your Space: Expanding the Fair Credit Reporting Act to Ensure Accountability and Fairness in Employer Searches of Online Social Networking Services*, KAN. J.L. & PUB. POL'Y 237, 244 (Winter 2006–07) (pointing out that online social networking profiles often present personal information about a potential employee that would not be appropriate subjects of employer-employee dialogue within the scope of the hiring process, i.e. religious views).

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* note 6 (Delta Airlines flight attendant fired after posting risqué pictures of herself in her uniform on

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. NEWS & WORLD REP. (Mar 11, 2008), http://www.money.usnews.com/money/careers/articles/2008/03/11/5-ways-your-computer-use-can-get-you-fired (CNN producer Chez Pazienza fired when the company discovered his personal blog).

15. *Compare* Leventhal v. Knapek, 266 F.3d 64, 74 (2d Cir. 2001) (holding that employee had reasonable expectation of privacy in contents of workplace computer where the employer did not have a general practice of routinely searching office computers, and had not notified the plaintiff that he should have no expectation of privacy in the contents of his office computer), *with* Kelleher v. City of Reading, No. CIV.A.01-3386, 2002 WL 1067442, at *8 (E.D. Pa. May 29, 2002) (holding that employee did not have a reasonable expectation of privacy as to her e-mail messages sent and received using the employer-provided e-mail system, because the employer's guidelines explicitly provided that there was no such expectation of privacy).

16. *See, e.g.*, Wall St. Source, Inc. & Niki Lee, No. 2-CA-38727, 2009 WL 909251 (N.L.R.B. Apr. 1, 2009) (employee fired when IM exchanges with fellow employee complaining about the company's insurance policies were forwarded to supervisor); Kathleen Elliott Vinson, *The Blurred Boundaries of Social Networking in the Legal Field: Just "Face" It*, 41 U. MEM. L. REV. 355, 399 (2010) (discussing a judge's discovery, by way of Facebook, that an attorney who had asked for a continuance due to an alleged death in the family had instead engaged in a week of partying); Rick Borutta, *Waitress Serves Sour Grapes on Facebook, Gets Fired,* CBS NEWS (May 25, 2010), http://www.cbsnews.com/8301-501465_162-20005894-501465.html (waitress fired for complaining about customers on her Facebook page).

17. *See, e.g.*, Emily H. Fulmer, *Privacy Expectations and Protections for Teachers in the Internet Age,* 2010 DUKE L. & TECH. REV. 14, 53 (2010) (teacher allegedly coerced by school administrators into resigning after they questioned photographs on the teacher's Facebook

Most employees would not think that their jobs could be at stake on the basis of having done something regrettable during a spring break trip while in college, or by griping to a friend on Facebook about a bad day at work; however, that is exactly what can occur.[18]

THE ELECTRONIC MONITORING LAWS AS THEY NOW STAND

The laws regarding the "interception" and use of electronic "communications" is a hodgepodge of federal and state rules.[19] Some were enacted at a time when the internet did not exist,[20] while others were enacted without foresight as to how they might be employed in the workplace.[21] The application of these laws to discharge situations requires judges and arbitrators to "put a square peg in a round hole." While lawmakers may have envisioned monitoring employees' work-related, egregiously inappropriate behavior, in practice it has extended far outside of the regular workday.[22]

---

page that were taken during a past European vacation and depicted her with alcoholic beverages); *see also* Catharine Smith & Craig Kanalley, *Fired over Facebook: 13 Posts that Got People Canned*, HUFFINGTON POST (July 26, 2010), http://www.huffingtonpost.com/2010/07/26/fired-over-facebook-posts_n_659170.html#s115707&title=Swiss_Woman_Caught.

18. *See, e.g.*, Davis, *supra* note 10, at 239 (citing a survey finding that sixty-three percent of employers that search social networking profiles online have rejected candidates based upon information found within those profiles).

19. *See generally* Dorothy Glancy, *At the Intersection of Visible and Invisible Worlds: United States Privacy Law and the Internet*, 16 SANTA CLARA COMPUTER & HIGH TECH. L.J. 357, 359 (2000) (describing United States privacy laws as "a very diverse collection of many different types of privacy laws," which has generated widespread criticism of America's privacy laws as "piecemeal" or "fragmented"). "A number of years ago a federal appeals court judge described United States privacy law as like a 'haystack in a hurricane.'" *Id.*

20. *See, e.g.*, Communications Act of 1934, 47 U.S.C. §§ 151–621 (2012); Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. §§ 2510–22 (2012); Wiretap Act of 1968, 18 U.S.C. §§ 2511–19 (2012); Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510–21, 2701–10, 3121–26 (2012); Stored Communications Act of 1986, 18 U.S.C. §§ 2701–11 (2012). *See generally* Susan Freiwald, *Online Surveillance: Remembering the Lessons of the Wiretap Act*, 56 ALA. L. REV. 9, 41 (2004) (emphasizing that "when Congress passed the ECPA [Electronic Communications Privacy Act] in 1986, electronic communications were in their infancy," the World Wide Web had not yet been developed, and only a small number of people used electronic mail).

