Draft June 16, 2011
Forthcoming 114 West Virginia Law Review

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."

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 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 stating that 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 employees, 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 he were a SWAT (Special Weapons and Tactics) team officer and sent a higher number of salacious text messages, if the computer policy was extended to text messages in writing, 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").

The ECPA has been described by experts as dense[3], intricate,[4] and difficult for lawmakers,[5] lawyers,[6] and even scholars to interpret.[7] Because it contains criminal as well as civil provisions, many scholars addressing the ECPA deal with its application in the criminal law context rather

---

[1] 130 S. Ct. 2619 (2010).
[2] *Id*. at 2630.
[3] Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1208 (2004) ("Courts, legislators, and even legal scholars have had a very hard time making sense of the [Title II of the ECPA]. The statute is dense and confusing, and few cases exist explaining how the statute works.").
[4] 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.'").
[5] Steve Jackson Games, Inc. v. U. S. Secret Serv., 36 F.3d 457, 462 (5th Cir. 1994) (noting that [Title I of the ECPA] is "famous (if not infamous) for its lack of clarity"); Jeremy E. Gruber & Lewis Maltby, *The Need for Reasonable Policies*, 213 FEB. N.J. LAW. 41, 43 (2002) ("ECPA is quite notorious among courts and legal scholars for its lack of clarity and rampant ambiguity.").
[6] 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.")(citation omitted).
[7] Hornung, *supra* note 4, at 129 (2005)("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.").

than the employment law context.[8] 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 mechanism 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*,[9] 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.[10]

---

[8] *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."); Susan Freiwald, *Online Surveillance: Remembering the Lessons of the Wiretap Act*, 56 AL. 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.").

[9] Paul M. Schwartz, *Preemption and Privacy*, 118 YALE L.J. 902 (2009); Daniel Solove & Chris Hoofnagle, *A Model Regime of Privacy Protection*, 2006 ILL. L. REV. 357 (2006).

[10] Richard A. Bales & Richard O. Hamilton, Jr., *Workplace Investigations in Kentucky*, 27 N. KY. L. REV. 201 (2000); Kevin J. Baum, Comment, *E-mail in the Workplace and the Right of Privacy*, 42 VILL. L. REV. 1011 (1997); Elise M. Bloom, et al, *Competing Interests in the Post 9-11 Workplace: The New Line Between Privacy and Safety*, 29 WM. MITCHELL L. REV. 897 (2003); Lisa Smith-Butler, *Workplace Privacy: We'll be Watching You*, 35 OHIO N.U. L. REV. 53 (2009); Leonard Court & Courtney Warmington, *The Workplace Privacy Myth: Why Electronic Monitoring is Here to Stay*, 29 OKLA. CITY U.L. REV. 15 (2004); Jon Darrow & Steve Lichtenstein, *Employment Termination for Employee Blogging: Number One Tech Trend for 2005 and Beyond, or a Recipe for Getting Dooced?*, 2006 UCLA J.L. TECH. 4 (2006); Philip L. Gordon, *Job Insecurity?*, 79 DENV. U. L. REV. 513 (2002); Paul E. Hash & Christina M. Ibrahim, *E-Mail, Electronic Monitoring, and Employee Privacy*, 37 S. TEX. L. REV. 893 (1996); Christine E. Howard, *Invasion of Privacy Liability in the Electronic Workplace: A Lawyer's Perspective*, 25 HOFSTRA LAB. & EMP. L.J. 511 (2008); Stuart J. Kaplan, *E-mail Policies in the Public Sector Workplace: Balancing Management Responsibilities with Employee Privacy Interests*, 15 LERC MONOGRAPH SER. 103 (1998); Jay P. Kesan, *Cyber-Working or Cyber-Shirking?: A First Principles Examination of Electronic Privacy in the Workplace*, 54 FLA. L. REV. 289 (2002); Diana J.P. McKenzie, *Information Technology Policies: Practical Protection in Cyberspace*, 3 STAN. J.L. BUS. & FIN. 84 (1997); Christopher S. Miller & Brian D. Poe, *Employment Law Implications in the Control and Monitoring of E-mail Systems*, 6 U. MIAMI BUS. L.J. 95 (1997); Richard A. Paul & Lisa Hird Chung, *Brave New Cyberworld: The Employer's Legal Guide to the Interactive Internet*, 24 LAB.

