Toward a Cohesive Interpretation of the Electronic Communications Privacy Act for the Electronic Monitoring of Employees

Ariana R. Levinson
University of Louisville School of Law

Follow this and additional works at: https://researchrepository.wvu.edu/wvlr

Part of the Privacy Law Commons

Recommended Citation
Available at: https://researchrepository.wvu.edu/wvlr/vol114/iss2/6

This Article is brought to you for free and open access by the WVU College of Law at The Research Repository @ WVU. It has been accepted for inclusion in West Virginia Law Review by an authorized editor of The Research Repository @ WVU. For more information, please contact ian.harmon@mail.wvu.edu.
TOWARD A COHESIVE INTERPRETATION OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT FOR THE ELECTRONIC MONITORING OF EMPLOYEES

Ariana R. Levinson

"The devil is in the details."

ABSTRACT

This Article proposes a cohesive interpretation of the Electronic Communications Privacy Act ("ECPA") designed to protect employees' basic right to privacy in their electronic communications. The difficulty of new technology outpacing the law's ability to protect employees' privacy from electronic monitoring by employers is widely acknowledged. Yet, scholars have generally overlooked or dismissed the potential of the ECPA to provide privacy protection for employees in the electronic workplace, calling instead for reform through the legislative process. Nevertheless, despite increasing calls from a broad range of entities for stronger privacy protections, passage of new legislation designed to adequately protect employees is, at best, not close at hand, and at worst, unlikely. On the other hand, several recent cases suggest that the courts are beginning to interpret the ECPA in ways that accommodate the changes in technology. Indeed, despite the admittedly limited scope of its coverage, the ECPA can and should be interpreted to provide employees some significant level of protection for their electronic communications. This Article attempts to describe the details of how this can be done.

* Assistant Professor, University of Louisville, Louis D. Brandeis School of Law; J.D., University of Michigan. The author extends thanks to the many scholars who helped with this piece. The author cannot overstate her appreciation for Nancy Levit’s review of earlier drafts. The author also thanks Mark Rothstein, Rafael Gely, Eileen Ridley and the other participants at the Privacy Law Scholars Conference at the George Washington University, and the scholars at the Labor and Employment Law Colloquium at Seton Hall University School of Law, the Southeastern Law Schools Association conference, and the Privacy Scholars Seminar Series at Berkeley Law School who provided valuable feedback on earlier drafts. For research assistance, the author thanks Kristen Staley, Meg Stewart, and Scott Wallitsch. She thanks Joe Leitsch, Technology Specialist, for several helpful conversations and Andrew Petti and Ben Basil for help with final edits. All views are solely those of the author, as are all errors.
I. INTRODUCTION

Dale Quinn, a firefighter employed by and living in a small city where most everyone knows each other, is issued a pager by the city. The service provider is a third party. While a city policy explicitly states that the use of the city's computers may be monitored, no policy explicitly references the pagers. Dale's supervisor states orally several times that the computer use policy will apply to the pagers. Once the pagers are actually issued, however, several em-
ployees, including Dale, send a greater number of text messages than anticipated by the city and incur costs above the plan's allotted amount. The supervisor tells Dale and others that rather than searching their pagers to determine how many messages were personal and how many work-related, the employees may simply pay the additional fees. Dale elects for several months to pay the additional fees. He does so because he has used his pager approximately thirty times each month to text his partner with adoring, and sometimes flirtatious, messages.

After four months, the supervisor tires of having to collect the overages from the five or so employees who go over the allotted amount each month. When the supervisor reports to his superior that he is tired of being a "bill collector," his superior decides to perform an internal investigation to determine whether the overages are due to personal or work-related messages. She intends to raise the number of text messages for which the city pays if the overages are due to work-related messages. Thus, she requests copies of Dale's text messages for the past two months from the third party service provider. The service provider complies with the request, and she reviews the records including fifty-seven messages from Dale to his partner and fifty-five messages from his partner to Dale. She decides not to increase the amount of text messages the city pays for and instead to terminate Dale for personal use of city-issued equipment.

Whether Dale has any cause of action against the city for invading his privacy remains unclear as a result of the recent and much-anticipated Supreme Court decision in City of Ontario v. Quon.1 Certainly, if Dale were a SWAT (Special Weapons and Tactics) team officer rather than a firefighter, if he had sent a higher number of salacious text messages rather than fifty-seven sometimes flirtatious ones, if the computer policy was extended to text messages in writing rather than simply orally, and if the superior had limited the review of the records to those texts sent during work time, Dale would likely be unsuccessful with any Fourth Amendment claim for invasion of privacy against his employer.2 Dale, however, is likely not completely remediless because, at a minimum, Dale has a viable claim against the third party service provider for violating the Electronic Communications Privacy Act ("ECPA").3

The ECPA generally provides a private civil cause of action against any person or entity who intentionally intercepts an electronic communication or who obtains unauthorized access to stored electronic communications.4 The ECPA provides minimum statutory damages for each violation of it.5 The ECPA has been described by experts as dense,6 intricate,7 and difficult for lawmakers,8

---

1 130 S. Ct. 2619, 2630 (2010).
2 Id. at 2630–33.
lawyers, and even scholars to interpret. Because it contains criminal as well as civil provisions, many scholars addressing the ECPA deal with its application in the criminal law context rather than the employment law context. Yet it is imperative that scholars writing about workplace privacy and those litigating and deciding cases involving electronic monitoring by employers understand the ECPA. The ECPA has been applied in a variety of different employment situations involving electronic monitoring of employees, and recent cases suggest that a cohesive interpretation of the many terms in the ECPA would provide protections for employees’ privacy in their electronic communications in varied types of factual situations. The ECPA may admittedly be a less than ideal me-

scholars have had a very hard time making sense of [Title II of the ECPA]. The statute is dense and confusing, and few cases exist explaining how the statute works.”). Meir S. Hornung, Note, Think Before You Type: A Look at Email Privacy in the Workplace, 11 FORDHAM J. CORP. & FIN. L. 115, 130 (2005) (“Federal circuit courts have called [Title I of the ECPA] ‘complex,’ ‘convoluted,’ and ‘ambiguous.’”) (footnotes omitted).


Charles E. Frayer, Employee Privacy and Internet Monitoring: Balancing Workers’ Rights and Dignity with Legitimate Management Interests, 57 BUS. LAW. 857, 866 (2002) (“[T]he ECPA is notorious for its lack of clarity. This perception may explain why few employees and their lawyers have attempted to claim any privacy protection under the ECPA, and thus, why it remains largely untested in this context.”) (footnotes omitted).

Hornung, supra note 7, at 129 (“Despite their obvious importance, the statutes remain poorly understood. Courts, legislators, and legal scholars alike have had a very hard time making sense of these federal statutes. They are dense and confusing, and the two sections of the amended Federal Wiretap Act, at times, seem to contradict or diminish the use of one another.”) (footnotes omitted).

See, e.g., James X. Dempsey, Communications Privacy in the Digital Age: Revitalizing the Federal Wiretap Laws to Enhance Privacy, 8 ALB. L.J. SCI. & TECH. 65, 69 (1997) (“The focus of this article is limited to government access to communications and stored electronic data and attendant issues, deferring to others the consideration of important questions concerning the disposition of control over personal information as between employers and employees or between businesses and customers.”) (footnotes omitted); Susan Freiwald, Online Surveillance: Remembering the Lessons of the Wiretap Act, 56 ALA. L. REV. 9, 15 (2004) (“In limiting my focus to government surveillance, I do not mean to minimize the threat to privacy that surveillance by private entities poses.”) (footnotes omitted).

See, e.g., Quon v. Arch Wireless Operating Co., 529 F.3d 892 (9th Cir. 2008), cert. denied, 130 S. Ct. 1011 (Dec. 14, 2009) (holding a service provider violates the ECPA by releasing an employee’s text messages to a subscribing employer without the employee’s consent); United States v. Councilman, 418 F.3d 67, 85 (1st Cir. 2005) (intercepting includes acquiring an electronic communication in “transient electronic storage that is intrinsic to the communication process”); Global Policy Partners, LLC v. Yessin, 686 F. Supp. 2d 631, 638 (E.D. Va. 2009) (explaining that “interception includes accessing messages in transient storage on a server during the course of transmission”); Pietrylo v. Hillstone Rest. Grp., No. 06-5754 (FSH), 2009 WL 3128420, at *5 (D.N.J. Sept. 25, 2009) (jury could infer employee was pressured into providing a password and as such did not authorize employer’s use of online chat group); Brahma v. Lembo, No. C-09-00106 RMW, 2009 WL 1424438, at *3 (N.D. Cal. May 20, 2009) (denying motion to dismiss...
chanism for protecting employees’ privacy rights. But with the longstanding failure of the law to catch up with technology and with the failure of the Supreme Court to lend clarity to the potential of the Fourth Amendment to protect public employees’ privacy, the ECPA presents one of the few viable potential avenues of protection for employees’ privacy from electronic monitoring by their employers. Interpretation of the ECPA as currently enacted is particularly important because recent calls for legislative reform have not been successful. Calls for reform from entities as diverse as the ACLU and Microsoft and from scholars published in high-profile academic journals, such as the Yale Law Journal,\textsuperscript{13} have not produced legislative action. In the current climate of political stalemate, any sort of labor or employment reform, including privacy protection, is unlikely to pass soon.

Many employment law articles that discuss the ECPA do so only briefly with the purpose of simply providing employers guidance on policies governing electronic communications.\textsuperscript{14} Generally, scholars writing about workplace pri-
vacy have overlooked or dismissed the potential of the ECPA to provide privacy protection for employees in the electronic workplace,\(^6\) some calling instead for its amendment\(^7\) or for federal\(^8\) or state legislation.\(^9\) For instance, one author

\(^{15}\) David C. Yamada, *Voices from the Cubicle: Protecting and Encouraging Private Employee Speech in the Post-Industrial Workplace*, 19 BERKELEY J. EMP. & LAB. L. 1 (1998) ("The ECPA, however, includes a 'business use' exception that effectively precludes any sort of general check on electronic surveillance of employees.").


has proposed changes to the ECPA's consent exception based on European law.\textsuperscript{19} A few have proposed a judicial interpretation of the ECPA addressing some particular problem.\textsuperscript{20} For instance, one author, among other proposals, has proposed a judicial interpretation of ECPA to protect employees from disclosure of personal e-mails.\textsuperscript{21} Another has proposed that courts incorporate standards from English law, such as relevance, quality, proportionality, finality, and a right to know, under the ordinary course of business exception to the Wiretap Act.\textsuperscript{22} Some authors focus only on one title of the ECPA rather than on both the relevant titles as an integrated whole.\textsuperscript{23}

This Article attempts to fill a gap in the scholarly literature by offering a cohesive interpretation of the ECPA that, if adopted by the courts, would, in many contexts, provide a relatively high level of protection for the privacy of employees' electronic communications.\textsuperscript{24} It provides novel means of interpret-
ing terms such as “intercept” and “authorization” consistent with the text of the ECPA and the purpose of protecting privacy.\textsuperscript{25} It compares and contrasts some provisions of the ECPA in ways heretofore overlooked\textsuperscript{26} and digs into the legislative history, finding support for the proposed interpretations.\textsuperscript{27} It is also the only recent scholarly article to assess in a detailed manner the application of the ECPA to employer electronic monitoring of employees and to synthesize the cases, including the more recent cases that are more protective of employees’ privacy. It, thus, not only contributes to the scholarship in the area of employer surveillance, but also seeks to serve as a useful tool for litigators and courts addressing privacy cases in the employment setting.


\textsuperscript{25} \textit{See infra} Part V.A.1. (Interception), V.B.2. (Access and Authorization).

\textsuperscript{26} \textit{See infra} notes 249–250 and accompanying text (contrasting provider exceptions).

\textsuperscript{27} \textit{See infra} note 254 and accompanying text (provider exception); note 273 and accompanying text (term “telephone” modifies term “equipment”); note 331 (interstate commerce requirement).
This Article proceeds in six parts. Section II describes the privacy conundrum created by the advancement of technology and the need for the law to adapt to address the problem. Section III briefly discusses several recent cases that suggest courts are beginning to interpret the ECPA in a manner that provides some level of protection for employees from employer monitoring. Section IV describes the principles underlying the cohesive interpretation of the ECPA proposed by this Article. It outlines why employees’ privacy in their electronic communications is a basic right and explains why protection of that right is the primary guiding principle behind the suggested interpretation. Section V describes in detail the proposed cohesive interpretation of the ECPA as applied to employer monitoring of employees. Section VI concludes by calling on the courts to implement the proposed interpretation while legislative change is awaited.

II. ADVANCING TECHNOLOGY AND THE PRIVACY CONUNDRUM

As technology advances it creates novel work practices and problems. Technology permits a “boundary-less” workplace in which employees work during non-work hours and while at home. It also permits employees a greater ability to perform personal tasks while at work and during work time. As for employers, the technology provides more ability to monitor employees’ communications, made both at work and away from work.

The scope of employer electronic monitoring of employees is extensive. The American Management Association (“AMA”) provides the most recent and comprehensive data regarding employer electronic monitoring practices. Notwithstanding that the majority of the employers surveyed by the AMA are likely large companies, the data indicates that a great number of employers electronically monitor their employees. The AMA’s 2007 data indicates that forty-three percent of employers monitored employees’ e-mail and computer files, sixty-six percent monitored the Internet, twelve percent monitored the blogosphere, and ten percent monitored social networking sites.

These practices affect millions of employees. In January 2001, the Privacy Foundation found that 40.7 million employees were regularly using e-mail or Internet at work. One workplace privacy expert suggested in his 2002 ar-

28 Use of this phrase has been attributed to Professor Kathy Stone. See Michael Selmi, Privacy for the Working Class: Public Work & Private Lives, 66 LA. L. REV. 1035, 1037 n.8 (2006).
article that 14 million of these employees were under continuous surveillance, a number that excluded spot-checking and reasonable suspicion surveillance. He estimated that twelve percent of employers did not inform employees of their policies regarding electronic monitoring. A 2003 employer survey supports his estimates, suggesting that two out of three employers who electronically monitor their employees have no policy requiring acknowledgment or consent.

SpectorSoft is an example of the type of software that employers might use to monitor their employees. The co-founder of the SpectorSoft-producing company stated that the software “is designed to make it easier for parents to monitor their children’s Internet use and for employers to monitor their employees’ Internet use.” The software “virtually” contemporaneously captures “all instant messages, sent and received e-mails, web searches, online chats, file transfers, electronic data, and other activity from the computer . . . .”

Scholars have written extensively about the law’s inadequacy to protect employee privacy from employer electronic monitoring. Several scholars have addressed the general inadequacy of the tort of invasion of privacy to protect employees from employer electronic monitoring that lacks appropriate safeguards for the employees’ privacy. The tort requires a reasonable expectation of privacy, which is normally found to be reduced in the employment setting. It also requires the invasion of privacy to be offensive, and courts often find that employers’ rights outweigh those of employees to privacy protection. Under Quon, it remains unclear how much protection for electronic communications the Fourth Amendment will provide to employees, and in any event, those protections do not extend to the private sector. Scholars have also noted the limitations of the ECPA, particularly as previously interpreted by some courts.

32 Finkin, supra note 31, at 474.
33 Id. at 477.
36 Id. at *6 (quoting Chesley’s affidavit).
39 MATTHEW W. FINKIN, PRIVACY IN EMPLOYMENT LAW 346 (2d ed. 2003).
40 Id. at 346; Clyde W. Summers, Individualism, Collectivism and Autonomy in American Labor Law, 5 EMP. RTS. & EMP. POL’Y J. 453, 469 (2001).
42 Levinson, supra note 38, at 340 n.37 (listing scholars).
In addition to scholars, other countries have noted the failure of the law in the United States to adequately protect the privacy of employees’ electronic communications. Because Europe considers the United States to provide inadequate protections, companies receiving information about electronic monitoring of European employees must adopt safeguards additional to those provided under United States law. Several options are available for U.S. companies, which do business in Europe, to adopt adequate safeguards that meet European directive requirements, including participation in the U.S. Commerce Department’s safe-harbor program. This program requires employers to adopt privacy policies governing the electronic communications of their European employees.

Advancing technology permits employers more ability to monitor at the same time it permits employees to perform more personal tasks while at work and during work time. Indeed, the current scope of employer monitoring of employees is extensive. Thus, the likelihood of employers obtaining communications that employees consider private has risen substantially as technology has advanced. Moreover, scholars have written extensively about the law’s inadequacy to protect employee privacy from employer electronic monitoring, and other countries have indicated that U.S. law should provide a higher level of safeguards. There is, therefore, a need for the law to adapt to address the problem, and recent cases suggest that such legal developments are possible.

III. RECENT CASES

Several recent decisions suggest that courts are beginning to interpret the ECPA to provide some level of protection for employees from electronic monitoring. For instance, one recent decision suggests that courts will interpret

44 Id. at 391–92.
46 Herbert, supra note 43, at 393.
47 While the two cases discussed here are from courts located in the Ninth Circuit, other cases, discussed below, that have recently arisen in other circuits point toward the same conclusion. See United States v. Councilman, 418 F.3d 67, 85 (1st Cir. 2005) (intercepting includes acquiring an electronic communication in “transient electronic storage that is intrinsic to the communication process”); Global Policy Partners v. Yessin, 686 F. Supp. 2d 631, 638 (E.D. Va. 2009) (explaining that “interception includes accessing messages in transient storage on a server during the course of transmission”); Pietrylo v. Hillstone Rest. Grp., No. 06-5754 (FSH), 2009 WL 3128420, at *5 (D.N.J. Sept. 25, 2009) (jury could infer employee was pressured into providing a password and as such did not authorize employer’s use of online chat group); Pure Power Boot Camp v. Warrior Fitness Boot Camp, 587 F. Supp. 2d 548, 562 (S.D.N.Y. 2008) (an employee should have the opportunity to refuse or withdraw consent to monitoring); Potter v. Havlicek, No. 3:06-cv-211, 2007 WL 539534 (S.D. Ohio Feb. 14, 2007) (adopting the position that interception need not
the ECPA to protect employees from employers who attempt to intentionally access obviously personal communications. Another, the controversial Quon decision in which the United States Supreme Court recently issued a decision on the separate Fourth Amendment issue, suggests that the courts will interpret the ECPA to protect employees from release of even work-related communications from a third party to an employer when the employee has not consented to the release of those communications. These decisions are discussed in more detail below. Notably, other decisions also suggest that courts are beginning to interpret related concepts, such as the attorney-client privilege, in a manner that will protect employee communications made on employer-issued equipment. The recent willingness of the courts to grapple with changing technology and to protect the privacy of employees' electronic communications indicates the timeliness of a cohesive interpretation of the ECPA designed to protect employees' basic right to privacy in their electronic communications.

A. Intentionally Accessing Personal Communications

In Brahama v. Lembo, the employer allegedly used a system to monitor an employee's keystrokes on an employer-issued keyboard to discover an employee's personal e-mail password. The employer then allegedly used the password to access the personal e-mail account. The employee asserted that the employer violated the ECPA by unlawfully intercepting and using his personal password. The court denied the employer's motion to dismiss these...
ELECTRONIC MONITORING OF EMPLOYEES

ECPA claims because the pleaded facts indicated the keystrokes possibly were captured while in transit, constituting an interception. Certainly, intentionally monitoring employees, without notice, to discover a personal password and to use it to log into the employee’s personal e-mail account is conduct that should be regulated.

B. Reviewing Communications

In Quon v. Arch Wireless Operating Co., the employer, the Ontario Police Department, issued “two-way alphanumeric pagers” to its employees. The City contracted with an outside service provider, Arch Wireless Operating Co., to provide the text messaging services on the pagers. The lieutenant in charge of the pagers permitted the employees, including the plaintiff, to use the pager for personal text messages so long as they paid for the cost of any messages over the allotted amount of twenty-five thousand characters. But when the lieutenant tired of badgering people for payment, the lieutenant’s chief decided to investigate the employees’ usage and whether it was work-related. The department then requested a copy of plaintiff’s text messages from the service provider, and the service provider released them. Neither the chief nor the service provider notified the plaintiff that the lieutenant, the chief, and the plaintiff’s supervisor would be reading his text messages; they also did not seek consent from the plaintiff.