21. *See, e.g.*, Corey A. Ciocchetti, *The Eavesdropping Employer: A Twenty-First Century Framework for Employee Monitoring*, 48 AM. BUS. L.J. 285, 293–94 (2011) (pointing out that the Electronic Communications Privacy Act is futile in today's workplace environment, because "technology has advanced to a point that almost no transmissions are covered by the statute").

22. *See* Charles E. Frayer, *Employee Privacy and Internet Monitoring: Balancing Workers' Rights and Dignity with Legitimate Management Interests*, 57 BUS. LAW. 857, 859 (2002) (noting that "[a]ccording to the American Management Association, which asked employers whether they monitor Internet connections, an astounding sixty-one percent of

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-monitoring software sales have reached $140 million annually."). *But see, e.g.*, COLO. REV. STAT. § 24-34-402.5 (2012) (forbids termination by employer based on "any lawful activity [conducted] off the premises of the employer during nonworking hours . . . ."); N.D. CENT. CODE § 14-02.4-03 (2011) (forbids failing or refusing to hire, in addition to forbidding discharge, based on lawful off-duty conduct during nonworking hours); *see also* Davis, *supra* note 10, at 245–46 (noting that some states have placed limits on employer monitoring outside the workplace).

23. Omnibus Crime Control and Safe Streets Act of 1968, *supra* note 20.

24. *See* JUSTICE INFORMATION SHARING, U.S. DEPARTMENT OF JUSTICE, OFFICE OF JUSTICE PROGRAMS, *Privacy and Civil Liberties* (Mar. 20, 2012), http://it.ojp.gov/default.aspx?area=privacy&page=1284 (Title III of the Omnibus Crime Control and Safe Streets Act was known as the "Wiretap Act." The Act strictly regulates the interception of wire and oral communications, providing both criminal and civil liabilities for violators of the statute's prohibitions. Congress passed the Act in response to investigations and studies finding extensive wiretapping had been conducted by government agencies and private individuals without the consent of the parties or legal sanction.).

25. Electronic Communications Privacy Act of 1986, *supra* note 20; *see also* Jarrod J. White, *E-Mail@work.com: Employer Monitoring of Employee E-Mail,* 48 ALA. L. REV. 1079, 1080–81 (1997) ("The ECPA amended Title III of the Omnibus Crime Control and Safe Streets Act of 1968, and was passed in response to Congress' perception that the privacy protection of the 1968 Act was limited to narrowly defined 'wire' and 'oral' communication.").

26. *But see* United States v. Councilman, 418 F.3d 67, 79 (1st Cir. 2005) (analyzing application of the Wiretap Act outside the context of telephone communications, holding that "temporarily stored e-mail messages . . . constitute electronic communications within the scope of the Wiretap Act . . . .").

27. 18 U.S.C. § 2511(1)(a) (2012).

28. *Id.* §§ 2511(2)(d)–(e). Consent is an overlapping concept, because a person who is employed could theoretically consent directly to a particular type of monitoring, or consent to refraining from doing something in a very broad sense (such as maintaining a harassment free

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 defined as acquiring the contents of a communication while the communication was in transit prior to its arriving at its destination (such as listening in on a phone conversation).[30] However, many of these courts were forced to struggle with the technical details of email messages in an attempt to determine whether the message was intercepted en route, or acquired after it had been delivered.[31]

Also at issue, at least in terms of the employer and employee relationship, was whether an interception, if it occurred in a legal sense, fell within one of the statutory exceptions.[32] The two primary exceptions to the statute are related to (1) whether the interception occurs within the ordinary course of business, and (2) whether the employee has consented to the monitoring.[33] As previously indicated,

---

environment at work). Consent need not be explicit, it can also be implied. *See* Williams v. Poulos, 11 F.3d 271, 281 (1st Cir. 1993). "Implied consent is 'consent in fact' which is inferred from surrounding circumstances indicating that the party *knowingly* agreed to the surveillance." *Id.* The indirect consent is what can be expanded so that the employee might be consenting to monitoring not originally considered.

29. *See generally* Michael D. Roundy, *The Wiretap Act-Reconcilable Differences: A Framework for Determining the "Interception" of Electronic Communications Following United States v. Councilman's Rejection of the Storage/transit Dichotomy*, 28 W. NEW ENG. L. REV. 403, 414 (2006) (noting that the question of when the acquisition of an electronic communication constitutes an "intercept" in violation of the Act is one that has posed major challenges for courts).