Generally, scholars writing about workplace privacy have overlooked or dismissed the potential of the ECPA to provide privacy protection for employees in the electronic workplace,[11] some calling instead for its amendment[12] or for federal[13] or state legislation.[14] For instance, one author has proposed changes to the ECPA's consent exception based on European law.[15] A few have proposed a judicial interpretation of the ECPA addressing some particular problem.[16] For

---

LAW. 109 (2008); Marc A. Sherman, *Webmail at Work: The Case for Protection Against Employer Monitoring*, 23 TOURO L. REV. 647 (2007); Mia G. Settle-Vinson, *Employer Liability for Messages Sent by Employees Via Email and Voice Mail Systems*, 24 T. MARSHALL L. REV. 55 (1998); Matthew E. Swaya & Stacy R. Eisenstein, *Emerging Technology in the Workplace*, 21 LAB. LAW. 1 (2005); Jarrod J. White, *E-mail@work.com: Employer Monitoring of Employee E-mail*, 48 ALA. L. REV. 1079 (1997); John Araneo, Note, *Pandora's (E-Mail) Box: E-mail Monitoring in the Workplace*, 14 HOFSTRA LAB. L.J. 339 (1996); Ira David, Note, *Privacy Concerns Regarding the Monitoring of Instant Messaging in the Workplace: Is it Big Brother or Just Business?*, 5 NEV. L.J. 319 (2004).

[11] 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) (mentioning and dismissing).

[12] Matthew A. Chivvis, *Consent to Monitoring of Electronic Communications of Employees as an Aspect of Liberty and Dignity: Looking to Europe*, 19 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 799 (2009); Benjamin F. Sidbury, *You've Got Mail . . . and Your Boss Knows It: Rethinking the Scope of the Employer E-mail Monitoring Exceptions to the Electronic Communications Privacy Act*, 2001 UCLA J.L. & Tech. 5 (2001); Thomas R. Greenberg, Comment, *E-mail and Voice Mail: Employee Privacy and the Federal Wiretap Statute*, 44 AM. U.L. REV. 219 (1994); Lois R. Witt, Comment, *Terminally Nosy: Are Employers Free to Access Our Electronic Mail?*, 96 DICK. L. REV. 545 (1992).

[13] Shefali N. Baxi & Alisa A. Nickel, *Big Brother or Better Business: Striking a Balance in the Workplace*, 4 KAN. J.L. & PUB. POL'Y 137 (1994); Robert G. Boehmer, *Artificial Monitoring and Surveillance of Employees: The Fine Line Dividing the Prudently Managed Enterprise from the Modern Sweatshop*, 41 DEPAUL L. REV. 739 (1992); Frayer, *supra* note 7; Peter J. Isajiw, *Workplace E-mail Privacy Concerns: Balancing the Personal Dignity of Employees with the Proprietary Interests of Employers*, 20 TEMP. ENVTL. L. & TECH. J. 73 (2001); Laurie Thomas Lee, *Watch Your E-Mail! Employee E-Mail Monitoring and Privacy Law in the Age of the "Electronic Sweatshop,"* 28 J. MARSHALL L. REV. 139 (1994); Ray Lewis, *Employee E-mail Privacy Still Unemployed: What the United States Can Learn from the United Kingdom*, 67 LA. L. REV. 959 (2007); Larry O. Natt Gantt, II, *An Affront to Human Dignity: Electronic Mail Monitoring in the Private Sector Workplace*, 8 HARV. J.L. & TECH. 345 (1995); Michael L. Rustad & Sandra R. Paulsson, *Monitoring Employee E-Mail and Internet Usage: Avoiding the Omniscient Electronic Sweatshop: Insights from Europe*, 7 U. PA. J. LAB. & EMP. L. 829 (2005); Peter Schnaitman, *Building a Community Through Workplace E-Mail: The New Privacy Frontier*, 5 MICH. TELECOMM. & TECH. L. REV. 177 (1998-1999); S. Elizabeth Wilborn, *Revisiting the Public/Private Distinction: Employee Monitoring in the Workplace*, 32 GA. L. REV. 825 (1998); Note, *Addressing the New Hazards of the High Technology Workplace*, 104 HARV. L. REV. 1898 (1991); Susan Ellen Bindler, Note, *Peek and Spy: A Proposal for Federal Regulation of Electronic Monitoring in the Work Place*, 70 WASH. U. L.Q. 853 (1992); Mindy C. Calisti, Note, *You Are Being Watched: The Need for Notice in Employer Electronic Monitoring*, 96 KY. L.J. 649 (2008); Donald R. McCartney, Comment, *Electronic Surveillance and the Resulting Loss of Privacy in the Workplace*, 62 UMKC L. Rev. 859 (1994); David Neil King, Note, *Privacy Issues in the Private-Sector Workplace: Protection from Electronic Surveillance and the Emerging "Privacy Gap,"* 67 S. CAL. L. REV. 441 (1994); Amanda Richman, Note, *Restoring the Balance: Employer Liability and Employee Privacy*, 86 IOWA L. REV. 1337 (2001).