The court reversed the lower court’s grant of summary judgment to the service provider. The court held that a service provider that “provides the ability to send or receive wire or electronic communications” violates the ECPA by releasing to a subscribing employer an employee’s text messages without the employee’s consent. Thus, to the extent that more employers are issuing handheld devices that use third party service providers to transmit messages, rather than providing their own equipment and services, the ruling provides a potential avenue of providing more comprehensive protection for employees’ privacy.

54 Id. at *3. The court discussed the requirement that any transfer of electronic data must affect interstate commerce and reasoned whether the keystrokes affected interstate commerce was “better resolved after some discovery.” See also infra Part V.A.3. (Interstate Commerce Requirement).
55 529 F.3d 892 (9th Cir. 2008), cert. denied, 130 S. Ct. 1011 (Dec. 14, 2009).
56 Id. at 895.
57 Id.
58 Id. at 897.
59 Id. at 897–98. Another employee with an overage was also investigated. Id. at 898.
60 Id. at 898.
61 Id. at 906, 909.
62 Id. at 903.
63 Id. at 900 (citing Stored Communication Act, 18 U.S.C. § 2510 (15) (2006)).
64 While difficult to quantify, popular perception indicates that the use of employer issued handheld devices is on the rise. See, e.g., Tresa Baldas, Overtime Suits May Ripen with BlackBer-
Several principles underlie the cohesive interpretation of ECPA suggested in this Article. The primary guiding principle is that privacy is a basic right that should protect employees from electronic monitoring by their employers. A related guiding principle is the legislative intent to protect individuals from electronic monitoring. The canons of statutory construction may also be helpful in some instances. Additionally, the potential negative impacts on the employee and, ultimately, the employer from electronically monitoring employees are considered. Each of these principles is discussed further in the following subsections.

Another important guiding principle is that any interpretation of the ECPA should be adaptable enough to protect employees’ privacy from current and future technology without requiring reenactment of new legislation each time. This principle suggests that the many terms and intricacies in the ECPA should be interpreted in a technical manner only when doing so protects, rather than precludes, employees’ basic right to privacy.

This Article takes the position that the ECPA should be interpreted to provide the greatest level of safeguards for the privacy of employees’ electronic communications given the text of, and legislative intent behind, the ECPA. This position is not intended to devalue the interests of employers; indeed, in many instances employers have valid reasons for electronically monitoring their em-

---

rysts, The Nat’l L. J., Apr. 28, 2008 (implying that because employers are giving out so many smartphones, lawsuits surrounding overtime pay are on the rise); BlackBerry, BlackBerry Customer Success, http://us.blackberry.com/newsroom/success/ (last visited Oct. 24, 2011) (listing hundreds of employers’ case studies regarding their use of BlackBerry smartphone devices for their employees); Stephanie Chen, Personal Texting on a Work Phone? Beware Your Boss, CNN (Apr. 20, 2010, 9:34 AM), http://www.cnn.com/2010/LIVING/worklife/04/20/work.text.email.privacy/index.html (“The use of cell phones and mobile internet service has skyrocketed over the last decade, and some of the growth can be attributed to companies giving cell phones and smartphones to their employees, said Lee Rainie, director of the Pew Internet & American Life Project.”). On the other hand, another commonly perceived trend, the increased use of cloud computing, is not likely to increase the extent of privacy guaranteed employees under the ECPA because many cloud computing providers will likely be classified as remote computing service rather than electronic communication service. See William Jeremy Robison, Note, Free at What Cost?: Cloud Computing Privacy Under the Stored Communications Act, 98 Geo. L.J. 1195, 1209–10 (2010) (explaining that “many of today’s popular cloud computing services are designed for purposes other than communication, such as word processing or digital photo storage”).

Blackowicz, Note, supra note 21, at 103–04 (because of the “gap” in statutory terminology created by new technology, “courts should be more willing to accommodate plaintiffs, especially when a case turns upon a technicality in the statute that does not recognize the new technology”); see Levinson, supra note 38, at 422 n.532.

ELECTRONIC MONITORING OF EMPLOYEES 475

ployees.67 The ECPA, however, is already tilted toward employers’ interests. For instance, the ECPA provides no protection at all for employees from several types of monitoring, including GPS68 and silent video.69 The ECPA also provides no baseline of privacy, such as prohibiting monitoring of communications made between employees and family members in their homes regardless of whether an employee consents. The ECPA is not flexible enough to provide any alternate safeguards other than consent or business necessity, such as a right to review information collected through monitoring or a requirement of equal discipline for similar infractions. Because of the lack of flexibility in the exceptions, they are each construed restrictively to protect employees.

A. Employees’ Basic Right to Privacy

The basic right to privacy is recognized by the U.S. Constitution as well as internationally. Both the Constitution and international law have been extended to protect employees in the workplace. Additionally, the United States has always recognized the private nature of postal mail, which has certainly been replaced in considerable measure by electronic communication in recent times.

1. Constitutional Precedent

The Fourth Amendment to the U.S. Constitution provides a basic right to privacy.70 While the protection extends only to governmental invasions of privacy and not to invasions of privacy by private actors, such as private employers, the cases interpreting the Fourth Amendment illustrate the basic nature of the right.71 The precedents also illustrate how the basic right to privacy extends to protection from electronic surveillance and to searches of employees by

67 See Levinson, supra note 38, at 403 (listing harms to employer that may justify monitoring with appropriate safeguards for employees’ privacy).
70 U.S. CONST. amend. IV (The Fourth Amendment protects “[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures . . . .”).
71 See Joseph R. Grodin, Constitutional Values in the Private Sector Workplace, 13 INDUS. REL. L.J. 1, 2, 25–30 (1991) (discussing how constitutional values have found their way into the private workplace and how the common law doctrines regarding privacy are the most “historically and analytically intertwined” with constitutional doctrine).
their employers. The precedents, as a matter of principle, therefore, support interpreting the ECPA in a manner that provides the highest possible level of protection for employee privacy.  

Decades ago the Supreme Court interpreted the Fourth Amendment to protect the privacy of wire communications, even those made outside the home from a telephone booth, and to protect against electronic eavesdropping. While decades before that the Court had found no such protection, advances in technology made clear that if individuals were to retain privacy in their homes and papers, communications made by new technologies must be protected. Today, keeping pace with continuing change in technology, some lower courts have found that individuals have a reasonable expectation in the privacy of computer files and various electronic communications such as text or e-mail messages.

As for workplace privacy, in O'Conner v. Ortega the Court recognized that employees may have a right to privacy even from their employers. An employee brought a Fourth Amendment claim because his employer had searched the employee's employer-issued desk and file cabinets, removing personal items. A plurality of the Court held that the employee had a reasonable expectation of privacy in the employer-issued desk and file cabinets because he

---

72 While the Constitutional right to privacy is traditionally thought of as a liberty interest, the concept of a dignitary interest in privacy is recognized not only in Europe but also in the privacy torts originally propounded by Brandeis and Warren. Chivvis, supra note 16, at 800; see also Avner Levin, Is There a Global Approach to Workplace Privacy?, in SURVEILLANCE, PRIVACY, AND THE GLOBALIZATION OF PERSONAL INFORMATION: INTERNATIONAL COMPARISONS 328, 329–30 (E. Zureik et al. eds., 2010) (describing rights approach to privacy in the employment relationship that focuses on dignity), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=998105.


75 S. REP. No. 99-541, at 2 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3556 (noting that Olmstead v. United States, 277 U.S. 438 (1928), in which the court found no violation because wiretapping did not consist of searching or physical trespass, "is often remembered more for Justice Brandeis' prescient dissent than for its holding").

76 Katz, 389 U.S. at 353; Berger, 388 U.S. at 63–64.

77 See NTS AM JUR. 2d Computers and the Internet § 22 (2011) (citing cases protecting the privacy of computer files and text messages, and also those finding no reasonable expectation of privacy); Mitchell Waldman, Annotation, Expectation of Privacy in Internet Communications, 92 A.L.R.5th 15, §§ 3(a), 3(b) (2011) (citing cases finding expectation of privacy in e-mail message, and those that did not); Robin Miller, Annotation, Expectation of Privacy in Text Transmissions to or from Pager, Cellular Telephone, or Other Wireless Personal Communications Device, 25 A.L.R.6th 201, §§ 4, 5 (2007) (citing cases finding expectation of privacy in text messages, and those that did not).


79 Id. at 716–19.

80 Id. at 713.
ELECTRONIC MONITORING OF EMPLOYEES

81 Id. at 718, 731 ("[W]e recognize that the undisputed evidence suggests that Dr. Ortega had a reasonable expectation of privacy in his desk and file cabinets.").

82 Id. at 719 ("Finally, we note that there was no evidence that the Hospital had established any reasonable regulation or policy discouraging employees such as Dr. Ortega from storing personal papers and effects in their desks or file cabinet . . . ").


84 The Supreme Court stated:

For present purposes we assume several propositions arguendo: First, Quon had a reasonable expectation of privacy in the text messages sent on the pager provided to him by the City . . . and third, the principles applicable to a government employer’s search of an employee's physical office apply with at least the same force when the employer intrudes on the employee’s privacy in the electronic sphere.

Id. at 2630.

shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence . . . "

A brief review of European law on the subject illustrates the basic nature of the right to privacy and the appropriateness, therefore, of interpreting the ECPA to provide a high level of safeguards for employee privacy. European governing documents emphasize the basic nature of the right to privacy; privacy in correspondence and communications are particularly encouraged, including electronic communications. The European Convention for the Protection of Human Rights and Fundamental Freedoms states that "[e]veryone has the right to respect for his private and family life, his home and correspondence." The Charter of Fundamental Rights of the European Union substitutes the term "communications" for the term "correspondence."

The European Court of Human Rights has held that the protection of private life extends to the employer monitoring of employees and protects e-mails sent from work and Internet use at work. In Halford v. United Kingdom, the European Court held that an employer's interception of an employee's personal phone calls violated the Convention. In Copland v. United Kingdom, the European Court held that an employer violated the Convention by collecting and storing data about an administrative assistant's use of e-mail and the Internet for

86 G.A. Res. 2200, supra note 85, at art. XVII; G.A. Res. 217, supra note 85, at art. XII.
87 A review of the laws of all countries is beyond the scope of this Article. There are a few articles that investigate the laws of other countries that address electronic monitoring of employees. See Levinson, supra note 38, at 372–90 (listing articles).
personal reasons. While in both cases the employer was a public entity, the Convention applies to public and private employers.

Furthermore, the legislative bodies of the European Union, the European Parliament and the Council of the European Union, have recognized that the right to privacy is so important that they adopted a Directive designed to respect the basic right of privacy when processing personal data. A Working Party was established to administer the Directive. The Working Party has issued detailed documents providing the specific manner in which privacy of employees' electronic communications must be protected.

Thus, the European Court and the European Union recognize privacy as a basic right. The right extends to protect employees of private employers from electronic surveillance. This recognition indicates that it is appropriate to treat privacy as a basic right and to guarantee employees the highest level of protection possible under the ECPA.

3. Protection of Postal Mail

The longstanding statutory protections for communications made through postal mail also indicate that privacy of employees' personal communications is a basic right deserving of protection when made electronically. A federal statute, originally enacted in 1948, protects the privacy of communications made through the postal system, and the protection extends against employers even when an employee's personal mail is delivered to the employer's address. The statute protects against theft of mail, but its protections extend

---

96 Id. at art. 29.
97 Some even refer to this Directive as the “Privacy Directive.” See Herbert, supra note 43, at 388.
99 Richard J. Link, Postal Service and Offenses against Postal Laws, 72 C.J.S. Postal Service § 79 (May 2010).
101 MERRICK T. ROSEIN, MONITORING THE WORKPLACE: ELECTRONIC COMMUNICATION AND OTHER TECHNOLOGIES, EMPLOYMENT LAW DESKBOOK HUMAN RESOURCES PROFESSIONAL § 24:21 (2009) ("In general, an employer is not authorized to open mail directed to a person at the workplace that appears to be personal."). While no specific case has applied the postal statute to an employer, employers generally understand opening personal mail without authorization would
well beyond traditional theft. For instance, per the statute, taking mail before delivery with the intent to "pry into the business of another" is a felony offense. Moreover, the statute creates a misdemeanor offense for any unauthorized person to open or destroy another's mail. On their face, these prohibitions apply in the employment setting to employers who might otherwise read their employees' personal mail. Additionally, the statute also insures that postal employees handle the mail only as necessary to perform their jobs. It prohibits postal employees from unlawfully opening or delaying mail, or from permitting anyone else from destroying or delaying the mail. Just as individuals rely on third parties to deliver postal mail without inquiring as to the contents of the mail, they rely on electronic communications to securely deliver their communications. Thus, the relatively high level of protection for communications traveling by postal mail indicate the importance of protecting employees' right to privacy in electronic communications as well.

B. Legislative Intent

The explicitly stated intent of the ECPA is to extend privacy protections to electronic communications, including data shared by computer. That intent violate the statute. See Robert J. Nobile, Essential Facts: Employment 8:13 (Jeanne P. Dawson et al., Thomson West 2006); Bales & Hamilton, supra note 14, at 252–53.

107 § 1703; 72 C.J.S. Postal Service, supra note 99, § 78.
109 S. Rep. No. 99-541, at 1 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3555 ("to protect against the unauthorized interception of electronic communications"); id. at 11 ("Title I of the Electronic Communications Privacy Act expands chapter 119 to take into account modern advances in electronic telecommunications and computer technology."); H.R. Rep. No. 99-647, at 18 (1986) ("Unfortunately the same technologies that hold such promise for the future also enhance the risk that our communications will be intercepted by either private parties or the government."); id. at 19 ("But most important, if Congress does not act to protect the privacy of our citizens, we may see the gradual erosion of a precious right."); id. at 34 ("This expansion [adding electronic communications] permits the inclusion in the general wiretapping and bugging law of many new forms of communication. For example, digitized transmissions and electronic mail will be provided with protection against interception.").
ELECTRONIC MONITORING OF EMPLOYEES

is stated numerous times in the Senate and House reports.110 Before the enactment of the ECPA, the provisions of the Wiretap Act covered only common carriers, and Congress recognized that with changes in technology many communications system options beyond the common carrier were available.111 Congress’s intent to protect the privacy of individual’s electronic communications sent through these other systems, including internal company systems, is clear.112

110 S. Rep. No. 99-541, at 1 ("to protect against the unauthorized interception of electronic communications"); id. at 11 ("Title I of the Electronic Communications Privacy Act expands chapter 119 to take into account modern advances in electronic telecommunications and computer technology."); H.R. Rep. No. 99-647, at 18 (1986) ("Unfortunately the same technologies that hold such promise for the future also enhance the risk that our communications will be intercepted by either private parties or the government."); id. at 19 ("But most important, if Congress does not act to protect the privacy of our citizens, we may see the gradual erosion of a precious right."); id. at 34 ("This expansion [adding electronic communications] permits the inclusion in the general wiretapping and bugging law of many new forms of communication. For example, digitized transmissions and electronic mail will be provided with protection against interception.").

111 S. Rep. No. 99-541, at 1 ("in light of dramatic changes in new computer and telecommunications technologies"); id. at 5 ("This is so, even though American citizens and American businesses are using these new forms of technology in lieu of, or side-by-side with, first class mail and common carrier telephone services.").

112 The Senate commented as follows:

Since the divestiture of AT&T and deregulation, many different companies, not just common carriers, offer a wide variety of telephone and other communications services. It does not make sense that a phone call transmitted via common carrier is protected by the current federal wiretap statute, while the same phone call transmitted via a private telephone network such as those used by many major U.S. corporations today, would not be covered by the statute.

Id. at 2–3. The House of Representatives also stated:

This statutory framework appears to leave unprotected an important sector of the new communications technologies. Many communications today are carried on or through systems which are not common carriers. Electronic mail, videotex[] and similar services are not common carrier services. . . . Moreover, totally private systems are rapidly being developed by private companies for their own use.

H.R. Rep. No. 99-647, at 17–18; id. at 31 ("As a result of this change, a company whose activities affect interstate commerce and which installs its own private telephone or electronic communication system would have that system covered by the statute."). See 132 Cong. Rec. H4039-01, H4045-46 (June 23, 1986) (statement of Rep. Kastenmeier) ("Let me take a few moments to highlight what I believe to be the fundamental principles which guide this legislation. . . . The second principle which should be followed in this area is recognition that what is being protected is the sanctity and privacy of the communication."); Baumhart, supra note 20, at 926 ("[T]o blindly adopt the view that the statute imposes no access limitations on employers who possess their own systems ignores Congress’ stated intent to procure parity in the protection of personal communications, regardless of the medium of transmission."); see also Robert W. Kastenmeier et al., Communications Privacy: A Legislative Perspective, 1989 Wis. L. Rev. 715, 737 (1989) ("By including under its protection private branch exchanges and other internal communications systems, especially in the corporate context, ECPA engendered a dramatic expansion of the privacy protections under the law.").
Congress also intended to extend protection to electronic communications in a manner adaptable enough to cover future technologies, like the Internet. When introducing the ECPA in the House, Representative Kastenmeier, a key sponsor of the bill, emphasized the need for adaptability in the law to protect the privacy of electronic communications as the first basic principle guiding the legislation. He stated that the legislation “should be comprehensive, and not limited to particular types or techniques of communicating” because “[a]ny attempt to write a law which tries to protect only” existing technologies “is destined to be outmoded within a few years.”

Thus, the basic purpose of the ECPA is to protect individuals’ privacy in their electronic communications. The legislative history manifests no intent to exclude employees from the protections of the ECPA. There is no explicit mention of employer monitoring of employees electronic communications in the Senate or House Report, or in the statements made by the bill’s sponsors at the times of passage. On its own, silence no more indicates a blanket exclusion than a blanket inclusion. But before the ECPA amendments, the Wiretap Act clearly applied to employers and had been so construed by the courts; nothing indicated a modification of that statutory coverage.

Representative Kastenmeier stated:

> Let me take a few moments to highlight what I believe to be the fundamental principles which guide this legislation. The first principle is that legislation which protects electronic communications from interceptions by either private parties or the Government should be comprehensive, and not limited to particular types or techniques of communicating. . . . Any attempt to write a law which tries to protect only those technologies which exist in the marketplace today; that is, cellular phones and electronic mail is destined to be outmoded within a few years.

132 CONG. REC. H4039-01, H4045.

113 Representative Kastenmeier stated:

114 See Baumhart, supra note 20, at 925 (“The Senate Report on the ECPA underscores individual privacy concerns as the primary reason for including E-mail and similar forms of electronic communications within the purview of the statute.”).

115 Howard, supra note 14, at 512 (“The Federal Wiretap Act generally prohibits the interception, disclosure or intentional use of wire, oral or electronic communications, including those that occur in the workplace.”) (footnotes omitted); Droke, supra note 20, at 182 (determining that few of the limited exceptions of the ECPA are likely to protect corporate review of employees’ electronic mail); Steven B. Winters, Note, Do Not Fold, Spindle, or Mutilate: An Examination of Workplace Privacy in Electronic Mail, 1 S. CAL. INTERDISC. L.J. 85, 119 (1992) (“[N]othing in the legislative history of the ECPA clearly suggests that Congress did not intend the ECPA to cover private employer monitoring of employee E-mail transmissions.”) (footnotes omitted). A statement by an advocate from one organization cannot be taken as determinative of legislative intent. See Baumhart, supra note 20, at 926 n.19 (citing Ruel Torres Hernandez, ECPA and Online Computer Privacy, 41 FED. COMM. L.J. 17, 40 (1988) (quoting Jerry Berman, Counsel, ACLU as stating “ECPA ‘goes right up to the water’s edge [of employee privacy protection] but stops short’ and to have included some privacy protection against employers in the corporate context ‘would have killed the bill.’”) (alteration in original)).