30. *See, e.g.*, Deal v. Spears, 980 F.2d 1153 (8th Cir. 1992) (finding an interception when defendant store owners used a recording device to monitor telephone calls to and from the store).

31. *See, e.g.*, United States v. Councilman, 418 F.3d 67 (1st Cir. 2005); Hall v. EarthLink Network, Inc., 396 F.3d 500 (2d Cir. 2005); Steve Jackson Games, Inc. v. U.S. Secret Serv., 36 F.3d 457 (5th Cir. 1994).

32. *See, e.g.*, Williams v. Poulos, 11 F.3d 271, 280 (1st Cir. 1993) (holding that defendant company's system for electronically monitoring employee phone calls was not protected by neither the "business extension" nor "consent" exceptions to federal wiretap law, and that the system was "precisely the type of intercepting device Congress intended to regulate heavily when it enacted Title III"); Watkins v. L.M. Berry & Co., 704 F.2d 577, 581 (11th Cir. 1983) (analyzing the applicability of the consent exception in a Title III action brought by an employee of a telemarketing firm based upon her employer's interception of a personal telephone call); Briggs v. Am. Air Filter Co., 630 F.2d 414, 420 (5th Cir. 1980) (holding that where a supervisor listened in on a business call between an employee and his friend, an employee of a competitor, based on his suspicion that the employee was revealing confidential information to the competitor, his actions fell under the business use exemption).

33. 18 U.S.C. §§ 2511(2)(d), (e); *see also* Benjamin F. Sidbury, *You've Got Mail . . . and Your Boss Knows It: Rethinking the Scope of the Employer E-Mail Monitoring Exceptions to the Electronic Communications Privacy Act*, 2001 UCLA J. L. & TECH. 5 (2001) (discussing the "consent" and "ordinary course of business" exceptions to Title III of the

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. Supp. 2d at 559, the court held that the employer's consent defense, which was based on the company's email policy, could not apply to e-mails on systems maintained by outside entities such as Microsoft

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 or her a cellphone might expect that employer to object if scrutiny of cellphone usage revealed that the employee was making personal calls that were charged to the company. An employee of a customer service firm might expect an employer to object if screen captures demonstrated that the employee was doing things on the internet other than dealing with customers. Quite often, employees will acknowledge an employer's right to so monitor when accepting an offer of employment.

But in terms of what might be monitored on the job, employers have other concerns that go beyond productivity and profitability. Employers are obligated to provide a safe and non-threatening environment for employees[39] and often have internal policies regarding safety, and proscribing threatening behavior (both sexual threats and harassment, as well as physical threats). Employees can easily prevail in an action against the employer if inappropriate behavior occurs in the workplace and the employer "should have known about it."[40] Moreover, employers are liable for harm

---

or Google, because the policy, by its own terms, was limited to "Company equipment." *See also TBG Ins. Services Corp. v. Superior Court,* 117 Cal. Rptr. 2d 155, 163 (Cal. Ct. App. 2002) (holding that employee had no reasonable expectation of privacy when he used his home computer for personal matters, because he had consented to such monitoring by signing his employer's "electronic and telephone equipment policy statement," thus agreeing in writing that his employer could monitor his computers).

39. *See, e.g.*, Garrity v. John Hancock Mut. Life Ins. Co., No. 00-12143-RWZ, 2002 U.S. Dist. LEXIS 8343, at *6 (Mass. Dist. Ct. 2002) (holding that even if the employees terminated for sending sexually explicit emails had a reasonable expectation of privacy in their work email, the employer's legitimate business interest in protecting its employees from harassment in the workplace would likely trump the two former employees' privacy interests). *See generally* Meritor Sav. Bank v. Vinson, 477 U.S. 57, 76 (1986) (explaining that a supervisor's responsibilities do not begin and end with the power to hire, fire, and discipline employees, but rather he or she is also charged with the day-to-day supervision of the work environment and with ensuring a safe, productive workplace).

40. *See* Hawkins v. Anheuser-Busch, Inc., 517 F.3d 321, 341 (6th Cir. 2008) (holding

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-by-case basis and assess what was an individual's expectation of privacy, and whether an employer may have overstepped the bounds of its consent to monitor.

However, many alleged invasions of privacy in the workplace have nothing at all to do with either monitoring or retrieval. Consider the matter of the forwarded email that a co-worker regards as sexually harassing, or even the forwarded email that expresses personal sentiments that were intended to be private. Consider also a situation where browsing the internet yields a discovery of information about

---

that an employer's responsibility to prevent future harassment is heightened where it is dealing with a known serial harasser and therefore has clear notice that the same employee has engaged in inappropriate behavior in the past); Fuller v. City of Oakland, Cal., 47 F.3d 1522, 1528 (9th Cir. 1995) (holding that once an employer knows or should know of harassment, a remedial obligation kicks in).