[14] Kevin J. Conlon, *Privacy in the Workplace*, 72 CHI.-KENT L. REV. 285 (1996) (calling generally for legislation); Alexander I. Rodriguez, *All Bark, No Byte: Employee E-mail Privacy Rights in the Private Sector Workplace*, 47 EMORY L.J. 1439 (1998) (proposing federal or state legislation).

[15] Chivvis, *supra* note 13.

[16] Jared D. Beeson, *Cyberprivacy on the Corporate Intranet: Does the Law Allow Private-Sector Employers to Read Their Employees' E-mail?*, 20 U. HAW. L. REV. 165 (1998) (arguing for interpretation of ECPA protective of employee e-mail messages sent on intranet systems); Julia Turner Baumhart, *The Employer's Right to Read Employee E-mail: Protecting Property or Personal Prying?*, 8 LAB. LAW. 923 (1992) (arguing, among other things, that legislative history suggests provider exception is not broad enough to exempt employers wholesale from the SCA's protections); Michael W. Droke, Comment, *Private, Legislative and Judicial Options for Clarification of*

instance, one author, among other proposals, has proposed a judicial interpretation of ECPA to protect employees from disclosure of personal e-mails.[17] Another has proposed that courts incorporate standards from English law, such as a right to know, relevance, quality, proportionality, and finality, under the ordinary course of business exception to the Wiretap Act.[18] Some authors focus only on one title of the ECPA rather than on both the relevant titles as an integrated whole.[19] None have proposed a cohesive interpretation of the ECPA designed to protect employees' basic right to privacy in their electronic communications.[20]

Employee Rights to the Contents of Their Electronic Mail Systems, 32 SANTA CLARA L. REV. 167 (1992); Kevin P. Kopp, Comment, *Electronic Communications in the Workplace: E-mail Monitoring and the Right of Privacy*, 8 SETON HALL CONST. L.J. 861 (1998) (proposing protection for purely person email sent on service provided to employer, who has no governing policy, provided by third party service provider); *see also* Tatsua Akamine, *Proposal for a Fair Statutory Interpretation: E-mail Stored in a Service Provider Computer is Subject to an Interception Under the Federal Wiretap Act*, 7 J.L. & POL'Y 519 (1999) (non-employment law article arguing intercept should be interpreted to encompass some stored communications); Dan McIntosh, *E-Monitoring@Workplace.com: The Future of Communication Privacy in the Minnesota Private-Sector Workplace*, 23 HAMLINE L. REV. 539 (2000) (proposing Minnesota courts apply Fourth Amendment expectation of privacy standard in ECPA cases).

[17] Jeremy U. Blackowicz, Note, *E-mail Disclosure to Third Parties in the Private Sector Workplace*, 7 B.U. J. SCI. & TECH. L. 80 (2001) (discussing judicial changes that would protect employees from disclosure of personal e-mails).

[18] Laura Evans, Comment, *Monitoring Technology in the American Workplace: Would Adopting English Privacy Standards Better Balance Employee Privacy and Productivity?*, 95 CAL. L. REV. 1115 (2007).

[19] Court & Warmington *supra* note 10; Kenneth A. Jenero & Lynne D. Mapes-Riordan, Electronic Monitoring of Employees and the Elusive "Right to Privacy," 18 EMP. REL. L.J. 71 (1992); Michael Newman & Shane Crase, *What in the World is the Electronic Communications Privacy Act? An Overview of the ECPA Hurdles in the Context of Employer Monitoring*, 54 FED. LAW. 12 (Nov./Dec. 2007); Eric P. Robinson, *Big Brother or Modern Management: E-Mail Monitoring in the Private Workplace*, 17 LAB. LAW. 311 (2001).