116 Baumhart, supra note 20, at 926 (citing Senate Report for the proposition that “while the Senate Report accompanying passage of the ECPA acknowledges the existence of internal corporate E-mail systems, it does not address the anticipated effect of the legislation on these systems”) (footnotes omitted).
cates that the ECPA was intended to change that reality.117 Because the legislative history so strongly intends a broad level of protection with limited necessary exceptions, the exceptions should be construed narrowly to provide as much protection as possible to employees' electronic communications.

C. Canons of Construction

The canons of construction are an often used tool of statutory interpretation designed as aids to discerning the meaning of a statute.118 There are several instances when certain canons are helpful to discern the meaning of the ECPA. The canons that are useful, each of which is applied at some point in the analysis below, are the following rather elementary canons. Words should be given their ordinary meaning.119 The statute should be interpreted as a whole.120 When comparing similar provisions, differences in drafting indicate differences in meaning.121 *Expressio unius:* "expression . . . of one thing indicates exclusion of the other." 122

One often heard complaint about the canons is that they can be used to support any position and even to support diametrically opposing interpretations of the same statute.123 Nonetheless, they are somewhat helpful in understanding the ECPA when used in a manner that is reasoned and mindful of the legislative objective to protect, rather than diminish, the privacy protection for electronic communications. Of course in some instances, courts have misused the canons by applying them in a rote manner, depriving employees of privacy protec-

---

117 Baumhart, *supra* note 20, at 927 ("Congress expressly intended the pre-ECPA prohibitions apply to employers who intercept employee telephone conversations. The courts consistently have given effect to that intent. Thus, it is feasible that Congress saw no need to specify that ECPA coverage likewise extends to employers.").


119 *Id.* at 849 ("Typically, courts will assume that the legislature uses words in their ordinary sense . . . ."); Norman J. Singer & J.D. Shambie Singer, *Sutherland Statutes and Statutory Construction* § 47:27, at 443 (7th ed. 2007); see *infra* Parts V.A.1.b., Contemporaneous (interpreting term "intercept") and V.A.1.c.i., Device (interpreting terms "device" and "apparatus").

120 Eskridge, *supra* note 118, at 862; Singer & Singer, *supra* note 119, §46:5, at 189–205; see *infra* Part V.B.1., Electronic Storage (interpreting "stored" in light of interpretation of suggested interpretation "intercept").

121 See Eskridge, *supra* note 118, at 867 ("Where Congress includes particular language in one section of a statute but omits it in another . . . . it is generally presumed that Congress acts intentionally and purposely in the disparate inclusion or exclusion.") (quoting Keene Corp. v. United States, 508 U.S. 200, 208 (1993) (alteration in the original omitted); *infra* Part V.A.1.b., notes 249–250 and accompanying text (comparing language of different provider exceptions).

122 Eskridge, *supra* note 118, at 867.

123 See *id.* at 942 (quoting Karl Llewellyn, *Remarks on the Theory of Appellate Decision and the Rules or Canons About How Statutes Are To Be Construed*, 3 Vand. L. Rev. 395, 401 (1950)) ("Hence there are two opposing canons on almost every point.").
tion.\textsuperscript{124} Overall, however, the application of the canons supports an interpretation of the statute that protects employees' basic right to privacy of their electronic communications.

D. Empirical Evidence of Negative Impacts of Electronic Monitoring

The right to privacy in electronic communications is not only of theoretical value but of practical concern. Legal writers have noted the negative health effects of electronic monitoring, including stress, physical health problems, and fatigue, on many employees.\textsuperscript{125} They have also reasoned that "efficiency and productivity levels are at their highest in workplaces that recognize and respect employee privacy."\textsuperscript{126} The psychology literature on employer monitoring of electronic communications confirms that while different types of monitoring can have different effects, in certain instances electronic monitoring can lead to negative health effects, such as stress and physical discomfort,\textsuperscript{127} and that for certain employees monitoring might decrease efficiency.\textsuperscript{128}

\textsuperscript{124} See, e.g., infra Part V.A.1.a., notes 161–62 and accompanying text (discussing courts' reliance on the canon suggesting interpreting a statute as a whole to interpret "intercept" not to include stored communications).


\textsuperscript{126} Kopp, supra note 20, at 864 (citing Gantt, supra note 17, at 419–24); see also Hornung, supra note 7, at 123–24 (noting that monitoring may lead to a perceived lack of trust and lower morale causing less efficiency).


\textsuperscript{128} Aiello & Kolb, supra note 127, at 348 (testing 202 undergraduate students in a laboratory setting and concluding that low-skilled participants were less efficient when monitored, while high-skilled participants were more efficient).
V. THE ELECTRONIC COMMUNICATIONS PRIVACY ACT

The ECPA is divided into parts, two of which are relevant to the protection of privacy of employees' electronic communications.129 Title I prohibits intentional interception of electronic communications130 and is commonly referred to as the Wiretap Act because it amended the previously enacted Wiretap Act to extend coverage to electronic communications. Title II, the Stored Wire and Electronic Communications and Transactional Records Access Act, prohibits unauthorized access to stored electronic communications and is commonly referred to as the Stored Communications Act ("SCA").

Both titles are important means of protecting the privacy of employees' electronic communications from employer monitoring. Because, however, the Wiretap Act provides for greater statutory damages131 and is subject to an interpretation that provides for more limited exceptions to liability than the SCA,132 a cohesive interpretation of the ECPA will provide coverage for as much employer monitoring as possible under the Wiretap Act, rather than solely under the SCA. The Wiretap Act also provides protections that may not be available under the SCA by prohibiting certain use and disclosure of intercepted electronic communications.133

---

129 Title III addresses pen registers and trap and trace devices.
131 18 U.S.C. § 2520(c)(2) (2006) (providing for greater of actual damages and profits or statutory damages of $100 a day for each day of violation up to $10,000); 18 U.S.C. § 2707(c) (2006) (providing for greater of actual damages and profits in no case less than $1,000); see Steve Jackson Games, Inc. v. U.S. Secret Service, 36 F.3d 457, 460 n.5 (5th Cir. 1994) ("Title I of the ECPA increased the statutory damages for unlawful interception from $1,000 to $10,000. On the other hand, as noted, Title II authorizes an award of 'the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation, but in no case . . . less than the sum of $1000.'") (citation omitted). Additionally, the Fourth Circuit has held that the SCA permits statutory damages only when actual damages are proved whereas the Wiretap Act permits statutory damages regardless. Van Alstyne v. Electronic Scriptorium, Ltd., 560 F.3d 199, 206–08 (4th Cir. 2009). But other lower courts have held differently. Id. at 206.
132 Compare infra Part V.A.2.b. (Wiretap Provider Exception) to Part V.B.3.a. (SCA Provider Exception).
133 18 U.S.C. § 2511(1)(b)–(d) (2006). In § 2702, the SCA does place restrictions on disclosure by entities providing "service[s] to the public." There is support for the argument that an employer that provides electronic communications services to its employees provides services to the public. The legislative history indicates that when a service provider such as the GSA's Federal Technology Service provides services only to governments and not the public more generally, it provides service to the public. H.R. REP. NO. 99-647, at 48 (1986). The distinction between the term "to the public" and the term "to the general public" used in another section also suggests that a service need not be open to everyone. Anderson Consulting LLP v. UOP, 991 F. Supp. 1041, 1042 (N.D. Ill. 1998); Blackowicz, supra note 21, at 98. And in some employment law contexts, such as suits
This section first addresses how the Wiretap Act should be broadly interpreted to cover employers' acquisition of a variety of employees' electronic communications. It then discusses how the SCA should be interpreted to prevent employers, who lack authorization, from accessing employees' stored communications.

A. The Wiretap Act

This section suggests interpretations of several of the terms in the Wiretap Act that courts have interpreted differently, leaving open issues about the level of protection employees will be afforded under the ECPA. To provide the greatest protection for employees' basic right to privacy, courts should interpret the Wiretap Act as follows: 1) to cover acquisition of a range of electronic communications, including some stored communications; 2) to restrict applicability of the three exceptions to coverage; and 3) to encompass electronic communications sent through any system that affects interstate commerce.

1. Interception

The Wiretap Act defines a prohibited interception, stating that an intercept is "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device."134

Contents "[include] . . . any information concerning the substance, purport, or meaning of that communication."135 The term "content" has been generally understood to exclude information such as to whom or from whom an electronic communication is being sent and also information such as that contained in a subject line of an e-mail message.136 While at first glance an inter-

---

136 Myrna L. Wigod, Privacy in Public and Private E-Mail and On-Line Systems, 19 PACE L. REV. 95, 113 (1998) (suggesting that contents does not include e-mail title headers); Blackowicz, supra note 21, at 88 ("It is important to note that the ECPA only protects the contents of messages, leaving employers free to monitor the transactional information of the e-mail, including who the sender and recipient are, the length of the message, and e-mail subject headings."). But see Matthew J. Tokson, The Content/Envelope Distinction in Internet Law, 50 WM. & MARY L. REV. 2105, 2130 (2009) ("Nonetheless, both the Department of Justice and the one district court to have
ELECTRONIC MONITORING OF EMPLOYEES

pretation of content that includes the information in a subject line might appear more protective of employees' privacy, by providing the employer a means to determine that a message is personal and not necessary to read further, the current understanding is actually protective of employees' privacy rights. An analogy to phone conversations is appropriate; generally, when an employer hears a personal call, the employer must stop monitoring or it violates the Wiretap Act. Two interrelated open issues under the Wiretap Act are whether an interception encompasses acquisition of stored communications and whether the acquisition must be contemporaneous with transmission. Courts that have not yet ruled on the issue can take the opportunity to read the Wiretap Act to apply to interception of stored electronic communications. To do otherwise renders the protection of the Wiretap Act generally inapplicable to e-mail and text messaging in the workplace. Excluding stored communications from interception also relies on a technical distinction that is unlikely to keep pace with changes in technology as demonstrated by the exceedingly brief storage of e-mail at various points during transmission.

Additionally, an intercept should not be interpreted to require contemporaneity. Rather, to intercept should mean acquiring any electronic communication 1) while being composed by or stored for transmission by the sender, 2) while in transit to the recipient, 3) while stored before being opened by the recipient, 4) while being opened by the recipient, and 5) while being stored by the recipient for a reasonable time period after opening the communication necessary to ensure an employer does not do an end run around the prohibitions of the Wiretap Act. The reasonable time period would be dependent on the totality of the factual circumstances. It would simply ensure that the employer was not engaging in the practical equivalent of an interception by simply waiting to retrieve the received, stored, but not yet deleted communication. The reasonable

commented on the matter have concluded that the subject header, despite its location in an email transmission, should be treated as content.”); Finkin, supra note 31, at 479 (“Thus, it remains to be seen whether or not tracking of addressees alone works a statutory ‘interception.’”).

See infra Part V.A.2.b. (Wiretap Provider Exception) and Part V.A.2.c. (Ordinary Course of Business Exception).

See infra Part V.A.2.c.

United States v. Councilman, 418 F.3d 67, 80 (1st Cir. 2005) (explicitly reserving the issue of whether an interception must be contemporaneous with transmittal).

Blackowicz, supra note 21, at 103 (“With an understanding of the nature of modern computers, a court may interpret the definition of ‘electronic communication’ to include the storage necessary before a message is acquired by the user.”).

Hall v. Earthlink Network, Inc., 396 F.3d 500, 503 n.1, 505 (2d Cir. 2005) (suggesting service providers’ continued receipt constitutes an interception unless it falls within the ordinary course of business exception).

Kerr suggests that “[w]hen stored communications are accessed in a way that makes the access the functional equivalent of a wiretap” such that the “purpose of the surveillance is to obtain copies of all incoming messages,” the stored communications should be considered inter-
time period should include the time in which any employer-provided equipment acquires and records the communication.143

a. Stored

An interception should be interpreted to include some stored communications to bring a wide variety of monitoring within the scope of the Wiretap Act, thereby protecting employees' basic right to privacy. To “intercept” is defined as to acquire the contents of an electronic communication.144 Nothing in the language of the definition indicates that stored communications are somehow exempt from acquisition.145 The definition of electronic communications excludes various communications but does not exclude stored communications.146 Thus, on its face, the Wiretap Act includes interception of stored electronic communications.147

Moreover, the clear legislative intent was to protect the privacy of electronic communications. More specifically, the Wiretap Act was to be interpreted flexibly to protect new types of electronic communications from interception.148 Because technologies like e-mail and pagers store electronic communications for minute time periods while in transit from sender to recipient, excluding stored communications renders the protection of the Wiretap Act inapplicable to many types of electronic communications.149 Employers can easily acquire the

cepted. Kerr, supra note 6, at 1232. This proposal builds on Kerr’s suggestion by subjecting not only an employer who acquires all messages but also the employer who acquires only three messages because, for instance, it suspects an employee of misconduct, to the Wiretap Act.

143 See Shefts v. Petrakis, 758 F. Supp. 2d 620, 630 (C.D. Ill. 2010) (“Based upon the undisputed facts concerning how the BES server functioned to log Plaintiff's text messages, the Court finds that an 'intercept' under the ECPA occurred when the BES software acquired and logged Plaintiff's text messages.”). But see Pure Power Boot Camp v. Warrior Fitness Boot Camp, 587 F. Supp. 2d 548, 557 (S.D.N.Y. 2008) (rejecting interpretation of contemporaneous as including employer's accessing employee's personal web based e-mail during “some undefined, short period of time after the e-mail had been delivered” because no authority to support that proposition was provided and no time frame was suggested); Bohach v. City of Reno, 932 F. Supp. 1232, 1236 (D. Nev. 1996) (holding that when a computer stores a message sent on the computer to a pager company, it does not intercept a communication but rather stores the communication, making the SCA and not the Wiretap Act apply to any claim involving a computer that records a message sent on that computer).


145 Id.


147 United States v. Szymuszkiewicz, No. 07-CR-171, 2009 WL 1873657, at *9 (E.D. Wis. June 30, 2009) (“The statutory definition of 'electronic communication' does not exclude messages in storage, and by its terms appears broad enough to include at least those communications stored temporarily as part of the e-mail transmission process.”).

148 See supra Part IV.B.

149 Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 888 (9th Cir. 2002) (Reinhardt, J., concurring in part and dissenting in part) (stating that electronic communications spend infinitesimal
contents of the communications while they are stored rather than while they are not. Thus, reading a stored communication exclusion into the definition results in less protection for employees' basic right.

The First Circuit's approach in United States v. Councilman, while not an employment case, is instructive on why the term "intercept" should be interpreted to include stored communications. In Councilman, the government prosecuted the owner of an Internet service provider for conspiracy to violate the Wiretap Act. Councilman ran an "online rare and out-of-print book listing service." His company provided e-mail service to book dealer customers. His information technology department arranged to intercept all e-mails from Amazon.com to the dealers before delivery to the recipient. The intercepted e-mails were copied, and the copy was placed "in a separate mailbox that Councilman could access." He and his employees read the e-mails to try to gain a commercial advantage. At all times, including when intercepted, the e-mails were "in the random access memory ("RAM") or in hard disks, or both, [of the company's] computer system." The court held that intercepting includes acquiring a communication in "transient electronic storage that is intrinsic to the communication process for such communications." The court first reasoned that a contrary interpretation would require an "inferential leap" rather than "a plain text reading of the statute." The court also reasoned that Congress's intent to include stored communications within the definition of electronic communications subject to an intercept is manifested by the specific exclusion of other categories of communications from the definition of electronic communication but not the exclusion of stored communications.

amounts of time in transmission so intercepting one, by definition, involves obtaining a copy made en route or at the destination).

150 418 F.3d 67 (1st Cir. 2005).
151 Id. at 79. See also Konop, 302 F.3d at 886–87 (Reinhardt, J., concurring in part and dissenting in part) (concluding that stored electronic communications are subject to the prohibition on interception); Konop v. Hawaiian Airlines, Inc., 236 F.2d 1035, 1046 (9th Cir. 2001), overruled by 262 F.3d 972 (9th Cir. 2001) (holding "that the Wiretap Act protects electronic communications from interception when stored to the same extent as when in transit"); Potter v. Havlicek, No. 3:06-cv-211, 2007 WL 539534, at *7 (S.D. Ohio Feb. 14, 2007) (relying on the dissents in Konop and Councilman to adopt the position that interception need not exclude stored communications).
152 Councilman, 418 F.3d at 70.
153 Id.
154 Id.
155 Id.
156 Id. at 70–71.
157 Id. at 71.
158 Id. at 79. See also Potter v. Havlicek, No. 3:06-cv-211, 2007 WL 539534, at *7 (S.D. Ohio Feb. 14, 2007) (stating that Councilman is the better reasoned decision).
159 Councilman, 418 F.3d at 73.
160 Id. at 75.
Several circuits have, however, interpreted the term "intercept" to exclude stored communications. They rely primarily on the structure of the ECPA being divided between prohibitions on interception and prohibitions on unauthorized access to stored communications. Yet the legislative history indicates that Congress understood the term "intercept" to be defined broadly. While at one point, the legislative history does indicate that stored communications include electronic communications that are in transit, it does not indicate that an interception of a stored communication is not possible. Even if stored communications in transit and those stored for a reasonable time period after opening the communication fall within both the Wiretap Act and SCA, there remain many circumstances when a communication would be stored long after the reasonable time period and have only the protection of the SCA. Additionally, when both the Wiretap Act and SCA apply to prohibit an employer's monitoring, the more stringent requirements of the Wiretap Act should apply because that approach is more protective of employees' right to privacy.

---

161 Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107, 113–14 (3d Cir. 2004); United States v. Steiger, 318 F.3d 1039, 1049–50 (11th Cir. 2003); Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 878 (9th Cir. 2002); Steve Jackson Games, Inc. v. U.S. Secret Service, 36 F.3d 457, 461–62 (5th Cir. 1994). Lower courts have also so held, including in some employment cases. Wesley Coll. v. Pitts, 974 F. Supp. 375, 384–89 (D. Del. 1997) (discussing how employees could not have intercepted e-mails unless they were in transit and not stored); Hudson v. Goldman Sachs & Co., 283 A.D.2d 246, 247 (N.Y. App. Div. 2001) (stating in passing that the Wiretap Act "prohibits only intercepts that are contemporaneous with transmission, i.e., the intercepted communication must be in transit, not in storage").

162 See, e.g., Konop, 302 F.3d at 878–79 (reasoning that law enforcement must follow more burdensome procedures under the Wiretap Act and that requiring law enforcement to comply with those procedures would defeat Congress's definition of stored as including "temporary, intermediate storage").

163 132 CONG. REC. H4039-01, H4045 (statement of Rep. Kastenmeier) ("The first principle is that legislation which protects electronic communications from interceptions by either private parties or the Government should be comprehensive, and not limited to particular types or techniques of communicating... ").

164 H.R. REP. No. 99-647, at 63 ("An 'electronic mail' service, which permits a sender to transmit a digital message to the service's facility, where it is held in storage until the addressee requests it, would be subject to Section 2701."). The report also indicates, however, that e-mail is protected by the Wiretap Act as well. Id. at 34 ("[Adding electronic communications] permits the inclusion in the general wiretapping and bugging law of many new forms of communication. For example, digitized transmissions and electronic mail will be provided with protection against interception.").

165 See also Konop, 302 F.3d at 889–90 (Reinhardt, J., concurring in part and dissenting in part) (reasoning that the SCA provides liability for computer hackers who acquire no content, permits law enforcement to seek content through service providers rather than through direct wiretapping, and permits a means to police unauthorized access).

166 A related concern arises in the criminal context because such an overlapping approach would require the government to obtain a court order under the Wiretap Act, rather than a search warrant or order under the SCA, to intercept the stored communications. While such an approach is no doubt more burdensome for the government, it also coincides with the legislative intent to provide a high level of privacy for electronic communications. The Councilman court noted that
The First Circuit effectively debunked the assertion that the distinction between the definition of wire communication, which explicitly included stored communications at the time the ECPA was enacted, and the definition of electronic communication, which did not explicitly so include, requires the exclusion of stored electronic communications from the definition of electronic communication. The definition of wire communication was included in the Wiretap Act before enactment of the ECPA and was only amended to make clear that stored communications were included. On the other hand, the definition of electronic communication was added to the Wiretap Act by the ECPA. Thus, no intent contrary to the plain language of the definition or contrary to the legislative intent to protect persons’ privacy should be inferred from the lack of parallel structure between the two definitions.

b. Contemporaneous

There is no indication in the definition of an interception that the acquisition must occur contemporaneously with transmission. While the plain meaning of the term “intercept” may, in some circumstances, indicate stopping on route to a destination, in others it indicates secretly obtaining a message. Both definitions are included in dictionaries. Thus, interpreting the term “in-
"intercept" to encompass not only acquisition while in transit, but also acquisition for a reasonable time period after opening the communication during which an employer could easily circumvent the intent of the statute to protect the privacy of electronic communications, fits sensibly within the common understanding of interception.