41. *See, e.g.*, Med. Assur. Co., Inc. v. Castro, 302 S.W.3d 592, 597 (Ark. 2009) (holding that an employer may be held directly liable when an employee harms a third party and the employer knew or should have known of the danger).

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 absence of any work rules, such as in an at-will employment situation.[42]

And perhaps the question that many might ask is, is this fair—especially if it is not the employee who has made the information available to the employer, but rather a third party?

Certainly an employee who is complaining to a friend about a bad day at work (whether the communication happens through a company email or during an after-hours Facebook chat), would neither expect the conversation to get back to her employer, nor expect to be disciplined for it, but it does happen. From an employer's perspective, if one person can discover the information, it can be discovered by a multitude of people. If the information disparages the reputation of the employer or puts the employer in jeopardy of liability, then the employer should be able to discipline or discharge the employee. Thus, absent clear policies about what can be used for disciplinary purposes, chances are that anything discoverable on the internet is fair game for use as a basis for discipline or discharge.

Although it would be ideal to suggest that federal and state laws should be modified to compel employers to write policies that explain what electronic information could be used and how, this is an unrealistic goal. Given that majority of employees are at-will, it is unlikely that there would be any real motivation for employers to explain what will not be used. Rather, it might be in the best interests of the employer to keep any policies it has as broad as possible in order to cover situations that are not necessarily foreseeable.

That said, this might not be the best tactic to take when formulating work rules or even unwritten policies. It is generally

42. *See, e.g.*, Smyth v. Pillsbury Co., 914 F. Supp. 97, 101 (E.D. Pa. 1996) (holding that the termination of the plaintiff employee for transmitting inappropriate and unprofessional comments over the employer's email system was proper, even though the employer had no policy forbidding the sending of such emails).

agreed that employees have the right to engage in discussions about "conditions in the workplace."[43] Criticizing management is sometimes considered to be part of discussing conditions of the workplace, and various courts,[44] as well as the National Labor Relations Board, have upheld an employee's right to engage in dialogue critical of management without fear of reprisal.[45] But there is a question as to when critical statements aimed at perhaps improving a work situation become disparaging, derogatory, or nonproductive. At what point does an employee lose his/her right to vent on, for example, a public internet forum? Also, does it matter what line of work that employee is in? Where the lines are should be more specifically spelled out in order to benefit both employers and employees.

---

43. Under the National Labor Relations Act (NLRA), codified as amended at 29 U.S.C. § 151–69, disciplining an employee for discussing conditions of employment may be considered an unfair labor practice if the discussion involved a protected concerted activity. Under section 7 of the Act, concerted activities are those that are engaged in "for the purpose of collective bargaining or other mutual aid or protection." 29 U.S.C. § 157. *See, e.g.*, Carson Strege-Flora, *Wait! Don't Fire That Blogger! What Limits Does Labor Law Impose on Employer Regulation of Employee Blogs?,* 2 SHIDLER J. L. COM. & TECH. 11, 12 (2005) (discussing the limits imposed by the NLRB on employers' regulation of employee blogging and noting that before disciplining a blogging employee, the employer must determine if the blogger is engaged in protected "concerted activity." For example, if an employee can show that complaints made about a supervisor are aimed at initiating, inducing, or preparing for group activity, such discussion may be protected under the NLRA.).

44. *See, e.g.*, Konop v. Hawaiian Airlines, Inc., 302 F.3d 868 (9th Cir. 2002) (protecting employee's right to maintain a website in which he posted bulletins using strong language attacking his employer's management and president); NLRB v. Oakes Mach. Corp., 897 F.2d 84, 86 (2d Cir. 1990) (finding that three employees were protected when they wrote a letter complaining about the activities of their company's president). *But see* NLRB v. Sheraton P. R. Corp., 651 F.2d 49, 51-52 (1st Cir. 1981) (holding that employee protest over general manager was not protected since it was essentially a dispute among managers and had no distinct impact on working conditions).

45. *See, e.g.*, Steven Greenhouse, *Labor Panel to Press Reuters Over Reaction to Twitter Post* (April 6, 2011), http://www.nytimes.com/2011/04/07/business/media/07twitter.html?_r=2&scp=1&sq=reuters%20and%20twitter&st=cse (discussing the NLRB's defense of a reporter reprimanded for a public Twitter post criticizing management. The NLRB asserted that disciplining the employee violated her right to discuss working conditions.); Sam Hananel, *Feds Settle Case of Woman Fired over Facebook Comments* (February 7, 2011), http://www.msnbc.msn.com/id/41465076/ns/technology_and_science-tech_and_gadgets/t/feds-settle-case-woman-fired-over-facebook-comments/ (discussing the NLRB's settlement of lawsuit brought on behalf of a woman fired for criticizing her boss on her Facebook page. The Board argued that the employer's Internet policies interfered with workers' right to discuss wages, hours, and working conditions with co-workers.).

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 governed by a union employee's collective bargaining agreement and its grievance procedure. Very few of these collective bargaining agreements include any specific provisions related to the use of electronic information, or even rules regarding what, specifically, will be monitored.

In a collective bargaining setting, work rules are generally the prerogative of the employer and are not even negotiated with the union. According to the NLRA, employers working with a union must negotiate the "terms and working conditions" of employment. Quite often, the terms and working conditions of employment are interpreted to mean (for the most part) hours, wages, lay-off procedure, disciplinary step procedures, job duties, and seniority rights.[48] Ordinarily, things like lunch breaks, attendance policies, vacation selection, and policies regarding a non-threatening work environment are encompassed by a company's work rules, and, in general, formulating work rules are the prerogative of the employer. Often the rights to manage the workforce and formulate work rules

46. Those negotiating individual contracts have the power to negotiate some aspects of their working environment. Professional athletes can do some of the same but are also represented by a collective bargaining unit.

47. *See* 5 U.S.C. §§ 7201–03 (2012).

48. Note that some state legislatures are now attempting to block unions from negotiating over pension contributions. *See, e.g.*, *Florida Teachers File Lawsuit Over Pension*, NBC MIAMI (June 21, 2011), http://www.nbcmiami.com/news/local/Florida-Teachers-File-Lawsuit-Over-Pension-124281874.html (discussing a lawsuit filed by the Florida Education Association challenging a recent law requiring teachers, state workers, and many local government employees to contribute 3 percent of their pay to the state pension fund).

are encompassed in a collective bargaining agreement's management rights clause.

Sometimes, however, a union will reserve the right to negotiate over work rules, or just some specialized "term and working condition," (such as an attendance policy) while allowing the company to formulate other work rules and general policies. In some instances, work rules are incorporated into a collective bargaining agreement through negotiation, and thus the rules themselves may not be changed during the life of the agreement absent negotiation. Finally, sometimes there is a dispute as to whether a clause is a "rule" that management may change unilaterally, or a contractual provision where a change must be negotiated. When there is a dispute, the matter may be submitted to arbitration, or an unfair labor charge (failure to negotiate a unilateral change in terms and conditions of working conditions) may be brought before the National Labor Relations Board. If an employer adds a new work rule (such as a new policy on electronic monitoring) that was not a variation of what was already part of the contract, both arbitrators and courts have determined that a unilateral change cannot be made absent negotiation with the union.

Thus, when collective bargaining tribunals have attempted to interpret clauses related to the use of electronically acquired information, they have done so by interpreting more general clauses as opposed to specific clauses. Most disputes that have been arbitrated have taken more of a common sense, balancing of factors interpretation when applying work rules. Although some arbitrators have been called on to interpret work rules as they related to electronically acquired information, few (if any) have had the opportunity to interpret very specific clauses related to the use of electronically acquired information, especially information that was not acquired by on-the-job monitoring.

A few specific cases demonstrate some of the ways in which arbitrators have applied more general work rules in relation to electronically acquired information.

For instance, in *In re Baker Hughes* and *United Steelworkers*,[49] the arbitrator upheld the discharge of an employee who posted derogatory remarks about his supervisor on his MySpace page.[50] The

49. 128 Lab. Arb. (BNA) 37, (April 9, 2010) (Baroni, Arb.).

50. The employee had posted, "Ask any Baker Petrolite Employee what they think of the upper management. You might (hear) the words . . . German, green card terminator or

posting was done while the employee was off the job, and appeared on a MySpace blog that was open to the general public. In finding discharge appropriate, the arbitrator noted that the company had a code of conduct rule that prohibited threatening and harassing behavior, and further noted that the collective bargaining agreement gave the employer the right to adopt and enforce work rules. The arbitrator further determined that off-duty conduct could be punished if there was a sufficient nexus to the workplace.[51]

In *In re Shelby County Sheriff's Office,* and *FOP, Ohio Labor Council, Inc.*[52], the Arbitrator upheld the discharge of a police officer who had posted comments on a public blog. The comments criticized an individual who had been running for office, and alleged that a secretary had advanced her career by "sleeping around." Among other charges, the employee was accused of violating a work rule that prohibited an employee to "publicly criticize or ridicule the Sheriff's Office, its policies, personnel, or supervisors." In that case, the posted statement was made on a public blog, but the employee used a pseudonym rather than his real name (although he never denied that he was the one who posted the statements).