Because Congress intended to protect electronic communications from acquisition during transmission and to extend that protection beyond communications carried over common carrier systems, an interpretation of interception that includes time in transit and a reasonable time period thereafter best serves the legislative intent. An interpretation that extends to stored communications in transit but not communications immediately before and after transit would provide an unacceptable loophole in the employment context. Employers will argue that the provider exception to the SCA allows them to acquire the contents of their employees' electronic communications. This would lessen the incentive for employers to provide employees notice of the monitoring policy because of the Wiretap Act's consent requirement. It would, thus, risk lessening the number of safeguards available for employees' privacy.

However, even if the interpretation of interception is limited to including stored electronic communications while in transit, a number of methods currently used by employers to monitor employees' electronic communications

---

172 Potter v. Havlincek, No. 3:06-cv-211, 2007 WL 539534, at *7 (S.D. Ohio Feb. 14, 2007) ("This Court finds some merit in the position of Judge Reinhardt who opposes a hyper-technical application of the contemporaneous requirement emasculating the ECPA.") ; see United States v. Councilman, 418 F.3d 67, 76 (1st Cir. 2005) (quoting OFFICE OF TECHNOLOGY ASSESSMENT, FEDERAL GOVERNMENT INFORMATION TECHNOLOGY: ELECTRONIC SURVEILLANCE AND CIVIL LIBERTIES, available at http://www.fas.org/ota/reports/8509.pdf (1985)) (asserting that the desire was to protect five stages at which an e-mail could be intercepted: 1) "at the terminal or in the electronic files of the sender"; 2) "while being communicated"; 3) "in the electronic mailbox of the receiver"; 4) "when printed into hardcopy"; and 5) "when retained in the files of the electronic mail company for administrative purposes"); Baumhart, supra note 20, at 930 n.37 (relying on quoted portion of OTA report to argue that interception need not be simultaneous with transmission).

173 See infra Part V.B.3.a. (SCA Provider Exception).

174 See infra Part V.A.2.a. (Wiretap Consent Exception).

175 See Global Policy Partners v. Yessin, 686 F. Supp. 2d 631, 638 (E.D. Va. 2009) (concluding that "interception includes accessing messages in transient storage on a server during the course of transmission, but does not include accessing the messages stored on a destination server"). The court should have focused on whether the message was actually received by a person rather than the server. For instance, if someone places a note on the recipient's desk and before the recipient can hurry over to obtain it, someone else grabs the note, most would consider the note to have been intercepted despite having arrived on the desk. See Kinesis Adver., Inc. v. Hill, 652 S.E.2d 284, 296 (N.C. Ct. App. 2007) (employer who reviewed employees' e-mail accounts after they left the company did not intercept electronic communications because it "accessed the messages after they had been received and stored in the system"); Expert Janitorial v. Williams, No. 3:09-CV-283, 2010 WL 908740, at *7 (E.D. Tenn. March 12, 2010) (obtaining stored e-mail user-names and passwords over a time when the communications were not in "flight" is not an intercept).
will fall within the definition of an interception.\textsuperscript{176} Spyware such as Spectorsoft software that acquires electronic communications while in transmission\textsuperscript{177} and keyloggers that record keystrokes as electronic communications are devised\textsuperscript{178} would both run afoul of the Wiretap Acts prohibitions, unless an exception applies.

While some circuit courts have asserted that prior to the enactment of the ECPA the term interception had been interpreted to mean contemporaneous acquisition,\textsuperscript{179} only one cited circuit decision appears to have so held.\textsuperscript{180} There is no indication in the House or Senate reports or in statements on the floor that the legislators were aware of the case.\textsuperscript{181} The clarification of the definition of the term wire communication to include stored communications indicates Congress did not agree with the case.\textsuperscript{182}

Another potential concern is that the ECPA provides a time period of 180 days to determine when the government must have a warrant before acquiring stored communications from an electronic communications service.\textsuperscript{183} But the 180 day requirement does not suggest that an interception must be limited to transmission or exclude stored communications. Including a reasonable time period after opening the communication simply ensures that an employer's initial acquisition of an electronic communication will constitute an intercept, the-

\textsuperscript{176} See United States v. Councilman, 418 F.3d 67, 80 (1st Cir. 2005) (leaving issue of contemporaneity open but noting that when the message has not yet reached the recipient the interception would be contemporaneous under any definition); see also United States v. Szymuszkiewicz, No. 07-CR-171, 2009 WL 1873657, at *7 (E.D.N.Y. June 30, 2009) (finding use of auto-forwarding of e-mails to be contemporaneous).

\textsuperscript{177} The manufacturer of one such type of software "has characterized the new software as 'almost a wiretap."' Hornung, supra note 7, at 152 (citing Doug Fowler, President of SpectorSoft Corp., speaking about his e-mail monitoring program eBlaster). One court has held in the context of a divorce case that the use of Spector spyware results in an intercept because it contemporaneously acquires electronic communications at the time of transmission. O'Brien v. O'Brien, 899 So.2d 1133, 1137 (Fla. Dist. Ct. App. 2005) ("The Wife argues that the communications were in fact stored before acquisition because once the text image became visible on the screen, the communication was no longer in transit and, therefore, not subject to intercept. We disagree. We do not believe that this evanescent time period is sufficient to transform acquisition of the communications from a contemporaneous interception to retrieval from electronic storage.").


\textsuperscript{179} See, e.g., Steve Jackson Games, Inc. v. U.S. Secret Serv., 36 F.3d 457, 460 (5th Cir. 1994).

\textsuperscript{180} United States v. Turk, 526 F.2d 654, 658 (5th Cir. 1976) (pre-ECPA case requiring contemporaneous acquisition).

\textsuperscript{181} Konop v. Hawaiian Airlines, Inc., 236 F.2d 1035, 1046 (9th Cir. 2001), overruled by 262 F.3d 972 (9th Cir. 2001) (stating that the Fifth Circuit case that adopted the contemporaneity requirement had not been widely adopted by other courts when Congress passed the ECPA).

\textsuperscript{182} Congress has since amended ECPA to delete the inclusion of stored communications in the definition of wire communication. But later amendments do not reflect Congressional intent at the time of enactment.

reby encouraging employers to promulgate monitoring policies and to institute related safeguards. It does not deter the government from obtaining electronic communications that have been stored for over 180 days without a warrant, or even from obtaining most communications that have been stored for 180 days or less with a warrant rather than the court order required by the ECPA. Six months is a far longer time period than would typically be found to constitute a reasonable time period after opening the communication necessary to ensure an employer does not run around the prohibitions of the Wiretap Act.

Interpreting the term “intercept” broadly protects employees’ basic right to privacy but does not leave employers unable to satisfy their legitimate interests. Two exceptions to coverage—consent and the provider exception—can be interpreted by the courts in a manner that sensibly provides a high level of protection to employees while also enabling employers to monitor in appropriate circumstances.

2. Exceptions to Interception

The Wiretap Act contains three exceptions through which employers might be permitted to intercept electronic communications despite a relatively broad interpretation of interception that includes stored communications. These exceptions—the consent exception, the provider exception, and the ordinary course of business exception—should be restrictively interpreted.

a. Consent Exception

The Wiretap Act contains a consent exception that permits one party to an electronic communication to give prior consent to interception. The exception has been and should be interpreted to require knowing assent to monitoring. Such a construction encourages employers to implement safeguards for employees’ privacy, such as promulgating policies alerting employees to monitoring that are specific about the type, times, and extent of monitoring and using

---

184 Id.
185 18 U.S.C. § 2511(2)(d) (2006) (“It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State.”). While the legislative history focuses on the requirement that the purpose not be for a criminal or tortious act, the meaning of consent is more important in terms of protecting employees’ basic right to privacy.
186 See, e.g., Jandak v. Vill. of Brookfield, 520 F. Supp. 815, 820 n.5 (N.D. Ill. 1981) (“[C]onsent may be implied in fact, from surrounding circumstances indicating that the party knowingly agreed to the surveillance.” Consent will not be implied by law “if the party reasonably should have known.”).
The issue of consent arises fairly frequently in the employment law field. The term consent can be interpreted to have a variety of different meanings that might provide more or less protection for employees from electronic monitoring. Because employers and employees are generally in unequal bargaining positions, ensuring consent is often viewed as problematic. At one end, granting the most protection for employees would be the type of strong consent often required by European laws.\textsuperscript{187} Valid consent would allow an employee to refuse to agree to the proposed monitoring without suffering negative job consequences, including not only job loss but also other types of negatively perceived changes in terms and conditions of employment. At the other end, constructive consent would permit employers to claim employees consented to monitoring in situations where they "should have known"\textsuperscript{188} they were monitored or based on law, such as an employer's property right in an employer-issued computer.\textsuperscript{189} Just beyond that type of consent on the possible spectrum is implied consent based on the most minimal type of notice. For instance, the employer might promulgate a handbook that states the employer "may monitor" or "reserves the right to monitor." Then, by virtue of using employer-issued equipment, the employee impliedly consents to monitoring.\textsuperscript{190} In between is an interpretation of consent that requires actual notice of electronic monitoring and assent to the monitoring, or one or the other.

While expecting the courts to adopt strong European-style consent is probably unrealistic,\textsuperscript{191} several decisions dealing with the similar user authorization exception under the SCA do adopt an interpretation of consent similar to the European view.\textsuperscript{192} For instance, in one case, managers accessed a chat group

\textsuperscript{187}See Opinion 8/2001, supra note 98.

\textsuperscript{188}Jandak, 520 F. Supp. at 820 n.5 (stating that consent will not be implied by law "if the party reasonably should have known").

\textsuperscript{189}See Deal v. Spears, 980 F.2d 1153, 1156–57 (8th Cir. 1992) (rejecting employer’s arguments that employee consented to recording of her calls when she knew the employer had an extension line and employer had asked her to stop making personal calls and mentioned that employer might be forced to monitor or restrict her phone privileges if she continued to use the phone for personal calls).

\textsuperscript{190}See Chivvis, supra note 16, at 812 (criticizing case that found consent to monitoring of sales calls—but not personal calls—based on employee’s knowledge of employer policy of monitoring sales calls).

\textsuperscript{191}Even if the courts do adopt such a standard, there would be the difficulty of enforcing it. There is no means of enforcement apparent under the ECPA for an employee who does not consent and is not monitored but then receives negative job actions.

\textsuperscript{192}See, e.g., Pure Power Boot Camp. v. Warrior Fitness Boot Camp, 587 F. Supp. 2d 548, 562 (S.D.N.Y. 2008) (requiring that employee have opportunity to refuse or withdraw consent to monitoring); infra Part V.B.3.b. (SCA User Exception).
that was by invitation only and required a password. The employee who provided the password stated that “she felt she had to give her password to [a manager] because she worked [for the employer] and for [the manager].” She claimed that she would not have given him the password if he had not been a manager. The jury could infer that she was pressured or coerced into providing the password and as such did not authorize the use.

Absent the occurrence of most courts adopting an interpretation of consent requiring strong European-style consent, the courts should adopt a type of consent which requires, at a minimum, actual notice of and assent to the monitoring being conducted. Indeed, the majority of courts to interpret the term “consent” have required what is termed “consent in fact”—the employee or individual knew of the particular type of monitoring taking place, and evidence indicated that the individual assented to the monitoring. Not all courts have required explicit assent through a written or verbal statement; rather some have implied consent from the circumstances where the employee or individual knowing of the monitoring proceeds to engage in the monitored conduct. While a requirement of express consent would be most protective of employees’ rights, the legislative history corresponding to the original Wiretap Act manifests Congress’ intent that consent may be implied, at least in limited circumstances. These circumstances should be extremely limited in the employment context due to the general imbalance in power between the parties.

---

194 Id. at *3.
195 Id.
196 Id.
197 Griggs-Ryan v. Smith, 904 F.2d 112, 116–17 (1st Cir. 1990) (“Rather, implied consent is ‘consent in fact’ which is inferred ‘from surrounding circumstances indicating that the [party] knowingly agreed to the surveillance.’”) (quoting United States v. Amen, 831 F.2d 373, 378 (2d Cir. 1987)).
198 See, e.g., id. at 118 (holding that when landlord told a lodger she was recording all calls, he had imnpliely consented to her listening to one of his calls).
199 Berry v. Funk, 146 F.3d 1003, 1011 (D.C. Cir. 1998) (quoting United States v. Lanoue, 71 F.3d 966, 981 (1st Cir. 1995) (“Without actual notice, consent can only be implied when ‘[t]he surrounding circumstances . . . convincingly show that the party knew about and consented to the interception.’”) (emphasis added), overruled by United States v. Watts, 519 U.S. 148 (1997)); Jandak v. Vill. of Brookfield, 520 F. Supp. 815, 820 n.5 (N.D. Ill. 1981) (citing S. REP. No. 90-1097 (1968), reprinted in 1968 U.S.C.C.A.N. 2112, 2182). Ordinarily there is a distinction between notice and consent, indicating that some type of assent should be indicated by the facts. Of course, due to the inequality of bargaining power in the employment relationship, consent risks becoming a notice requirement. A notice requirement, however, does provide some type of safeguard for employees’ privacy. Ciocchetti, supra note 37, at 327; Levinson, supra note 29, at 652.
200 Some decisions indicate that the courts are willing to take the type of case into account when determining how to interpret terms in the ECPA as applied to a particular fact pattern. See, e.g., Watkins v. L.M. Berry & Co., 704 F.2d 577, 583 n.6 (11th Cir. 1983) (adopting more restricted interpretation of ordinary course of business exception in employment setting than in
Few employment cases address the issue of consent to interception of electronic communications, perhaps because there is guiding precedent for employers in the context of wire communications or perhaps because the issue is rarely reached with regard to electronic communications due to the narrow interpretation of intercept used by many courts. A broader interpretation of intercept will render the issue more salient.

The consent exception should be narrowly construed in order to provide strong protection for the privacy of employees' electronic communications. Indeed, several courts have emphasized that the consent exception should be narrowly construed. On the other hand, other pre-ECPA courts, most notably the Second Circuit, have stated in passing that the consent exception should be broadly construed. While such an interpretation would be contrary to the intent of the ECPA to robustly protect the privacy of electronic communications, the actual holdings in those cases have been based on facts that illustrate that the person monitored knew the monitoring was taking place and assented to it.

---

201 Sporer v. UAL Corp., No. C 08-02835 JSW, 2009 WL 2761329, at *6 (N.D. Cal. Aug. 27, 2009) (holding that an employee "knew his work email account was not private and was being monitored . . . and thus his consent may be implied"); Bohach v. City of Reno, 932 F. Supp. 1232, 1236 (D. Nev. 1996) (stating in dicta that an employee who sends a pager text message from an employer's computer impliedly consents to the computer acquiring and retaining the message).

202 In re Pharmatrack, Inc., 329 F.3d 9, 20 (1st Cir. 2003) (quoting Griggs-Ryan v. Smith, 904 F.2d 112, 117 (1st Cir. 1990)) ("Consent 'should not casually be inferred.'"); Griggs-Ryan v. Smith, 904 F.2d 112, 117 (1st Cir. 1990) ("And the ultimate determination must proceed in light of the prophylactic purpose of Title III—a purpose which suggests that consent should not casually be inferred."); Watkins v. L.M. Berry & Co., 704 F.2d 577, 581 (11th Cir. 1983) ("Consent under [T]itle III is not to be cavalierly implied. Title III expresses a strong purpose to protect individual privacy by strictly limiting the occasions on which interception may lawfully take place."); Hay v. Burns Cascade Co., Inc., No. 5:06-CV-0137 (NAM/DEP), 2009 WL 414117 at *8 (N.D.N.Y. Feb. 18, 2009) ("Implied consent should not be casually inferred and may be limited.").


204 For instance, in Amen the court reasoned that the defendants, who were taped while using prison telephones, impliedly consented to "the interception of their telephone calls" because at least four sources put them on notice of the prison's policy of intercepting calls. Id. at 379. First, the Code of Federal Regulations provides notice "of the possibility of monitoring." Id. Second, inmates received actual notice because the monitoring and taping system was discussed at an admission and orientation lecture. Id. Third, the inmates received actual notice because the inmate handbook stated, "[t]hese phones utilized by the inmates are MONITORED and TAPE . . . ." Id. Fourth, a notice on each phone stated, "[t]he Bureau of Prisons reserves the authority to monitor conversations on this telephone. Your use of institutional telephones constitutes consent to this monitoring." Id. One of the defendants had attended the admissions and orientation lecture and received a copy of the handbook. The other had been presented with a "form containing the written notice of the monitoring and taping system" that he refused to sign. Id. See also, e.g., Sporer v.
Knowledge of monitoring requires notice that the monitoring is actually taking place. The defendants, agents of the employer, set up a system “for electronically monitoring employee phone calls.” The system was meant to reduce the cost of telephone bills and to decrease employee theft. The defendants informed all the managers that telephone calls “would be subject to random monitoring and recording” and instructed them to inform their subordinates. Employees were also directed “to record long distance phone calls on provided telephone logs.”

The plaintiff, a particular high-level employee, had been told about the monitoring of employee telephone calls. The court found, however, that the record was unclear about whether the plaintiff knew that monitoring meant that phone calls were being intercepted and was unclear as to whether he knew that he was subject to monitoring. The court also found that the district court did not err by determining that he did not know. Without that level of minimal knowledge, the court concluded, consent cannot be inferred.

The fact that an employer has access to or owns a computer or that a computer is capable of intercepting an electronic communication should be insufficient to establish actual notice. One non-employment case is illustrative of this approach. The defendant argued that his wife had consented to him

UAL Corp., 2009 WL 2761329, at *6 (N.D. Cal. Aug. 27, 2009) (holding that employee impliedly consented to employer monitoring work e-mail for obscene attachments when he received e-mails about policy prohibiting obscene data, signed a policy stating he “should assume no right of privacy,” received a warning notice when turning on the computer that it was private and monitored by a security system forcing him to click “OK” to proceed, and received a previous warning for sending an inappropriate e-mail); United States v. Rittweger, 258 F. Supp. 2d 345, 354 (S.D.N.Y. 2003) (holding an employee who, among other things, signed an acknowledgement and consent form and used phones with warning stickers consented to employer taping phone calls).

Berry v. Funk, 146 F.3d 1003, 1011 (D.C. Cir. 1998) (“The key question in such an inquiry obviously is whether parties were given sufficient notice.”).

Williams v. Poulos, 11 F.3d 271 (1st Cir. 1993).

Id. at 275.

Id.

Id. at 276.

Id.

Id. at 281–82.

Id. at 282.

Id.

See Berry v. Funk, 146 F.3d 1003, 1011 (D.C. Cir. 1998) (holding that caller does not consent to call being monitored even if the caller knows the dispatchers have the capability to monitor and the dispatcher did not state he was getting off the line); Sheinbrot v. Pfeffer, Nos. 93 CV 5343, 94 CV 0649, 1995 WL 432608, at *4 (E.D.N.Y. 1995) (“[C]onsent cannot be implied from the mere fact that the Corporation’s multi-line phone system permitted defendant to eavesdrop unless the privacy option were activated.”).

accessing her electronic communications. 216 The defendant gathered the electronic communications from a computer that his wife knew he could access. 217 His wife used a “remember me” feature on her e-mail account despite knowing the defendant had access to the computer. 218 The court held that setting an e-mail account on a “remember me” feature on a computer to which a defendant has access does not amount to implied consent. 219 The court interpreted consent not to include constructive consent, but rather to include implied consent. 220 Implied consent requires that the party knowingly agreed to the surveillance, and the evidence about the “remember me” feature does not indicate that the wife knowingly agreed to the monitoring by the defendant. 221 By analogy, if an employee accesses a personal web-based e-mail account on an employer issued computer and is careless enough to leave the “remember me” feature on, that does not indicate that an employee consents to an employer signing onto the personal account and reading the personal communications. 222

Such an interpretation indicates that the dicta in one of the few employment cases involving electronic communications and touching on consent should be treated exactly as such—non-persuasive dicta. 223 In Bohach v. City of Reno, the court stated that it would likely find that an employee who sends a pager text message from an employer’s computer impliedly consents to the computer acquiring and retaining the message for review by the employer at a later time. 224 While an average employee might understand that the computer intercepts the message to transfer it to the paging company, that does not mean that the average employee knows that the interception is actually taking place or assents, without any notice, to the interception and continued storage for review by the employer at a later time.