The arbitrator noted that, even though the union argued that the comments were protected by the First Amendment, there was nothing political at issue that would be protected by the First Amendment, given the critical comments occurred long after the election mentioned was over. The arbitrator also stated that even though no humiliation was intended by accusing the secretary of sleeping around (in fact, the union argued that the employee had made truthful statements), the topic was humiliating.[53] Thus, the arbitrator concluded, the work rule had been violated and the discharge was appropriate.[54]

Finally, in *In re Warren*[55] the arbitrator upheld the discharge of a teacher whose estranged wife posted nude pictures of her ex-husband

---

some other four letter words that I won't etch down on the scrolls. That's enough said on that subject. I could have sworn that Hitler committed suicide. Is there such a thing as reincarnation?" *Id.* (No pagination designated in the case.).

51. *Id.*; *see also* Burlington Indus., Inc. v. Ellerth, 524 U.S. 742, 748 (1998); Meritor Sav. Bank, FSB v. Vinson, 477 U.S. 57, 60 (1986); Ferris v. Delta Air Lines, Inc., 277 F.3d 128, 135 (2d Cir. 2001); Tomka v. Seiler Corp., 66 F.3d 1295, 1301–02 (2d Cir. 1995).

52. FMCS No. 08-00865, 2009 WL 7323374 (Dec. 8, 2009) (Fullmer, Arb.).

53. *Id.*

54. It should be noted that the employee was accused of many more work violations, so it is tough to separate any rule of law about electronic communications from the rest.

55. 124 Lab. Arb. (BNA) 532 (Oct. 4, 2007) (Skulina, Arb.).

on the internet so that students were able to see the pictures. In finding the discharge appropriate, the arbitrator noted that the Ohio Revised Code provided that teachers could be fired for engaging in immoral behavior. Although the arbitrator concluded that the pictures themselves were not immoral given that they were intended to be a private matter between husband and wife, the situation changed when they made their way to the internet. The arbitrator stated that although the teacher did not post the pictures, he was in a position to take steps to try to stop them from being posted and did not do enough. The arbitrator also stated that because the pictures made their way to the internet, the teacher could no longer undo the situation, and, therefore, the teacher could not rehabilitate his reputation and be an appropriate role model for his students.

In each of these situations, arbitrators took a common sense, case-by-case, totality of the circumstances view of resolving issues not directly controlled by any work rules or contractual provisions. While this has its benefits in the realm of labor law (especially given that majority of all labor arbitrations must look at balancing the unique factors of each case), the case-by-case methodology has its detriments outside the realm of labor law, where the damages can go beyond reinstatement and back pay.

Moreover, even in labor law, resolving issues can be made easier if there is clearer guidance for the parties and the arbitrator. If contractual provisions are clear and spell out specific instances of prohibited conduct, then it would ultimately be unnecessary for the parties to go through the grievance process and labor arbitration. For instance, in both *Baker* and *Shelby*, clear policies providing that electronic postings made about work related issues on public blogs were subject to discipline under the collective bargaining agreement may have made the employees think twice about posting on the internet. The teacher's discharge in *Warren* might have been prevented if there had been a clear policy indicating that a teacher was required to give notice of what amounted to a confidentiality breach compromising a teacher's reputation. Moreover, a clear policy related to internet posting by a third party might better protect an employer if a civil suit were brought by the teacher.

Unfortunately, too often, attorneys who are in the position to advise employers do not consider all of the measures that might be taken to avoid litigation. Rather, work rules and other policies tend only to be modified after a particular scenario has occurred or there has been costly litigation.

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 led to give backs and the elimination of numerous provisions in a collective bargaining agreement that may have been standard in many professions 40 years ago. Collective bargaining agreements often limited the use of independent contractors, and, moreover, focused promotions more on a seniority system rather than a system of merits or a review of qualifications. With the overall professionalism of the workforce, many union shops have begun looking more like private employers, nearly to the point where some unionized workforces have fewer protections than an at-will workforce.

As this article previously discussed, employers should and do have many rights regarding what on-the-job policies are best to ensure the success of the Company, and these may vary from employer to employer. One area where the rules have increased vastly in the last three decades has been in the area of drug testing. Few people would argue that an employer should not have the right to prevent a pilot suspected of being intoxicated from flying an airplane and then later disciplining that pilot if it was proved the pilot had been intoxicated. Moreover, it would not be unreasonable for an employer to fire an employee for being intoxicated while operating heavy machinery where being intoxicated could be dangerous to that employee and other employees. In fact, it would be hard to argue that an employer would not want any drugged or inebriated workers on the job whether a safety concern could become a main issue. Simply put, inebriated (or drugged) employees have their ability to function hindered, and this could result in a deficient work product that causes the employee profit or resources.

Although there has been drug testing in some professions for a long period of time, the real movement toward overall drug testing

began in the mid 1980s when Ronald Reagan signed an executive order that conditioned federal employment on refraining from (illegal) drug use, on or off the job. In 1988, Congress enacted the "Drug-Free Workplace Act."[56] Thereafter, the concept of routine drug testing became something more and more commonplace as time went on.[57]

The "War on Drugs" intensified as the 21st century approached, and in 1998, Congress enacted the Drug Free Workplace program appropriating money to give to businesses to keep workplaces drug free.[58] Thereafter, the concept of commonplace drug testing expanded far beyond those employed in a governmental position.

Now, over a decade later, many courts have ruled that in an at-will setting, there are few limitations on requiring employees to undergo drug testing.[59] Currently, even a trip to the local Home Depot might result in seeing a sign for job applications that adds the information, "We do random drug testing." Private employers can formulate nearly any (non-discriminatory) method for hiring and retaining its workforce, and employees have very little (if any) power to do anything about this if they wish to be employed.

Unions are a bit different with respect to something like random drug testing. Especially when dealing with safety issues, employers began pushing 40 years ago for various policies that would enable them to test those employees who were involved in industrial accidents and those suspected of being inebriated. Employers then pushed to negotiate provisions requiring random drug testing in order to ensure a consistent "clean" workforce.

It was at this point that unions really began to push back, and in many instances were able to negotiate provisions that limited the complete power of the employer to fashion drug testing policies. Rather, some unions were able to negotiate provisions that were

---

56. *See, e.g.*, 41 U.S.C. §§ 701–07 (1988); Pub. L. No. 100-690, 102 Stat. 4181 (1988) (The Drug-Free Workplace Act of 1988 is part of the Anti-Drug Act of 1988.).

57. The passage of the Drug-Free Workplace Act of 1988 spawned the creation of federal Mandatory Guidelines for Federal Workplace Drug Testing Programs (section 503 of Public Law 100–71). The mandatory guidelines apply to executive agencies of the federal government, the uniformed services (excepting certain members of the armed forces), and contractors or service providers under contract with the federal government (excepting the postal service and employing units in the judicial and legislative branches). For more information, see http://www.enotes.com/everyday-law-encyclopedia/drug-testing-2.

58. *See, e.g.*, THE VERMONT LEGISLATIVE RESEARCH SHOP, DRUG-FREE WORKPLACE LAWS: THE CONSTITUTIONALITY OF DRUG TESTING IN THE WORKPLACE, http://www.uvm.edu/~vlrs/Health/drugtesting.pdf (last visited Dec. 10 2012).

59. *Id.*

related to the reality of the work environment and situation.[60] This is a power that non-unionized workers do not have, and this lack of power is one that is making for what has really become a random hodge-podge in the application of privacy laws in the workplace.

Non-unionized workplaces are no different from unionized workplaces in terms of their unique natures. While it might make some sense for a religious organization to be concerned about whether it is possible to unearth any information on the internet about how an employee engaged in arguably immoral behavior ten years earlier, it would (at least in my opinion) make little sense to discharge an employee at Home Depot because someone was able to unearth a picture taken 10 years earlier where the employee was seen shopping at Lowe's. It would also make little sense if the employee were discharged for an employer's opinion about morals or beliefs, if morals and beliefs had no relation to the job being performed.

However, private employees can do little to negotiate such a provision as a condition of employment, and there are few states that have statutes that are of any benefit to private employees. Thus, unions, if they take the initiative, can not only negotiate clauses that protect its own employees, but may be able to provide examples of clauses that other employers can use as guideposts in formulating their own work rules.

In her article, *Carpe Diem: Privacy Protection in Employment Act*,[61] Professor Ariana Levinson[62] has proposed a model statute that, if adopted, would clarify and update federal legislation concerning employee monitoring.[63] While this author is in support of a federal

60. For example, teachers are not typically subject to random drug tests and their unions have achieved a sort of balance on that particular privacy issue by arguing that the tests are unwarranted. *See, e.g.*, Natalie Potts, *Teachers not Subject to Drug Tests,* WBBJTV EYEWITNESS NEWS (Oct. 26, 2012), http://www.wbbjtv.com/news/local/No-Random-Drug-Tests-for-Teachers—176048751.html. Similarly, unions could investigate whether monitoring is warranted for other professions, for example monitoring the work terminal of a forklift driver.