Additionally, notice of one type or method of monitoring should not indicate consent to a different type or method of monitoring. Several cases illu-

---

216 Id. at *8.
217 Id.
218 Id.
219 Id.
220 Id. (quoting Dukes v. ADS Alliance Data Sys., Inc., 2006 WL 3366308, *13 (S.D. Ohio Nov. 20, 2006)).
221 Id. at *9.
223 Contra Hornung, supra note 7, at 145. Hornung, despite acknowledging that some courts hold that “consent ‘is not to be cavalierly implied,’” advocates that “in the email context the sender knows that a record of an email is that a record of it can be downloaded, printed, saved, and stored on the company email system.” Id. (quoting Watkins v. L.M. Berry & Co., 704 F.2d 577, 581 (11th Cir. 1983)). “Accordingly, by the act of sending an email via the Internet, the sender ‘expressly consents by conduct to the recording of the message.’” Id. (quoting Commonwealth v. Proetto, 771 A.2d. 823, 829 (Pa. Super. Ct. 2001)).
strate this principle.\textsuperscript{225} For instance, in \textit{Dukes v. ADS Alliance Data Systems, Inc.},\textsuperscript{226} the plaintiff worked as a debt collection agent for the defendant. The employee handbook stated: "We periodically monitor and tape phone calls with our customers to improve our associates’ telephone skills and job performance."\textsuperscript{227} It also stated "that [the defendant company] would provide its associates with the ‘opportunity to review information obtained by electronic monitoring when such information is used as the basis for any employment decision.’"\textsuperscript{228} The plaintiff had signed two consent forms.\textsuperscript{229} The consent forms stated that the employer would periodically record phone calls between employees and customers.\textsuperscript{230} Employees could also use the phones for a minimal amount of personal use.\textsuperscript{231} There were also pay phones available to use for personal calls.\textsuperscript{232} Supervisors listened to two of the plaintiff’s personal calls with her husband where she discussed work-related incidents.\textsuperscript{233} The court held that the acknowledgments signed by the plaintiff did not express consent to monitoring of personal calls.\textsuperscript{234} The policy and acknowledgments provided for monitoring of calls with customers, whereas these supervisors decided to monitor while knowing that the plaintiff was speaking with her husband.\textsuperscript{235} The court determined that she had consented only to a more limited monitoring—that of periodic monitoring of calls with customers.\textsuperscript{236} By analogy, if an employee has consented to monitoring of business-related e-mail, that does not constitute consent to monitor personal e-mail. An employer might, in many situations, be able to discern that an e-mail is personal by the non-content information regarding to whom it is sent or the subject line. Thus, the consent exception encourages employers to be very explicit with employees when they intend to monitor personal electronic communications.

In another non-employment case, a prison argued that an inmate impliedly consented to monitoring of a call by extension phone.\textsuperscript{237} The prison re-

\begin{footnotes}
\textsuperscript{225} \textit{See, e.g., In re Pharmatrak}, 329 F.3d 9, 20 (1st Cir. 2003) (holding that consent to collect certain data did not provide consent to collect web page visitors’ personal data).
\textsuperscript{226} No. 2:03-CV-00784, 2006 WL 3366308 (S.D. Ohio Nov. 20, 2006).
\textsuperscript{227} \textit{Id.} at *4.
\textsuperscript{228} \textit{Id.}
\textsuperscript{229} \textit{Id.}
\textsuperscript{230} \textit{Id.}
\textsuperscript{231} \textit{Id.}
\textsuperscript{232} \textit{Id.}
\textsuperscript{233} \textit{Id.}
\textsuperscript{234} \textit{Id.} at *12. \textit{See also} Watkins \textit{v. L.M. Berry & Co.}, 704 F.2d 577, 581 (11th Cir. 1983) (holding that employee consented to monitoring of personal calls for only so long as necessary to determine the call was personal).
\textsuperscript{235} \textit{Dukes}, 2006 WL 3366308, at *12.
\textsuperscript{236} \textit{Id.} at *13.
\textsuperscript{237} Campiti \textit{v. Walonis}, 611 F.2d 387, 393 (1st Cir. 1979).
\end{footnotes}
ELECTRONIC MONITORING OF EMPLOYEES

lied on the common practice to monitor such calls by having a guard actually listen to what the inmate was saying. 238 The prison argued “that the expectation of inmates was that calls would be monitored and that he kept the call short and the conversation innocuous.” 239 The court stated: “This boils down to the proposition that [the inmate] should have known his call would probably be monitored and he, therefore, gave consent.” 240 The court summarily held this did not amount to implied consent. 241 By analogy, if an employer notified an employee it would monitor e-mail messages by keyword searches of the subject line, this notice would not constitute consent by the employee to intercepting and recording the content of all messages for later review.

Because whether an employee consented to an interception is a factual determination, 242 courts should consider not only an employer’s promulgated policies but also an employer’s actual practices concerning monitoring. For instance, if an employer notifies employees it will monitor, but does not actually monitor, and employees are aware monitoring is not actually taking place, then an employee is not on notice of monitoring. In such a situation, the consent exception should not apply.

Philosophically, actual consent may not be possible in the employment setting because of the frequently unequal relationship in which an employee does not have the ability to refuse consent to monitoring. An interpretation of consent that is similar to a notice provision, requiring notice and assent to monitoring, does provide some level of protection for employees from overreaching employer monitoring of electronic communications. It encourages employers to promulgate policies and to use consent forms, written or electronic. It thereby encourages employers to think about their monitoring policies before engaging in monitoring and hopefully that results in more sound monitoring practices. 243 Additionally, it permits employees to understand that they are in fact being monitored and provides an opportunity for employees to change their behavior accordingly, such as by electing not to send a particular personal e-mail over a monitored system. 244

---

238 Id.
239 Id. at 393.
240 Id.
241 Id. at 394.
242 Jandak v. Vill. of Brookfield, 520 F. Supp. 815, 820 n.5 (N.D. Ill. 1981) ("[C]onsent may be implied in fact, from surrounding circumstances indicating that the party knowingly agreed to the surveillance." Consent will not be implied by law, "if the party reasonably should have known.").
243 See Ciocchetti, supra note 37, at 321.
244 See Levinson, supra note 29, at 652.
b. Provider Exception

Another exception exempts providers from the prohibition on interception in specified circumstances.245 Like the consent exception, the provider exception should be interpreted narrowly to provide a high level of protection for employees’ basic right to privacy in their electronic communications. The text of the exception itself indicates that it applies only in narrow, specified circumstances, as does a comparison between its language and broader language used in another provider exception in the SCA. The legislative intent also indicates that the exception should be construed narrowly. Ultimately, the exception should apply only to those employees who must engage in the interception as part of their normal job responsibilities. Additionally, the employee must do so because the interception is required to ensure that the electronic communication service is functioning or to prevent a loss of property or rights integral to the electronic communications service.

The plain language of the exception imposes several requirements before the exception applies. First, an agent of the provider of the electronic communications service must be engaging in the interception.246 Second, the interception must take place “in the normal course of employment.”247 In addition, the interception must take place either because it “is a necessary incident to the rendition of” the employee’s service or because it is necessary “to the protection of the rights or property of the provider of that service.” Very similar language is used in one provider exception in the SCA, whereas broader language that simply exempts conduct authorized by a provider is used in another section of the SCA.250 The contrast in language between those two sections indicates that the requirements included in the plain language of the exception are intended to have meaning. Thus, cases that interpret the language to exempt a provider under any circumstances, or even broadly to protect against mone-

246 Id.
247 Id.
248 Id. The exception states that an “agent of a provider of . . . electronic communication service” can intercept a communication “in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of that service.” Id.
249 18 U.S.C. § 2702(b)(5) (2006) (permitting disclosure by electronic communication services to the public and remote computing services to the public “as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service”).
250 18 U.S.C. § 2701(c)(1) (2006) (exempting “conduct authorized by the person or entity providing a wire or electronic communications service”). For further discussion of this exception, see infra Part V.B.3.a.
251 Ideal Aerosmith, Inc. v. Acutronic USA, Inc., No. 07-1029, 2007 WL 4394447, at *4, *6 (E.D. Pa. Dec. 13, 2007) (holding that a company that bought another company at bankruptcy and continued to receive e-mails intended for prior employees, transferred them to its server, and
tary loss,\textsuperscript{252} have misinterpreted the exception to the detriment of employees’ basic right to privacy.

Moreover, the legislative history suggests that this is a narrow exception focused on uses of information technologies necessary for the electronic communications system to run properly and to avoid a crash of the system rather than a broad right of an employer to protect its business.\textsuperscript{253} For instance, the Senate Report in related discussion mentions monitoring “to properly route, terminate, or otherwise manage . . . individual messages.”\textsuperscript{254} Indeed, the exception was only changed slightly by the ECPA and, as one scholar has noted, the courts interpreted the predecessor exception, “the Title III common carrier exception, narrowly.”\textsuperscript{255}

The requirement that the employee or agent engaging in the monitoring do so within the normal course of employment suggests that the exception permits only certain employees performing certain tasks to fall within the scope of the exception.\textsuperscript{256} For instance, while an information technology (“IT”) employee may ordinarily review the content of some messages when a professor reports a problem receiving a message, the dean likely does not normally do so. And

---


\textsuperscript{253} Cf. Chivvis, supra note 16, at 813–14 (critiquing a decision for failing to incorporate a legitimate business interests test into the provider exception); Droke, supra note 20, at 193 (suggesting the courts could use a strict business interest test pursuant to the provider exception). \textit{But see} Gruber & Maltby, supra note 8, at 44 (suggesting that private employers will be exempt from ECPA liability as long as they are the provider of the electronic system); Newman & Crase, supra note 23, at 114 (suggesting that the exception is broad). \textit{See also} Hash & Ibrahim, supra note 14, at 902 (“Courts may find that this includes such reasons as the need to prevent abuses of the system, including computer crime, system abuse, or impermissible personal use.”); Hornung, supra note 7, at 138 (asserting that in relation to a “proprietary email system,” an employer falls “squarely within the confines of the service provider exception to the ECPA”); Kopp, supra note 20, at 872 (suggesting that based on an unpublished California trial level court decision that employer-providers are exempt even if they read everything on the system); Anne L. Lehman, Comment, \textit{E-mail in the Workplace: Question of Privacy, Property or Principle?}, 5 COMMLAW CONSPECTUS 99, 102 (1997) (suggesting exception be broadly interpreted to include “the owner and operator of a private network - such as within a company”).

\textsuperscript{254} S. REP. No. 99-541, at 19 (1986), \textit{reprinted in} 1986 U.S.C.C.A.N. 3555, 3574. The Senate Report mentions this type of monitoring in its explanation of why the second clause prohibiting a provider of wire communications from using “service observing or random monitoring except for mechanical or service quality checks” does not also apply to electronic communications service providers. \textit{Id.}

\textsuperscript{255} Beeson, supra note 20, at 189.

\textsuperscript{256} \textit{See} Berry v. Funk, 146 F.3d 1003, 1009–10 (D.C. Cir. 1998) (holding that 1) monitoring contrary to an employer’s guidelines is not within the normal course of employment; 2) that a switchboard operator may intercept under the exception only that momentary part of a call that must be overheard to insure the call is placed; and 3) that a “switchboard operator, performing only the switchboard function, is never authorized simply to monitor calls”).
while the IT employee may review messages in that and other circumstances expected of his information technology job duties, the IT employee likely would not read the e-mails of his spouse, who works as an administrative assistant, in the normal course of his duties.

The further requirements additionally limit the circumstances in which the provider exception should apply. While certain interceptions may be necessary to ensure the proper working of the electronic communications system, others certainly are not. The requirements thus impose upon an employer an obligation to make sure that employees engaged in interception as a normal part of their employment are doing so in a manner protective of the privacy of employees' electronic communications. For instance, technological capabilities may require that a computer or other device used to send certain electronic communications intercept and retain that communication for a certain time period or until a certain user action takes place. In such instances, the interception by the device would likely fall within the provider exception. In other circumstances, however, employers intercept and retain electronic communications for a longer period than that required by the technology. In those instances, the provider exception should not apply, and the employer should instead seek consent to the interception from the employees.

Finally, the requirement of protecting rights and property should be limited to interceptions necessary to protect rights and property integral to the electronic communications system. Certain threats, such as system crashes or employees using pornography over the electronic communications system, directly impact the rights and property of the employer in its capacity as an electronic communications service provider. Interceptions necessary to protect against those threats should fall within the exception. On the other hand, other threats to the employer's property or rights do not relate to the employer in its capacity as an electronic communications service provider, and interceptions to

The author agrees with commentators who have suggested that interception to prevent computer crime or system failure would fall within the exception but disagrees with those asserting that interception to prevent unpermitted personal use would as well. Unpermitted personal use can often be identified simply by monitoring non-content information. See Lee, supra note 17, at 156 (suggesting "the courts may find that this includes such reasons as the need to prevent abuses of the system such as computer crime, system failure, or unpermitted personal use"). Cf. Beeson, supra note 20, at 193 (suggesting that the courts should "require employers to limit their monitoring to the message's address").

For an atypical example, see United States v. Mullins, 992 F.2d 1472, 1478 (9th Cir. 1993) (holding that when an airline employee investigated a travel agent's misuse of the airline's electronic ticketing service, the employee "was acting within the scope of her employment to protect the rights and property of her employer").

See Kaplan, supra note 14, at 297 (relying on Beeson, supra note 20, to suggest that "courts are likely to allow employer-providers to monitor, but only when employing the least intrusive means possible").
ELECTRONIC MONITORING OF EMPLOYEES

2012

protect against those threats should not fall within the exception.\textsuperscript{261} In those instances, consent should be required before the interception is engaged in or other means of prohibiting the threat should be used.

Certainly, the provider exception would not apply when the employer itself is not an electronic communications service provider. Thus, to the extent that employers subscribe to Internet service or use other third party providers of electronic communications services, the exception does not apply.\textsuperscript{262} The common understanding of an agent does not extend to a subscriber to another's communications service, and such a broad interpretation would be contrary to the legislative intent and the basic nature of employees' privacy.\textsuperscript{263} If the term agent were so broadly interpreted, communications service providers could be liable for and bound by the actions of subscribers in a variety of contexts. But even if the employer were an agent, it could assert the exception only if it met the requirements of taking action necessary to maintain the service or protect the provider's, not its own, rights and property.\textsuperscript{264} Additionally, the exception

\textsuperscript{261} Some threats to property that are made more likely when electronic communications systems are readily available, such as breach of confidentiality or theft of trade secrets, do not relate to the employer in its role as service provider. Thus, employers should seek employee consent if they believe it is necessary to monitor electronic communications because of those threats. \textit{Cf}. O’Grady v. Superior Court, 139 Cal. App. 4th 1423, 1441-42 (Cal. Ct. App. 2006) (interpreting 18 U.S.C. § 2702(b)(5) (2006), a similar exception used in the SCA to exempt electronic communications services and remote computing services from the requirement that they not divulge communications to third parties and reasoning a cost to an employer, such as of not complying with an unenforceable subpoena for disclosures is not enough to make compliance incident to protecting rights or property).

\textsuperscript{262} Baumhart, \textit{supra} note 20, at 927 ("[E]ven if an employer with an in-house system qualifies under the exemption, an employer who subscribes to an E-mail service probably would not fall within the exception."); Gruber & Maltby, \textit{supra} note 8, at 44 (explaining that the provider exception would not apply to monitoring e-mail services provided by an outside company or "client-based software that monitors activity directly on a computer terminal"); Rodriguez, \textit{supra note} 261, at 1452 ("At a minimum, the provider exception should not be able to be utilized by employers who furnish networks through public providers.").

\textsuperscript{263} But see Lehman, \textit{supra} note 253, at 102–103 (1997) (suggesting that when a public network is the provider, a subscribing employer should constitute an agent and fall within the exception). See also Hash & Ibrahim, \textit{supra} note 14, at 902 ("The term ‘provider’ would likely include public E-mail networks such as Prodigy and CompuServe, and the term ‘agent’ may or may not be defined to include employers who subscribe to or use such E-mail services.").

\textsuperscript{264} \textit{Cf}. McClelland v. McGrath, 31 F. Supp. 2d 616, 619 (N.D. Ill. 1998) (stating that phone company motivated by desire to help officers with kidnapping investigation was not protecting its own property).
would not apply when an employee is using a personal web-based e-mail account or a personal cell phone or other handheld device.

c. Ordinary Course of Business Exception

What is typically known as the ordinary course of business exception is not truly an exception but rather an exclusion from the definition of what constitutes an interception.\(^{265}\) The definition of intercept requires acquisition through a device,\(^{266}\) and a device is defined to exclude certain equipment used in the ordinary course of business.\(^{267}\)

As to many interceptions by employers of electronic communications, the exception should not apply because it requires the use of telephone or telegraph equipment.\(^{268}\) As to any to which it may apply, such as text messages sent by cellular phone, the ordinary course of business exception should be interpreted narrowly to provide a high level of protection for the privacy of employees' electronic communications.

i. Device

A device is defined somewhat circularly as "any device or apparatus" that can intercept electronic communications with some exceptions.\(^{269}\) One exception is for "any telephone or telegraph instrument, equipment or facility" being used in the "ordinary course of business."\(^{270}\)

The words "telephone" and "telegraph" should be read to modify "equipment or facility," so that each time an employer's computer or other similar equipment acquires content of an electronic communication the acquisition is considered an interception.\(^{271}\) The plain language is easily susceptible to such an

---

\(^{265}\) Deal v. Spears, 980 F.2d 1153, 1157 (8th Cir. 1992) (explaining that the exception is really a "restrictive definition").

\(^{266}\) 18 U.S.C. § 2510(4) (2006) ("'Intercept' means the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.").

\(^{267}\) 18 U.S.C. § 2510(5)(a) (2006) ("'[E]lectronic, mechanical, or other device' means any device or apparatus which can be used to intercept a wire, oral, or electronic communication other than . . . any telephone or telegraph instrument, equipment or facility, or any component thereof. . . .").


\(^{269}\) 18 U.S.C. § 2510(5).


\(^{271}\) Court & Warmington, *supra* note 14, at 30 ("Commentators disagree about whether this exception will ever be applied to e-mail, since such monitoring is arguably not accomplished with a 'telephone or telegraph instrument' . . . ."); Hash & Ibrahim, *supra* note 14, at 901 ("The first provision has been relied upon in telephone extension monitoring cases, but may not pertain to E-
ELECTRONIC MONITORING OF EMPLOYEES

interpretation, and limiting the exception narrowly to telephone or telegraph equipment provides a high level of protection for the privacy of employees' electronic communications. 272 Indeed, the legislative history indicates that the Senate understood the terms to modify not only the term "instrument" but also the terms "equipment" and "facility" because it refers to "telephone equipment provided by the user and connected to the facilities of a service provider" when discussing the scope of the exception. 273

Moreover, even pre-ECPA courts interpreted the exception narrowly to apply only to telephone and telegraph equipment. 274 For instance, the Fourth Circuit held that a device does not include a voice logger that an employer uses to record all phone calls made by security contractor employees and that the resulting surreptitious recording of an officer's calls violates the Wiretap Act. 275 The recordings were erased weekly. 276 The court reasoned that the voice logger was not a telephone or telegraph instrument or equipment because the phone company does not sell voice loggers and because it "in no way furthers the plant's communication system." 277

mail monitoring unless telephone equipment or facilities are specifically involved."; Lee, supra note 17, at 155 ("One provision has been relied on in telephone extension monitoring cases, but may not pertain to E-mail monitoring unless telephone equipment or facilities are specifically involved. Yet, courts may not consider a network manager's modem, computer, or software program to be telephone or telegraph equipment, and the leasing of telephone lines may not necessarily qualify under this exemption. Even in telephone extension cases, the telephone equipment distinction has been narrowly construed.") (footnotes omitted); Lori E. Lesser, Social Networks and Blogs, 1001 PLI/PAT 101, 151 (Apr.–May 2010) (stating that the business use exception in 2510(5)(a) does not apply to e-mail); Smith-Butler, supra note 14, at 67 n.128 (noting that the ordinary course of business exception has been applied only to telephone monitoring and not extended to e-mail); White, supra note 14, at 1086 ("The plain language of this section indicates that telephone or telegraph equipment is required for the exclusion to apply, and it is doubtful that courts will consider a modem (assuming one is even involved) to be telephone equipment.").