61. *See* Ariana R. Levinson, *Carpe Diem: Privacy Protection in Employment Act*, 43 AKRON L. REV. 331 (2010), *available at* http://www.uakron.edu/dotAsset/1669393.pdf.

62. University of Louisville, Louis D. Brandeis School of Law.

63. There have been attempts to increase workers' privacy through new legislation. In 1993, Senator Paul Simon (D-IL) introduced the Privacy for Consumers and Workers Act. The measure would have established a standard for notice, access to information, and use limitations. However, the bill did not leave the committee to which it was assigned. *See generally Workplace Privacy*, EPIC.ORG, http://epic.org/privacy/workplace/ (last visited Dec. 12, 2012). The Notice of Electronic Monitoring Act (NEMA) was introduced by Representative Charles Canady (R-FL) and Senator Charles Schumer (D-NY) in 2000.

statute that would clarify and update laws concerning monitoring employees, the scope of this article is of a smaller scale and seeks to deal only with those employees who are covered by collective bargaining agreements. The article also seeks to point out that different work situation may require different rules regarding employee monitoring and that although an overarching federal statute might be preferable, it would be difficult or a federal statute of this nature to cover many of the unique situations that occur in many blue collar situations. Thus, it is this author's position that work rules and/or collective bargaining agreements may become a good starting point for protecting workers' privacy rights while also allowing employers appropriate authority over their employees.

It should be noted that the National Labor Relations Act already protects group communications where the communications relate to improving working conditions. However, issues arise when constructive discourse crosses over to defamation, threats, or general public denigration of one's employer. It is this author's position that clearer provisions relating to the reality of what communications do occur would be beneficial for both employer and employee.

PROPOSED PROVISION

Here is a proposed "base" provision that this author believes would add clarity to what type employer monitoring is permissible and what will result in the discipline of an employee:

All employer issued equipment may be monitored. This includes cellphones and laptops that employees may use for personal purposes.

Personal use of employer issued equipment is permissible, within reason, during working hours. Examples of "within reason" include checking email or social networking sites during lunch hours or breaks, making personal calls during breaks, and accepting emergency phone calls at any time. The company reserves the right to monitor phone and internet use in the workplace for business-related reasons or for the purpose of assessing productivity.

The content of messages (including text messages and email messages) will not be routinely scrutinized for content unless it comes to the attention of the employer that the employee is engaging in illegal activities or those that otherwise violate company rules (such

---

NEMA would have established a private right of action against employers who failed to give notice of wire or network monitoring. This measure also never left committee.

as alleged harassment or threatening of other employees). Any communication produced on employer issued equipment is subject to this rule, including those communications sent during non-working hours. The company reserves the right to monitor the use of its property for the purpose of guarding against illegal activity. The employer reserves the right to audit, inspect, and/or monitor employees' use of the Internet, including all file transfers, browsing history, and emails, as deemed appropriate.

Participation on a social network (by way of text or traditional posting) is forbidden during an employee's working hours, with the exception of scheduled breaks.[64]

An employee may be disciplined for postings in public forums that, among other things, suggest participation in an illegal activity, make any type of threatening or violent comments, or disparage the reputation of the employer or a colleague in a way that does not amount to a constructive discourse about working conditions. Examples of public forums include internet blogs that the employee personally maintains, other internet blogs that post participant comments, listservs (including closed membership listservs), and posts on social network sites that are not password protected. This rule applies even when the employee is using his/her own personal electronic equipment, and applies if a pseudonym used in a posting is traced back to the employee.

An employee may not be disciplined for a private conversation with any individual, unless the conversation involves a suggestion of participation in an illegal activity, or makes threatening or violent commentary directed toward a co-worker or supervisor. This rule covers phone conversations, text messages, email exchanges, and private chats on social networking sites. However, if the exchange occurs with a co-worker during working hours and is brought to the attention of a supervisor, the employer has the discretion to impose discipline.

Any electronic communication that is to be used for purposes of discipline is to be fully documented and brought to the employee's attention prior to discipline being imposed. The employer is entitled to union representation when confronted with any evidence that might result in discipline and is entitled to respond to the charges.

---

64. It should be noted that access to some websites may be blocked by an employer, which provides a good protection against web surfing that results in a lack of productivity. However, social networking sites may be accessed through smart phones.

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 communications thought to be "personal" may result in workplace discipline.

Because non-unionized employees have no ability to bargain over rules and regulations in the workplace, this author believes that union negotiation can be the starting point for drafting realistic rules affecting electronic privacy as it relates to the workplace. If this occurs, the provisions adopted as work rules may become the basis for standardized policies governing electronic privacy rights and result in an increased understanding of rights and restrictions from both the vantage point of the employer and the employee.