272 See Blackowicz, supra note 21, at 103 (arguing that to protect the privacy of employee's e-mail, computers should not constitute "an excepted interception device").

273 S. REP. NO. 99-541, at 13 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3567 (indicating the intent to extend the exception to "telephone equipment provided by the user and connected to the facilities of a service provider" but no intent to extend the exception beyond telephone and telegraph equipment).

274 United States v. Murdock, 63 F.3d 1391, 1396 (6th Cir. 1995) (holding that a recording mechanism is not telephone equipment); Beeson, supra note 20, at 185 ("The Sanders holding that recording devices do not qualify as 'telephone or telegraph' equipment suggests that the business-extension exception will not protect employers who monitor their employees' e-mail.") (footnote omitted).


276 Id. at 738.

277 Id. at 740. While there is a split in the circuits over whether, when a recorder is used, it is the recorder that intercepts, see, e.g., id., Deal v. Spears, 980 F.2d 1153, 1158 (8th Cir. 1992), or the telephone extension that intercepts, see, e.g., Epps v. St. Mary's Hosp., 802 F.2d 412, 415–16 (11th Cir. 1986), United States v. Harpel, 493 F.2d 346, 351 (10th Cir. 1974), there is no dispute in the circuit courts that a recorder would not constitute telephone equipment. But see, e.g., In re State Police Litig., 888 F. Supp. 1235, 1265 (D. Conn. 1995) (holding recording equipment con-
Thus, courts that construe the terms “telephone” and “telegraph” not to modify equipment and facility unnecessarily undermine the employees’ basic right to privacy.\textsuperscript{278} For instance, the Second Circuit has broadly applied the ordinary course of business exception to ISP providers although they do not use telephone or telegraph equipment. The court first reasons that the placement of the commas renders the statutory language ambiguous.\textsuperscript{279} The court then reasons that the legislative history exhibits an intent to include ISP providers.\textsuperscript{280} The court reasons that the legislature understood e-mail to be transmitted over telephone lines because that was the only technology available in 1986.\textsuperscript{281} The court further reasons it would be absurd not to include ISPs within the exception because otherwise they would be constantly engaged in unlawful interceptions.\textsuperscript{282} Yet, as discussed above, the legislative history indicates Congress did use the term “telephone” to modify the term “equipment.”\textsuperscript{283} More significantly, the primary intent of Congress to provide protection for the privacy of electronic communications is better served by a restrictive reading. Congress wanted the protections to apply to new technologies and applying the exception to interception by any type of device serves to undermine safeguards for employee privacy. In other words, interpreting the statute to adapt to new technology should be used to increase not decrease privacy protections. The result would be perfectly appropriate to require employers to rely on the consent or provider exception, rather than on the ordinary course of business exception, in instances when employers use computers and similar devices to intercept their employees’ electronic communications. Doing so permits employers to monitor while providing safeguards for employees’ privacy.

For similar reasons, courts that have gone one step further in denying employees protection for electronic communications by interpreting the term

\textsuperscript{278} But see Hornung, \textit{supra} note 7, at 138 (asserting that company e-mail system is a “component used in the ordinary course of business” and, thus, not “an electronic device for the purpose of the statute”); Newman & Crase, \textit{supra} note 23, at 12 (reading exception to apply to “any equipment or component used in the ordinary course of business”); Rodriguez, \textit{supra} note 18, at 1453 (suggesting that the “provision lawfully permits a network provider to access e-mail so long as . . . the intercepting device is part of the communications network”).

\textsuperscript{279} Hall v. Earthlink Network, Inc., 396 F.3d 500, 504 (2d Cir. 2005).

\textsuperscript{280} Id.

\textsuperscript{281} Id. at 504–05.

\textsuperscript{282} Id. at 505.

\textsuperscript{283} See S. Rep. No. 99-541, at 13 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3567 (indicating the intent to extend the exception to “telephone equipment provided by the user and connected to the facilities of a service provider” but no intent to extend the exception beyond telephone and telegraph equipment); cf. Beeson, \textit{supra} note 20, at 184–85 (arguing that the legislative history of Wiretap Act (pre-ECPA) demonstrates intent to limit telephone companies to listening to but not recording employee phone calls and that the narrow interpretation of the exception would “prevent employers from monitoring computerized forms of communication, such as e-mail”).

https://researchrepository.wvu.edu/wvlr/vol114/iss2/6

48
"device" not to include a computer\(^{284}\) have interpreted the Wiretap Act in a manner contrary to its primary intent—to protect the privacy of electronic communications. By their plain meaning, the terms "device" or "apparatus" encompass a computer,\(^{285}\) pager, or handheld device\(^{286}\) or a keylogger or spyware program.\(^{287}\) Interpreting "device" to exclude the acquisition of the majority of electronic communications from the prohibition on interception runs afoul of Congress' clear intent to protect electronic communications.

**ii. Ordinary Course of Business**

When telephone or telegraph equipment is being used to acquire an electronic communication, an employer must overcome an additional require-

\(^{284}\) Modrowski v. Pigatto, No. 09 C 7002, 2010 WL 2610656 (N.D. Ill. June 25, 2010) (suggesting that employer who opened former employee's e-mail account did not use a device); Conte v. Newsday, Inc., 703 F. Supp. 2d 126, 140 (E.D.N.Y. 2010) (stating in dicta that no intercept occurred because no device, other than the computer used by the recipients of the e-mails, was used); Ideal Aerosmith, Inc. v. Acutronic USA, Inc., No. 07-1029, 2007 WL 4394447, at \#4 (E.D. Pa. Dec. 13, 2007) ("The drive or server on which an e-mail is received does not constitute a device for purposes of the Wiretap Act"); Crowley v. Cybersource Corp., 166 F. Supp. 2d 1263, 1269 (N.D. Cal. 2001) (stating in its explanation of why Amazon, as the intended recipient of an electronic communication, did not intercept an e-mail, that Amazon "did not acquire it using a device other than the drive or server on which the e-mail was received"); see also Lehman, supra note 253, at 102 ("It is unclear from this definition whether a modem, software, or the specific computer system or organization used by the network manager will be considered an interception device by the courts. If these components are excluded from the definition of device, interception of e-mail would be permitted by this provision.").


\(^{286}\) Commonwealth v. Cruttenden, 976 A.2d 1176, 1181 (Pa. Super. Ct. 2009) (holding that the plain language of a Pennsylvania Wiretap Act does not require a device separate from the phone on which the text messages are composed to be used).

ment before falling within the exception for ordinary course of business. 288 Indeed, the exception requires that the equipment be used in the ordinary course of business. 289 Because the term "ordinary course of its business" is not defined, many telephone wiretap cases have addressed the exception,290 including a number dealing with employer monitoring of employees.

The exception should be interpreted to require an employer to act in a routine manner with a legitimate business purpose 291 and to provide notice to the employee of the monitoring. 292 Additionally, the monitoring of the content of personal electronic communications should take place only to the extent necessary to determine that the communication is personal. 293

288 Beeson, supra note 20, at 175 ("The first relevant exception to the ECPA is commonly known as the 'business-extension,' 'business use,' or 'ordinary course of business exception'.")

289 18 U.S.C. § 2510(5) (2006) ("electronic, mechanical, or other device" is defined, in pertinent part, as follows: any device or apparatus which can be used to intercept a wire, oral, or electronic communication other than—(a) any telephone or telegraph instrument, equipment or facility, or any component thereof, (i) furnished to the subscriber or user by a provider of wire or electronic communication service in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business or furnished by such subscriber or user for connection to the facilities of such service and used in the ordinary course of its business; or (ii) being used by a provider of wire or electronic communication service in the ordinary course of its business, or by an investigative or law enforcement officer in the ordinary course of his duties").

290 While Hall applies the exception to electronic communications, the interception involved would have been more appropriately analyzed under the provider exception. Hall v. Earthlink Network, Inc., 396 F.3d 500, 505 (2d Cir. 2005).

291 Hornung suggests that monitoring of web-based e-mail would not fall within the business use exception. "In the context of an employer email system, the monitoring aspect is built into the email system and is a basic part of its day-to-day function. However, in the web-based email context, any software that intercepts this type of email is extraneous to the company Internet system and has no necessary purpose for the business other than to monitor email." Hornung, supra note 7, at 151–52. The distinction between a provider and web-based e-mail is, however, more appropriately addressed by the provider exception because it makes provider status a key determination and is not limited to telephone equipment. Ordinary course of business should require more than simply being routine in order to adequately protect employees' rights, and, in some instances, if telephone equipment were used, an employer might monitor business communications similar to those of web-based e-mail in a routine manner because of a legitimate business concern and with notice to employees.

292 The Fifth Circuit in a pre-ECPA case made clear that the question of reasonable expectation of privacy is not the consideration that the statute makes primary in these cases. Briggs v. Am. Air Filter Co., Inc., 630 F.2d 414, 417 (5th Cir. 1980) ("The contention that an act of listening-in is not 'in the ordinary course of business' because the speaker had a reasonable expectation of privacy puts the cart before the horse. . . . The question before us is thus whether the act of listening-in was 'in the ordinary course of business.' If not, persons in situations similar to that of appellants have a reasonable expectation that private individuals will not violate federal law by listening-in to their calls.").

293 While some commentators perceive of two distinct approaches to interpreting the ordinary course of business requirement, one labeled a "context approach," which focuses on "the circumstances of the interception," and the other a "content approach," which focuses on whether it is a personal or business call, Newman & Crase, supra note 23, at 12, this proposal synthesizes both
One Sixth Circuit case illustrates the proposed approach to interpreting the term “in its ordinary course of business.” In the case, a police department employer tapped the pager issued to an officer employee without notice. For the employer to use the clone pager device in the ordinary course of business, the court held that the use must be: “(1) for a legitimate business purpose, (2) routine and (3) with notice.” The Sixth Circuit acknowledged that “there is some disagreement in the case law about whether ‘covert’ monitoring can ever be in the ‘ordinary course of business.’” It determined that while actual consent is not required, notice is required. The court further reasoned that “because it is undisputed here that plaintiff was not given any notice that his pager was being monitored, the exception cannot apply.” The court concluded that the defendant “did not routinely monitor officers’ pagers or give notice to officers that random monitoring of their department-issued pagers was possible.” It further reasoned that the plaintiff did not impliedly consent to the interceptions “simply because he accepted and used a department-issued pager.” A policy prohibiting personal use of employer-issued equipment does not constitute the necessary notice. This is particularly true when the policy is not enforced, and the employer is “aware that pagers were used by many” employees “for personal use.”

The requirement that the monitoring be routine necessitates that the monitoring must be the type normally engaged in by the employer. One of the many Wiretap Act cases dealing with prisons illustrates the principle well. Inmates’ calls were normally monitored by a guard standing close enough to hear what the inmate was saying. When an investigator for the security management team instead listened through an extension phone, the court held it was not within the ordinary course of business. By analogy, an employer who normally uses keyword searches to determine whether employees are sending porno-
graphic electronic communications could not one day decide, without precedent, to start reading the entire content of one employee’s communications because he suspected the employee was sending communications of a sexual nature.\(^{306}\)

The requirement that an employer monitor only with a legitimate business purpose limits protected acquisitions to those which are justified by a valid concern and are not overly intrusive.\(^{307}\) *Deal v. Spears* illustrates the principle that monitoring must be limited to that necessary for the stated business purpose to fall within the ordinary course of business exception.\(^{308}\) The court found the employer had

> a legitimate business reason for listening in: they suspected [the employee’s] involvement in a burglary of the store and hoped she would incriminate herself . . . . Moreover, [the employee] was abusing her privileges by using the phone for numerous personal calls even, by her own admission, when there were customers in the store. The [employer] might legitimately have monitored . . . calls to the extent necessary to determine that the calls were personal or made or received in violation of store policy.\(^{309}\)

But recording for twenty-two hours and listening to all the calls was not in the ordinary course of business.\(^{310}\) The suspicions did not “justif[y] the extent of the intrusion.”\(^{311}\) To the extent the employer’s purpose was to determine whether the employee was making personal calls, a proper interpretation would permit monitoring only for sufficient time to determine a call was personal. The case, nevertheless, well illustrates the application of a requirement of legitimate business purpose.

---

\(^{306}\) In certain circumstances, however, the provider exception might permit the employer to read the contents when necessary to protect against pornographic communications that violate the law. *See supra* Part V.A.2.b.

\(^{307}\) *See* Sanders v. Robert Bosch Corp., 38 F.3d 736, 741 (4th Cir. 1994). The court held that a voice logger used to record a sub-contractor’s employees’ calls was not used in the ordinary course of business. The justification the employer provided for the twenty-four hour surreptitious recording was bomb threats. The court reasoned that there was scant evidence of threats prior to the start of the recording and “no bomb threats were received throughout the period that recordings were made. We therefore question whether the record evidences a business justification for the drastic measure of 24-hour a day, 7-day a week recording of telephone calls.” *Id.* at 741. The dissent disagreed, reasoning that it is necessary to record 24-hours a day to capture bomb threats and was acceptable where calls were recorded but not listened to. *Id.* at 746 (Widener, J., dissenting).

\(^{308}\) 980 F.2d 1153, 1158 (8th Cir. 1992).

\(^{309}\) *Id.*

\(^{310}\) *Id.*

\(^{311}\) *Id.*
ELECTRONIC MONITORING OF EMPLOYEES

The notice requirement ensures that employers provide sufficient notice of the type of monitoring being engaged in so that employees should know of the monitoring. Many cases will be relatively clear-cut because employees have actual notice of the monitoring or because the employer has failed to provide the employees any notice of monitoring. Some cases, however, will involve an employer who has provided notice, despite an employee’s claim of lacking knowledge of the monitoring. The notice requirement ensures that, in such cases, an employer must have made a significant effort to notify the employee of the monitoring and the surrounding circumstances must prove that the employee should have known of the monitoring, so as not to dilute the level of protection afforded employees’ privacy. Jandak v. Village of Brookfield is illustrative. In the case, a supervisor listened to a recording of a call that a police officer had made on a routinely recorded line. The officer claimed not to know the line was recorded but the supervisor said all officers “are familiar with the equipment, have access to a chart designating which lines are recorded, and commonly know that the line used” was recorded. The court reasoned the recording was not “surreptitious; rather, it was routine monitoring of all calls on the investigative line, with more than adequate opportunity for” the officer to know of the monitoring. The court concluded that, “in the unusual circumstances of this case,” the officer “should have known that calls on the line he used were monitored. Considering his training and job situation, that he should have known constitutes sufficient notice.”

But see Arias v. Mut. Cent. Alarm Serv., Inc., 202 F.3d 553, 559 (2nd Cir. 2000) (“Whether notice is required depends on the nature of the asserted business justification, and here, where the recording is at least in part intended to deter criminal activity, the absence of notice may more effectively further this interest.”); Amati v. City of Woodstock, 176 F.3d 952, 955 (7th Cir. 1999) (reasoning that notice is not necessary, only that the monitoring take part for routine non-investigatory purposes); Berry v. Funk, 146 F.3d 1003, 1009 (D.C. Cir. 1998) (suggesting that covert monitoring must be justified by a valid business purpose).

James v. Newspaper Agency Corp., 591 F.2d 579, 581 (10th Cir. 1979) (noting that an employer who provides notice in writing in advance to its employees that it will monitor phone calls for abusive customers and help train employees on dealing with the public, acts in the ordinary course of business).

Sanders v. Robert Bosch Corp., 38 F.3d 736, 741 (4th Cir. 1994) (suggesting that most important to finding a voice logger was not used in the ordinary course of business was that employer never notified the employees of the recordings); cf. United States v. Harpel, 493 F.2d 346, 351 (10th Cir. 1974) (“[A] telephone extension used without authorization or consent to surreptitiously record a private telephone conversation is not used in the ordinary course of business.”).


ld. at 817.

ld. at 824.

ld. at 824-25. The court may not have properly applied the requirement that the employer act with a legitimate business purpose or even the requirement that notice of the type of monitoring be provided because the given reason for recording, “improve police emergency and investigative services,” id. at 824, was not the purpose for which the supervisor appeared to listen in—
The notice requirement serves to protect employees in a manner similar to the consent exception. Notice, however, is traditionally thought of as something different from and less protective of a person’s rights than consent. In the employment setting, the distinction between notice and consent is often problematic. Under the proposed cohesive interpretation of the Wiretap Act, the consent exception requires actual notice and assent to the monitoring. The ordinary course of business exception, applied in limited instances to electronic communications, requires a lesser protection: that employers provide sufficient notice that under the circumstances an employee should know of the monitoring. While the ordinary course of business exception does not in some instances provide the employee actual notice such that the employee can modify behavior accordingly, it does encourage employers to think about the types of monitoring in which they will engage and attempt to notify employees. It also works in tandem with the other requirements of routine monitoring justified by a legitimate business reason, again forcing the employer to conscientiously think about the types of monitoring in which it engages.

Some judges have objected that requiring notice under the ordinary course of business exception renders the consent exception superfluous. That objection is unwarranted when the requirements imposed by the terms “notice” and “consent” differ as they do in this proposed cohesive interpretation designed to protect employees’ basic right to privacy. Moreover, like the consent exception, permitting employers to monitor without notice only when the provider exception applies may appear somewhat inflexible; however, there are few probable instances, falling outside the provider exception, when an employer will be unable to stop problematic communications only without notice of monitoring. Because the goal is to provide a high level of protection for employee privacy, sacrificing the employer’s ability to act in such situations is a necessary
incident of providing a generally high level of protection of privacy for employees’ electronic communications. 324

If an employer discovers the employee is sending or receiving a personal electronic communication, the employer must cease monitoring because it is not in the ordinary course of business to acquire personal communications. The requirement that employers monitor only business related and not personal electronic communications provides a high level of protection for those electronic communications that should remain most private. Many courts have imposed this restriction in the context of telephone wiretap cases. 325 For instance, in one case the court reasoned that a conversation with a college friend or an adult who was not one of the employee’s clients would not fall within the business use exception, even if made during work hours. 326 "At the point defendants . . . determined that the call was personal and that plaintiff was not talking to a minor, they had an obligation to cease listening and hang up." 327

Because a search of non-content tracking information, such as a recipient name, subject line, or URL address, will often be sufficient to make such determinations, it often will not be permissible to search the content of a personal electronic communication at all. When a search of content is necessary, a keyword search may often be possible and, thus, required instead of acquisition of the complete content of the communication.

Given the somewhat inflexible nature of the ECPA and the limited protections for employees available under it, the limitation on monitoring personal electronic communications may seem somewhat restrictive. Nonetheless, this more protective interpretation, well-supported by the telephone cases, is preferable to one that would permit monitoring of personal electronic communications whenever monitoring was routinely performed with notice and for a legitimate

324 See supra Part IV.

325 See, e.g., Watkins v. L.M. Berry & Co., 704 F.2d 577, 583 (11th Cir. 1983) (A personal call can only be intercepted "to the extent necessary to guard against unauthorized use of the telephone or to determine whether a call is personal or not."); Hay v. Burns Cascade Co., Inc., No. 5:06-CV-0137 (NAM/DEP), 2009 WL 414117, at *15 (N.D.N.Y. Feb. 18, 2009) ("[A] personal call may not be intercepted in the ordinary course of business unless necessary to guard against unauthorized use of the telephone or to determine that the call is personal in nature."); Ali v. Douglas Cable Comm., 929 F. Supp. 1362, 1380 (D. Kan. 1996) (citing to Watkins as applying the accepted rule); In re State Police Litig., 888 F. Supp. 1235, 1266 (D. Conn. 1995) ("While the practice of recording calls in a police department generally may fall within the terms of the exception, the interception of private or privileged calls cannot."); Cady v. IMC Mortg. Co., 862 A.2d 202, 214 (R.I. Super. Ct. 2004) (noting that an employer listening in on personal conversations was not acting in course of ordinary business). But see Amati v. City of Woodstock, 176 F.3d 952, 956 (7th Cir. 1999) ("That personal as well as official calls were made on the line is irrelevant; all employees make personal calls on company phones; if all the lines are taped, as is the ordinary practice of police departments, then the recording of personal as well as official calls is within the ordinary course.") (italics omitted).


327 Id.
business reason. Additionally, personal communications could still be monitored consistent with the provider or consent exceptions. This would enable employers to monitor without notice under the provider exception in the most problematic circumstances, such as use of the system for child pornography or in a manner likely to cause a system crash, but would provide the employee the opportunity to consent to monitoring of personal communications for other reasons, such as breaches of confidentiality or inappropriate jokes.

3. Interstate Commerce Requirement

The ECPA defines “electronic communication” as “any transfer of signs . . . transmitted in whole or in part by a . . . system that affects interstate or foreign commerce . . . .” At least one court has indicated that monitoring of keystrokes does not constitute an interception when the keyboard is not connected to anything except a computer because the definition of an electronic communication requires that the system affect interstate commerce. Such an interpretation makes little sense in the majority of cases where employees are typing e-mails, and other communications, to be transferred throughout nationwide or international communications systems. The purpose of protecting employees’ basic right to privacy indicates that the composition of an electronic communication should be a point included within the protection from interception. Otherwise, employers, and others, could circumvent the ECPA by acquiring keystrokes rather than composed communications. The text of the Wiretap Act and the legislative history also indicate that such a restrictive reading of the interstate commerce requirement is erroneous.

By its plain terms, the Wiretap Act requires only that the system involved affect interstate commerce. The system should be interpreted to encompass not just the starting point of the keyboard or employee’s computer but the entire system involved. Such an interpretation is consistent with the choice

328 See supra Part IV.
329 The complete definition reads: “any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include—(A) any wire or oral communication . . . .” 18 U.S.C. § 2510(12) (2006) (exceptions (B)-(D) omitted). Unlike the definition for oral communication, protection is not dependent on the communicator’s reasonable expectation of privacy. McIntosh, supra note 20, at 546.
330 United States v. Ropp, 347 F. Supp. 2d 831 (C.D. Cal. 2004). See also Lee, supra note 17, at 153 (suggesting that courts may find the ECPA inapplicable to intracompany e-mail systems, “unless that system crosses state lines or perhaps connects to an interstate network”).
331 The placement of the restrictive clause “that affects interstate or foreign commerce” after the word “system” indicates that it modifies that term. The legislative history also makes clear that the restrictive clause modifies the word “system” because the House Report italicizes “system that affects interstate or foreign commerce” when discussing the requirement. H.R. Rep. No. 99-647, at 32 (1986). Even if the focus were on the “transfer” rather than the “system,” composing a communication that will travel through a system connected to the Internet affects interstate commerce.
of the term "system" rather than a more limited interpretation that the communication itself affects interstate commerce. Court interpretation of the related definition of wire communication indicates that the focus is on the entire system, not some discrete part or sub-system. 332 Additionally, as noted by one court, excluding acquisition of keystrokes "seems to read the statute as requiring the communication to be traveling in interstate commerce, rather than merely 'affecting' interstate commerce." 333 Indeed, the use of the term "affect" indicates that communications intended for transmission through the Internet or other global systems fall within the requirement. 334

Moreover, interpreting the interstate commerce requirement less restrictively furthers the legislative intent. The primary intent of the legislation was to protect the privacy of individuals' electronic communications, and e-mail was clearly intended to be protected. 335 Permitting the acquisition of e-mail while it is composed frustrates the intent to protect the privacy of such communications. Additionally, the House report discussing the requirement indicates that it is intended to be read broadly. The report states: "the Committee chose to extend federal jurisdiction to the maximum permissible constitutional limits by providing coverage of a person who provides or operates facilities for communications that affect interstate or foreign commerce." 336 The report further indicates that the system as a whole, not just a piece of equipment on the employer's property, is to be considered when determining whether interstate commerce is affected.

332 Epps v. St. Mary's Hosp., 802 F.2d 412, 414–15 (11th Cir. 1986) (reasoning that the focus should not be on one internal phone line between dispatch stations but rather on the entire phone system). But see Ropp, 347 F. Supp. 2d at 835 (rejecting the Government's argument that the employee "arrives at work each day, turns on her computer, and 'logs on' to a network that connects her to a server that, in turn, is connected to other servers that are part of the company's nationwide computer network").

333 Potter v. Havlicek, No. 3:06-cv-211, 2007 WL 539534, at *8 (S.D. Ohio Feb. 14, 2007) ("It seems to this Court that the keystrokes that send a message off into interstate commerce 'affect' interstate commerce."); see also Brahmana v. Lembo, No. C-09-00106 RMW, 2009 WL 1424438, at *6 (N.D. Cal. May 20, 2009) (reasoning that whether keystrokes had actually affected interstate commerce was better resolved after discovery, and, therefore, denying motion to dismiss).

334 White, supra note 14, at 1088 (stating the theory that employer systems that convey e-mails only within one state rests "on a frail foundation" because of "the encompassing construction 'affecting interstate commerce' has been given in Commerce Clause cases").

335 See e.g., S. Rep. No. 99-541, at 2 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3556 ("Today we have large-scale electronic mail operations . . . .); id. at 3 ("These services as well as the providers of electronic mail create electronic copies of private correspondence for later reference . . . . For the person or business whose records are involved, the privacy or proprietary interest in that information should not change."); id. at 4 (quoting Office of Technology Assessment report stating that "electronic mail remains legally as well as technically vulnerable to unauthorized surveillance."); id. at 8 ("Electronic mail systems may be available for public use or may be proprietary, such as systems operated by private companies for internal correspondence."); id. at 14 (An electronic communication . . . . includes electronic mail.").

336 H.R. Rep. No. 99-647, at 33 (1986). "The term 'electronic communication' is intended to cover a broad range of communication activities that affect interstate or foreign commerce." Id. at 35.
As to private equipment interconnected with outside providers, the report states that "interception of an electronic . . . communication at a point on the customer's premise" is a violation of the Wiretap Act.\textsuperscript{337} The report additionally notes that "where a user has interconnected its own equipment into a private network, communications carried on the network are fully entitled to the protections of" the Wiretap Act.\textsuperscript{338}

Under this proposal for a cohesive interpretation of the ECPA, an intercept is construed to include acquisitions of stored as well as transient communications, and only two exceptions apply to most interceptions of electronic communications, the consent and provider exceptions. Additionally, employers are not permitted to do an end run around the statute by using key-catchers to obtain keystrokes. Such an interpretation encourages employers to acquire electronic communications without consent only in certain circumstances when the acquisition is required to insure that the electronic communication service is functioning or because, without the acquisition, a loss of property or rights integral to the electronic communications service will result. The proposal, thus, encourages employers to promulgate policies governing use of electronic communications systems, to provide notice to employees of the types of monitoring in which they engage, to obtain express assent to such monitoring, and to enforce policies consistently.

**B. The Stored Communications Act**

The SCA provides protection from intentional unauthorized access of stored communications.\textsuperscript{339} The SCA remains an important source of protection for communications not covered by the Wiretap Act. For example, it protects an employee's post to a personal password-protected webpage that has been read by the intended recipients but has remained posted for a year thereafter. And it protects a personal electronic message sent on an employer system provided by

\textsuperscript{337} Id. at 33. While discussing the related interstate commerce requirement for a "wire communication" that uses the language "by the aid of wire . . . connection," the report points out that a sweeping reading would encompass any equipment with a "length of wire" in it. It confirms that equipment, like a switching station or keyboard, used to carry the communication to a significant extent from the point of origin to the point of receipt, is considered to affect commerce. Id. at 35.

\textsuperscript{338} Id. at 33.

\textsuperscript{339} The Stored Communications Act prohibits intentional access "without authorization [of] a facility through which an electronic communication service is provided" or exceeding "an authorization to access that facility" whereby the person "obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage . . . ." 18 U.S.C. § 2701(a) (2006). The ECPA defines "electronic storage" as "(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication." 18 U.S.C. § 2510(17) (2006). The ECPA defines "electronic communication service" as "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15) (2006).
ELECTRONIC MONITORING OF EMPLOYEES

an outside provider where the employee consented to the employer intercepting the message but not to retaining and later accessing it for disciplinary reasons.

This section suggests interpretations of several of the phrases and terms in the SCA that courts have interpreted differently, leaving open issues about the level of protection employees will be afforded under the ECPA. To provide the greatest protection for employees’ basic right to privacy, the SCA should be interpreted such that 1) “electronic storage” includes a broad range of stored communications, 2) an employer acts without authorization when it evades a structural barrier or acts without a legitimate business reason, and 3) the exceptions for authorization by the provider or user exempt a narrow range of conduct.

1. Electronic Storage

The SCA protects communications that are “in electronic storage.” A debate exists over whether the definition of “electronic storage” should be interpreted broadly or narrowly. Once the definition of “intercept” is clarified to

340 There has not been much, if any, controversy over the requirement that a person who accesses a stored communication without authorization must also obtain, alter, or prevent “authorized access to” the communication. Courts have interpreted it broadly to include viewing e-mails. See e.g., Fischer v. Mt. Olive Lutheran Church, Inc., 207 F. Supp. 2d 914, 926 (W.D. Wis. 2002) (reasoning that reading e-mails satisfies requirement and implying that changing a password and preventing user’s access to e-mail account also satisfies the requirement).

341 Electronic storage is defined as: “(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purpose of backup protection of such communication.” 18 U.S.C. § 2510(17).

342 The Ninth Circuit is, perhaps, the court to have most extensively discussed the definition of “electronic storage.” Theofel v. Farey-Jones, 359 F.3d 1066 (9th Cir. 2004). The court attempted to interpret “electronic storage” relatively broadly by holding that e-mails on NetGate’s servers “fit comfortably within” the definition of “backup” e-mails. Id. at 1075. The court reasoned that the definition of “back-up protection” applied to both intermediate and post-transmission communications and to communications recorded for the user or provider’s use. Id. at 1076. The court concluded that “an obvious purpose for storing a message on an ISP’s server after delivery is to provide a second copy of the message in the event that the user needs to download it again—if, for example, the message is accidentally erased from the user’s own computer.” Id. at 1075. Nevertheless, in an effort not to render the requirement superfluous, the court stated in dicta that a message retained by a service provider after the original copy has expired in the normal course would not be retained for back-up purposes and that messages between staff or messages a user has flagged for deletion from the server would likewise be excluded. Id. at 1076. But using an even broader definition of “back-up” that includes a broad swath of communications, whether opened or unopened and whether retained for purposes in addition to keeping a record for the user or provider, does not render the requirement that a communication be for “purposes of backup protection” superfluous. In some situations, for instance, a communication might inadvertently be retained despite the desire of both the user and the provider not to maintain a record of the communication. Moreover, as implied by one Judge, the ECPA is so complicated that regardless of the interpretation adopted, some provision will be rendered superfluous, but this should only occur in a manner that forwards the primary goal of protecting the privacy of electronic communications. Konop v. Hawaiian Airlines, Inc. 302 F.3d 868, 887–88 (9th Cir. 2002) (Reinhardt, J., dissenting).
include acquisition of certain stored communications, then an equally broad interpretation of the meaning of electronic storage makes sense. A broad interpretation prevents employers, or employees for that matter, from intentionally accessing electronic communications without authorization in instances when an intercept has not occurred. An interception may not have occurred, for instance, when contents are not acquired, when a device is not used, or when a communication is acquired at a time beyond a reasonable time period after opening the electronic communication.

In particular, the language, “any storage . . . for purposes of backup protection of such communication,” should be read broadly to include retention, rather than elimination, of an electronic communication when one of the functions of the retention is to provide a record of the communication for the user or provider. The fundamental purpose of protecting employees’ privacy supports a broad interpretation as does the legislative intent to protect the privacy of new forms of communications. The legislative history indicates that Congress was concerned that with the development of new technologies, records were maintained “which do not neatly fit within the legal categories which exist for older technologies.” The intent was to protect these records, specifically including those for back-up protection to maintain the system, preserve the integrity of the system, or preserve the property of the user. Congress intended that a

343 On the other hand, if the courts continue to apply the narrow definition of interception that excludes acquisition of stored communications, then perhaps a narrow interpretation of stored also makes sense. Then, interception of communications that were simply retained by employers but not for back-up purposes would possibly fall within the prohibition on intercepting the content of electronic communications. *Cf.* Baumhart, *supra* note 20, at 928 (stating that electronic storage exemptions are limited “to storage maintained for back-up purposes only” so that access is restricted to that only “for the convenience of the individual users whose messages may need to be ‘retrieved’ due to system malfunction”).

344 Jennings v. Jennings, 697 S.E.2d 671, 678 (S.C. Ct. App. 2010) (holding that e-mails on an internet service provider’s servers are stored for the purposes of back-up protection); White, *supra* note 14, at 1083 (“Based on this encompassing definition, most E-mail exists in electronic storage.”). *But see* United States v. Weaver, 636 F. Supp. 2d 769, 772 (C.D. Ill. 2009) (reasoning that electronic messages that remain archived, or stored, on the service system are not back-up copies because they are the only copy); Flagg v. City of Detroit, 252 F.R.D. 346, 363 (E.D. Mich. 2008) (reasoning that text messages that remain archived, or stored, on the service system are not back-up copies because they are the only copy).


347 H.R. Rep. No. 99-647, at 72 (discussing related sections of SCA and stating: “A person who subscribes to an electronic mail service may not realize it, but that service likely maintains a record of all system transactions for a period of time . . . Even if the subscriber reads the message and discards or deletes it, the system maintains it as a backup copy for system maintenance and integrity purposes.”).

348 *Id.* at 22 & n.34 (discussing how an e-mail provider “may retain copies of transmissions” and how “e-mail systems are designed to provide access to contents and copies of messages in case of system failure”); *id.* at 68 (noting in discussion of different government procedures to
wide breadth of stored materials would be covered. The Senate Report states that the term “electronic storage” covers “storage within the random access memory of a computer as well as storage in any other form including storage of magnetic tapes, disks or other media.” Ultimately Congress hoped that the SCA would tackle the “problem of unauthorized persons deliberately gaining access to, and sometimes tampering with, electronic or wire communications that are not intended to be available to the general public.”

Indeed, several courts have interpreted the definition broadly in the employment context. In one case, for example, an employer guessed the password to an employee’s Hotmail account to access messages that would support the employer’s claim that the employee was homosexual. The court held that e-mail “stored on a remote, web-based server that is owned by Microsoft, an electronic communication service provider” even when accessed by the employer on the employer’s computer is in electronic storage. In another case, the employer logged onto an employee’s Hotmail account, Gmail account, and e-mail account with another company. The court reasoned that the employer “accessed three separate electronic communication services,” and she obtained the employee’s e-mails “while they were in storage on those service providers’ access stored communications depending on amount of time stored that “[b]ack up protection preserves the integrity of the electronic communications system and to some extent preserves the property of the users of such as system”).

See Cardinal Health 414, Inc. v. Adams, 582 F. Supp. 2d 967, 976 n.2 (M.D. Tenn. 2008) (reasoning that when prior employee continued to read another employee’s e-mail, whether or not the e-mail had been opened, the e-mails remained in electronic storage); Pure Power Boot Camp v. Warrior Fitness Boot Camp, 587 F. Supp. 2d 548, 555 (S.D.N.Y. 2008) (“The majority of courts which have addressed the issue have determined that e-mail stored on an electronic communication service provider’s systems after it has been delivered, as opposed to e-mail stored on a personal computer, is a stored communication subject to the SCA.”); see also Bailey v. Bailey, No. 07-11672, 2008 WL 324156, at *6 (E.D. Mich. Feb. 6, 2008) (“The fact that Plaintiff may have already read the emails and messages copied by Defendant does not take them out of the purview of the Stored Communications Act. The plain language of the statute seems to include emails received by the intended recipient where they remain stored by an electronic communication service.”). But see KLA-Tencor Corp. v. Murphy, 717 F. Supp. 2d 895, 905 (N.D. Cal. 2010) (assuming, without deciding, that the definition of “electronic storage” is a narrow one and implying that because the employer’s server kept a copy of employee’s e-mails in order to synchronize the e-mails for viewing on different computers and not for the purpose of back-up protection, the e-mails on the employer’s server were not in “electronic storage”).

systems.\textsuperscript{357} Either of those actions, if done without authorization, would be a violation of the SCA.\textsuperscript{358} Moreover, the Third Circuit has noted that a lower court’s narrow interpretation of the term “stored communication,” was questionable when it excluded an employee’s e-mail stored on an employer’s server from protection by the SCA because it was simply in post-transmission storage and not in “backup storage.”\textsuperscript{359}

Some electronic communications, however, will be outside the protections of the SCA either because they are not stored by “an electronic communication service”\textsuperscript{360} or because the employer did not access “a facility through which an electronic communication service is provided.”\textsuperscript{361} Specifically, when an employer accesses electronic communications sent through a third party service but stored on the employer’s own equipment, the protections of the SCA will not apply.\textsuperscript{362} While at first glance this appears problematic, recognizing that

\textsuperscript{357} Id.

\textsuperscript{358} Id. at 556.


\textsuperscript{360} The ECPA defines “electronic storage” as “(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication.” 18 U.S.C. § 2510(17) (2006). The ECPA defines “electronic communication service” as “any service which provides to users thereof the ability to send or receive wire or electronic communications.” 18 U.S.C. § 2510(15) (2006). Cf. United States v. Steiger, 318 F.3d 1039, 1049 (11th Cir. 2003) (“Thus, the SCA clearly applies, for example, to information stored with a phone company, Internet Service Provider (ISP), or electronic bulletin board system (BBS). The SCA, however, does not appear to apply to the source’s hacking into” a personal computer to obtain self-made pornography “because there is no evidence to suggest [the computer] maintained any ‘electronic communication service’ . . . .”); Thompson v. Ross, No. 2:10-cv-479, 2010 WL 3896533, at *5 (W.D. Pa. Sept. 30, 2010) (noting that e-mail stored on hard drive of personal laptop is not in electronic storage); Hilderman v. Enea Teksci, Inc., 551 F. Supp. 2d 1183, 1204 (S.D. Cal. 2008) (suggesting that e-mails stored on employer-issued laptop computer are not stored by an electronic communication service).

\textsuperscript{361} The Stored Communications Act prohibits intentional access “without authorization [of] a facility through which an electronic communication service is provided . . . .” 18 U.S.C. § 2701(a)(1). It could be possible to interpret a “provider of an electronic communications service” and “entity providing a[n] . . . electronic communication service” to be different than “a facility through which an electronic communication service is provided” and “electronic communications service.” Such an interpretation would enable exclusion of employers who use third party providers from the provider exceptions while still permitting inclusion of communications stored on their databases and servers as protected by the SCA. One case well illustrates why such a technical distinction is not likely to become an accepted interpretation of the ECPA. Crowley v. Cybersource Corp., 166 F. Supp. 2d 1263, 1271 (N.D. Cal. 2001) (pointing out that if computers of users are considered facilities through which electronic communications service are provided, then a provider will be able to grant access to someone’s home computer to a third party). And, because of the strong protections of the Wiretap Act, little additional protection would be gained by such an interpretation.

the employer would have to have acquired the communication at some point that constituted an interception, and as a non-provider could do so only with the consent of the employee, demonstrates that overall this cohesive interpretation of the ECPA provides a relatively high level of protection for the privacy of employees' electronic communications. 363

2. Access and Authorization

The SCA prohibits accessing a facility through which an electronic communication service is provided without authorization. 364 No employment case located by the author discusses the term "access." 365 Generally, the term access should be interpreted broadly for several reasons noted by Professor Orin Kerr. 366 As a practical matter, carving out types of interactions with an electronic communication facility that should be exempt is difficult and creates the likelihood that the statute, designed to broadly prohibit "exceeding privileges," will exempt an "entire category of activity." 367 Additionally, due to the rapid rate of technological change, carving out types of interaction would "prove highly unstable and ultimately arbitrary." 368 Indeed, a broad interpretation well serves the goal of protecting the privacy of employees' electronic communications.

Courts have discussed the term "authorization" in employment cases. 369 An employer should be found to have acted "without authorization" or to have

---

employee email accounts, user-names, and passwords" sufficient to plead computer is a "facility through which an electronic communication is provided").

363 If on the other hand, the employer were considered a provider in such situations, then the SCA would apply to the communications stored on the employer's equipment, but this would also enable the employer to acquire some electronic communications without consent pursuant to the provider exception to the Wiretap Act, discussed supra Part V.A.2.b.


365 One court has held in a non-employment case that receiving a voluntary transmission of an electronic communication does not constitute access, defined as getting at or, somewhat circularly, gaining access. Crowley v. Cybersource Corp., 166 F. Supp. 2d 1263, 1271–72 (N.D. Cal. 2001).

366 Orin S. Kerr, Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes, 78 N.Y.U. L. Rev. 1596, 1646 (2003) (addressing computer misuse statutes and interpreting access to include "any time the user sends a command to that computer that the computer executes").

367 Id. at 1647–48.

368 Id. at 1648.


---
"exceeded" authorization when it circumvents a code-based restriction\(^{370}\) or acts without a legitimate business reason. Scholars and courts generally agree that a person who circumvents a code-based restriction, such as by guessing a password to an employee's personal e-mail, accesses the electronic communications without authorization.\(^{371}\) That interpretation protects employees' personal, structurally-protected electronic communications from prying from employers.\(^{372}\) Thus, electronic communications made by employees, particularly those made away from work or without use of employer equipment, such as employees’ privacy protected Facebook pages, restricted access web pages, and personal

\(^{370}\) See Kerr, supra note 366. The article argues for an interpretation of authorization in the related context of computer misuse statutes that is restricted only to circumventing code-based restrictions. It is concerned, among other things, that an interpretation that permits a breach of contract to constitute a lack of authorization permits a computer owner the power to define authorization and opens the floodgates of litigation to any instance when a user clicks through terms of use. Id. at 1649. Adding an additional prong of lacking a legitimate business reason does not open up the floodgates of litigation or provide control to computer users, like making any breach of contract constitute a lack of authorization would. It is a standard often used in employment cases, familiar to employers, and necessary given the generally unequal bargaining power and need to protect the privacy of employees' electronic communications. Moreover, the legislative history indicates that in some situations warnings might suffice as indicia of intended privacy. "A person may reasonably conclude that a communication is readily accessible to the general public if the telephone number of the system and other means of access are widely known, and if a person does not, in the course of gaining access, encounter any warnings, encryptions, password requests, or other indicia of intended privacy." H.R. REP. No. 99-647, at 62 (1986).

\(^{371}\) See, e.g., Pure Power Boot Camp v. Warrior Fitness Boot Camp, 587 F. Supp. 2d 548, 562 (S.D.N.Y. 2008) ("guessing" a password is not authorization, and would defeat the purpose of preventing hackers); Cardinal Health 414, Inc. v. Adams, 582 F. Supp. 2d 967, 976 (M.D. Tenn. 2008) ("Where the facts indisputably present a case of an individual logging onto another's e-mail account without permission and reviewing the material therein, a summary judgment finding of an SCA violation is appropriate."); Wyatt Tech. Corp. v. Smithson, No. CV 05-1309 DT (RZx), 2006 WL 5668246, at *9 (C.D. Cal. Aug. 14, 2006) (holding company monitored personal e-mail account without authorization), aff'd in relevant part, 345 F. App'x. 236 (9th Cir. Aug. 27, 2009); Sherman & Co. v. Salton Maxim Housewares, Inc., 94 F. Supp. 2d 817, 821 (E.D. Mich. 2000) (holding former employee did not access a database without authorization, when, among other things, the database was not structurally protected); Kerr, supra note 366, at 1649.

\(^{372}\) On the other hand, there is an explicit exclusion from the ECPA of electronic communications systems that are "configured so that such electronic communication is readily accessible to the general public." 18 U.S.C. § 2511(2)(g)(i) (2006). Some cases have undoubtedly interpreted "readily accessible to the general public" in an overbroad manner that would not be protective of employee's electronic communications. See, e.g., United States v. Ahrndt, No. 08-468-KI, 2010 U.S. Dist. LEXIS 7821, at *20–21 (D. Or. Jan. 28, 2010) (holding that when a user "shares files on iTunes over an unsecured wireless network" making the files available to "anyone with a laptop within 400 feet of" the user's house, that is enough to make the files "readily accessible to the general public"). Others have reasonably distinguished situations that require knowledge not publicly available, such as being on a list of eligible employee names, from situations where anyone can bypass a contractual warning and access the system. See, e.g., Snow v. DirecTV, Inc., 450 F.3d 1314, 1322 (11th Cir. 2006).
non-employer provided electronic mail, are protected from employers who attempt end-runs around the structural protections.\(^{373}\)

Additional protection is provided for the privacy of employees' electronic communications through the requirement that an employer act with a legitimate business reason, even when not circumventing a code-based restriction.\(^{374}\) When an employee uses employer-issued equipment to access electronic communications, those communications may then be stored on the employer's computer, server, or other equipment.\(^{375}\) In many potentially problematic instances, such as an employer who acquires and stores copies of an employee's personal web-based e-mails that the employee viewed on the employer's computer, the Wiretap Act and the requirement that an employer not circumvent a code-based restriction, like a password, will satisfactorily protect the electronic communication.\(^{376}\) In others, the additional requirement would be necessary. For instance, an employee's personal e-mail sent on an employer provided system, or system to which the employer subscribes, may have been acquired properly due to the provider exception or consent. Without this additional requirement, however, the employee's communication would lack protection from being accessed while stored such that an agent of the employer who has no need to do so could view the message for voyeuristic purposes or purposes of personal dislike rather than legitimate business reasons.

One case, while involving circumvention of a structural or code-based restriction, illustrates the possibility of such a situation. In *Global Policy Partners v. Yessin*, the plaintiff sued her husband and business partner, whom she was divorcing, for reviewing her work e-mail containing personal messages sent to her divorce attorney.\(^{377}\) The husband had somehow obtained the plaintiff's e-mail password and reviewed messages, some that she had not yet read,\(^{378}\) once they were in her mailbox. The husband claimed he was authorized to do so because he was a manager of the company.\(^{379}\) The court, however, declined to

\(^{373}\) Paul & Chung, *supra* note 14, at 41 ("[A]n employer should be careful when investigating an employee's password-protected Internet site, such as a MySpace page, blog, or forum so as not to violate the SCA."); see *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 879 (9th Cir. 2002) (assuming that employer accessed employee's website without authorization).

\(^{374}\) *But see* *People v. Klapper*, 902 N.Y.S.2d 305 (N.Y. Crim. Ct. 2010) (holding that, under New York statute that defines authorization, an employee must plead with specificity that the employee and not the employer owned a personal e-mail account and that the employee used a password or security device to protect the personal account).

\(^{375}\) This may happen either because the employer is a provider of the electronic communications system and acquires the communications pursuant to the Wiretap Act’s provider exception or because the employee has consented to the acquisition of the electronic communication.

\(^{376}\) The spy-ware or software used to acquire the structurally protected electronic communication would likely be found to circumvent a structural barrier because it performs an end-run around a password protected communication.


\(^{378}\) *Id.* at 639.

\(^{379}\) *Id.* at 635.
grant the husband’s motion to dismiss.\textsuperscript{380} The court reasoned that the inquiry into authorization is a fact specific one requiring a determination about expected norms in the particular type of situation.\textsuperscript{381} The court pointed out that the husband allegedly used a password to access someone else’s account and had no “legitimate business reason” to do so.\textsuperscript{382}

3. Exceptions

Additionally, the exceptions, somewhat circularly, provide that access without authorization is lawful if the conduct is authorized by the service provider or the user.\textsuperscript{383}

a. Provider Exception

The provider exception occurs “with respect to conduct authorized . . . by the person or entity providing a wire or electronic communications service . . .”\textsuperscript{384} As with the provider exception to the Wiretap Act, an employer should not be considered a provider when it subscribes to a third party service.\textsuperscript{385} Excluding such employers from the exception ensures that the protections of the Wiretap Act, requiring employee consent, apply if an employer intercepts such electronic communications. Likewise, if an employer accesses stored communications, it would again need the employee’s consent because an employer may

\textsuperscript{380} Id. at 637.
\textsuperscript{381} Id. at 636. The court relied on cases under the Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a) (2006), to so hold.
\textsuperscript{382} Id.; see also KLA-Tencor Corp. v. Murphy, 717 F. Supp. 2d 895, 905–06 (N.D. Cal. 2010) (reasoning that employee was authorized to use her own employer issued e-mail account in response to contention by employer that she had no legitimate business reason to delete particular communications).
\textsuperscript{383} 18 U.S.C. § 2701(c) (2006). The prohibition on unauthorized access does not apply “with respect to conduct authorized—(1) by the person or entity providing a wire or electronic communications service; (2) by a user of that service with respect to a communication of or intended for that user . . . .” There are additional exceptions not quoted here.
\textsuperscript{384} Id. An electronic communication service is defined as “any service which provides to users thereof the ability to send or receive wire or electronic communications.” 18 U.S.C. § 2510(15) (2006).
\textsuperscript{385} See note 262 and accompanying text; Kesan, supra note 14, at 296 (“[S]ome commentators warn that a narrow interpretation may not cover businesses that subscribe to a common carrier for e-mail.”); Blackowicz, supra note 21, at 90 (“If an employer provides e-mail service through an outside provider, then they may not fall under the provider exception.”). But see Bohach v. City of Reno, 932 F. Supp. 1232, 1236 (D. Nev. 1996) (holding that employer subscribing to commercial paging company was service provider because “the terminals, computer and software, and the pagers it issues to its personnel, are, after all, what provide those users with the ‘ability to send or receive’ electronic communications”); Kesan, supra note 14, at 296 (suggesting a broad reading of provider encompassing even employers who have an outside provider but store e-mails on their own computer or network).
not obtain stored communications without a user’s consent or that of the electronic communications service, which may not disclose the stored communications without the user’s consent.\textsuperscript{386} Thus, as more employers turn to providing employees Blackberries or other handheld devices where the service is provided by a third party rather than the employer, employees will have protection of those stored communications.\textsuperscript{387}

When an employer is the provider of the electronic communications system,\textsuperscript{388} such as with an internal e-mail system, despite the breadth of the exception permitting the employer to authorize anyone, including its own agents, to access the stored communications,\textsuperscript{389} the Wiretap Act continues to provide protection. The initial acquisition of the communication is governed by

\textsuperscript{386}18 U.S.C. § 2702(b)(3) (2006); Quon v. Arch Wireless Operating Co., 529 F.3d 892 (9th Cir. 2008), cert. denied, 130 S. Ct. 1011 (2009). One federal district court, addressing slightly different facts, reached a decision different than Quon and held that a public employer could obtain copies of text messages from a text messaging service that has ceased providing messaging but continued to retain text copies. Flagg v. City of Detroit, 252 F.R.D. 346, 363 (E.D. Mich. 2008). The court reasoned that the text messaging service was a remote computing service and not an electronic service provider, which would allow release pursuant to a subscriber’s consent. \textit{id}. The decision is flawed for several reasons, including that it does not mention that electronic communications service is defined by the Act. It also does not address the explicit subscriber exception for remote computing services, which it writes out of the ECPA by using a restrictive interpretation of the term “divulge.” It imports terms not in the Act such as “computer storage,” and it interprets the phrase “any storage . . . for purposes of backup protection” overly restrictively. \textit{id}. at 358–59, 363. Despite these flaws in the reasoning, the court’s logic would still protect the privacy of personal messages sent on an employer-issued text messaging device. \textit{See id}. at 358. In addition to using consent, public employers could use a warrant, court order, or administrative subpoena to require disclosure of employee’s electronic communications. 18 U.S.C. § 2701(c)(3); 18 U.S.C. § 2703(b)(3); \textit{see also} Thayer v. Chiczewski, No. 07 C 1290, 2009 U.S. Dist. LEXIS 84176, at *15 (N.D. Ill. Sept. 11, 2009) (implying that court could order plaintiff in civil suit to consent to disclosure).

\textsuperscript{387} \textit{See supra} note 64.

\textsuperscript{388} Some scholars have suggested that an employer should not fall within the provider exception. \textit{Mark A. Rothstein} & \textit{Lance Liebman}, \textit{Employment Law} 632 (6th ed. Found. Press 2007) (“For purposes of the ECPA, an employer has the same legal status as a commercial internet service provider to check on ‘system usage.’ Do you think this is what Congress intended?”); White, \textit{supra} note 14, at 1089 (predicting that because courts may define system providers narrowly to include only “public, commercial providers such as America On-line, Prodigy, and CompuServe,” employers should not rely on the provider exception). \textit{Cf.} Beeson, \textit{supra} note 20, at 199–200 (“Finally, a strong argument can be made that when an employer that owns its electronic communication system accesses employees’ stored communications for monitoring purposes, it is not acting as a service-provider and is not protected under Title II’s service-provider exception.”). While such interpretations would be more protective of employees’ privacy, they are difficult to reconcile with the text and with the legislative intent to include within the ECPA’s reach all types of providers of electronic communication systems, including intra-company systems.

\textsuperscript{389} \textit{See} Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107, 115 (3d Cir. 2004) (holding that employer that administered its own e-mail system fell within the literal terms of the provider exception); Freedom Calls Found. v. Bukstel, No. 05CV5460(SJ)(VVP), 2006 WL 845509, at *27 (E.D.N.Y. March 3, 2006) (noting an employer can access former employee’s stored messages where employer provides ability to send and receive electronic communications).
it and by the exceptions which require consent or very limited acquisition without consent under the provider exception. 390

b. User Exception

The SCA also excepts conduct authorized by a user. 391 The exception raises issues similar to those raised by the consent exception to the Wiretap Act. 392 To protect the privacy of employees’ electronic communications, user authorization should be found only in limited circumstances. As with the consent exception, the employee must have notice of the particular type of monitoring being conducted and must assent to the monitoring. 393 As noted by one court, carelessness that enables an employer to access an employee’s electronic communications does not amount to knowing assent. 394 Additionally, valid authorization is only given when the employee has the opportunity to refuse or withdraw assent to the monitoring and was not pressured into providing the employer a password or assenting to monitoring. 395 Moreover, the authorization should be valid only for the time and purpose and to the extent agreed to. 396

One case nicely illustrates the application of an understanding of user authorization that provides a high level of protection for employees’ privacy. 398

390 See supra Part V.A.
392 See supra Part V.A.2.a.
393 See Pure Power Boot Camp v. Warrior Fitness Boot Camp., 587 F. Supp. 2d 548, 559 (S.D.N.Y. 2008) (interpreting an employer’s monitoring policy to be limited to the company’s system and not to apply “to e-mails on systems maintained by outside entities such as Microsoft or Google”).
394 Id. at 561 (“The Court rejects the notion that carelessness equals consent.”).
395 Id. at 562 (requiring opportunity to refuse or withdraw consent to monitoring).
396 Pietrylo v. Hillstone Rest. Grp., No. 06-5754 (FSH), 2009 WL 3128420, at *1, *3 (D.N.J. Sept. 25, 2009) (suggesting that a jury could infer that an employee who provided a password to a chat group to a manager was pressured and as such did not authorize the use). For additional discussion of the facts of Pietrylo, see supra notes 193–196 and accompanying text.
397 Cf. Cardinal Health 414, Inc. v. Adams, 582 F. Supp. 2d 967, 977 (M.D. Tenn. 2008) (reasoning that former employee who continued to use a co-worker’s e-mail account, the password to which was provided by the co-worker when the employee still worked at the company and for work-related purposes, was not authorized to continue to use the account for non-work related purposes).
398 Pure Power Boot Camp, 587 F. Supp. 2d at 561. The understanding of authorization applied by the court does, however, differ in some respects from the proposed interpretation. 1) The proposed interpretation would not permit a notice that an employer may monitor to suffice for implied consent—rather there must be notice that monitoring is ongoing. Cf. id. (“Implied consent, at a minimum, requires clear notice that one’s conduct may result in a search being conducted of areas which the person has been warned are subject to search.”). 2) Considering whether an employee has a reasonable expectation of privacy is not necessary to determine, under the proposed standard, whether an employee authorized conduct. Rather the determination turns on notice and knowing unpressured assent. Cf. id. (“Because [the employee] had a reasonable expectation of
The court addressed an employer's claim that either an employer policy or an employee's conduct in leaving a username and password on an employer's computer constituted authorization for the employer to access the employee's web-based Hotmail account. The court held that the policy did not authorize the employer's conduct. The policy explicitly provided in part that "e-mail users have no right of personal privacy in any matter stored in, created on, received from, or sent through or over the system. This includes the use of personal e-mail accounts on Company equipment." The court interpreted the policy to be limited to the company's system and not to apply "to e-mails on systems maintained by outside entities such as Microsoft or Google." The court additionally reasoned that there was no evidence the e-mails obtained by the employer were "created on, sent through, or received" from the employer's computer.

The court also held that the employee did not authorize the employer's conduct by using the employer's computer to check personal web-based e-mail. The court reasoned: "[t]here is no sound basis to argue that [the employee], by inadvertently leaving his Hotmail password accessible, was thereby authorizing access to all of his Hotmail e-mails . . . If he had left a key to his house on the front desk at [the employer's facility], one could not reasonably argue that he was giving consent to whoever found the key, to use it to enter his house and rummage through his belongings."

VI. CONCLUSION

The enactment of a federal statute designed to regulate employer monitoring of employees would be ideal. It would be ideal for employees because it likely would cover more types of monitoring than the ECPA and would establish baseline protections for employees' basic right to privacy. It would also benefit employers because it would likely provide more consistent guidance across different jurisdictions and provide more selection of available safeguards for employees' basic right to privacy that employers could choose among in order to comply with the law. For all involved, it would likely be easier to interpret than the ECPA. Such federal legislation is unlikely to pass in the near

---

399 Id. at 552 ("Brenner states that she was able to access Fell's Hotmail account because he left his username and password information stored on PPBC's computers, such that, when the Hotmail website was accessed, the username and password fields were automatically populated.").

400 Id.

401 Id.

402 Id. at 559.

403 Id. at 560.

404 Id. at 561.
future, however, even with calls from major companies, civil rights groups, and scholars for privacy legislation.

Meantime, as shown in this Article, the ECPA can and should be consistently interpreted by the various courts in a cohesive manner designed to provide a high level of protection for employees' basic right to privacy. The Wiretap Act should be broadly interpreted to cover employers' acquisition of a variety of employees' electronic communications. The courts should interpret the Wiretap Act to cover acquisition of some stored communications, to restrict applicability of its three exceptions, and to encompass electronic communications sent through any system that affects interstate commerce. Further, the SCA should be interpreted to prevent employers, who lack authorization, from accessing employees' stored communications. The courts should interpret the SCA to include a broad range of stored communications within the term "electronic storage," to find an employer acts without authorization when it evades a structural barrier or acts without a legitimate business reason, and to exempt a narrow range of conduct under the exceptions by authorization. Adopting this consistent and cohesive interpretation would provide guidance for employers and encourage them to adopt monitoring policies consistent with the ECPA's requirements. It would also, however, provide employees recourse when employers fail to require the employees' consent and monitor personal communications without any appropriate reason. In this manner, the current United States law would further the goal of protecting employees' basic right to privacy.