[20] Some articles about employee privacy or related topics briefly discuss the ECPA. *See, e.g.*, Patrick Boyd, *Tipping the Balance of Power: Employer Intrusion on Employee Privacy Through Technological Innovation*, 14 ST. JOHN'S J. LEGAL COMMENT. 181 (1999) (privacy); Dr. Colette Cuijpers, *ICT and Employer-Employee Power Dynamics: A comparative Perspective of United States' and Netherlands' Workplace Privacy in Light of Information and Computer Technology Monitoring and Positioning of Employees*, 25 J. MARSHALL J. COMPUTER & INFO. L. 37 (2007) (privacy); John Edward Davidson, *Reconciling the Tension between Employer Liability and Employee Privacy*, 8 GEO. MASON U. CIV. RTS. L.J. 145 (1997-98) (privacy); Rod Dixon, *Windows Nine-to Five: Smith v. Pillsbury and the Scope of an Employee's Right of Privacy in Employer Communiations*, 2 VA. J.L. & TECH. 4 (1997) (discussing common law); Rod Dixon, *With Nowhere to Hide: Workers are Scrambling for Privacy in the Digital Age*, 4 J. TECH. L. & POL'Y 1 (1999) (privacy); Clifford S. Fishman, *Technology and the Internet: The Impending Destruction of Privacy by Betrayers, Grudgers, Snoops, Spammers, Corporations, and the Media*, 72 GEO. WASH. L. REV. 1503 (2004) (privacy); Burton Kainen & Shel D. Myers, *Turning off the Power on Employees: Using Employees' Surreptitious Tape-Recordings and E-mail Intrusions in Pursuit of Employer Rights*, 27 STETSON L. REV. 91 (1997) (discussing employer rights); Joshua M. Masur, *Safety in Numbers: Revisiting the Risks to Client Confidences and Attorney-Client Privilege Posed by Internet Electronic Mail*, 14 BERKELY TECH. L.J. 1117 (1999) (attorney-client privilege); Amy Rogers, *You Got Mail but Your Employer Does Too: Electronic Communication and Privacy in the 21st Century Workplace*, 5 J. TECH. L. & POL'Y 1 (2000) (privacy); Seth Safier, *Between Big Brother and the Bottom Line: Privacy in Cyberspace*, 5 VA. J.L. & TECH. 6 (2000) (privacy); Robert Sprague, *From Taylorism to the Omnipticon: Expanding Employee Surveillance Beyond the Workplace*, 25 J. MARSHALL J. COMPUTER & INFO. L. 1 (2007) (off duty privacy); Robert Sprague, *Orwell was an Optimist: The Evolution of Privacy in the United States and Its De-Evolution for American Employees*, 42 J. MARSHALL L. REV. 83 (2008); William A. Wines & Michael P. Fronmueller, *American Workers Increase Efforts to Establish A Legal Right to Privacy as Civility Declines in the U.S. Society: Some Observations on the Effort and Its Social Context*, 78 NEB. L. REV. 606 (1999) (privacy); Harry M. Gruber, Note, *E-mail: The Attorney-Client Privilege Applied*, 66 GEO. WASH. L. REV. 624 (1998) (attorney client privilege); Hornung, Note, *supra* note 4, at 129;Allegra Kirsten Weiner, Note,

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. It provides novel means of interpreting terms such as "intercept" and "authorization" consistent with the text of the ECPA and the purpose of protecting privacy.[21] It compares and contrasts some provisions of the ECPA in ways heretofore overlooked[22] and digs into the legislative history finding support for the proposed interpretations.[23] 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.

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[24] 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.[25]

Business-Only E-mail Policies in the Labor Organizing Context: It is Time to Recognize Employee and Employer Rights, 52 FED. COMM. L.J. 777 (2000) (NLRA); Kara R. Williams, Note, *Protecting What You Thought Was Yours: Expanding Employee Privacy to Protect the Attorney-Client Privilege from Employer Computer Monitoring*, 69 OHIO ST. L.J. 347 (2008) (attorney client privilege).

[21] *See infra* Part V.A.1 and V.B.2.

[22] *See infra* notes 221--222 and accompanying text (contrasting provider exceptions).

[23] *See infra* note 226 and accompanying text (provider exception); note 245 and accompanying text (term telephone modifies term equipment); note 295 (interstate commerce requirement).

[24] Use of this phrase has been attributed to Kathy Stone. Michael Selmi, *Privacy for the Working Class: Public Work & Private Lives*, 66 LA. L. REV. 1035, 1037 n.8 (2006).

[25] *See* Ariana R. Levinson, *Industrial Justice: Privacy Protection for the Employed*, 18 CORNELL J.L. & PUB. POL'Y 609, 615 (2009).

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 indicate that a great number of employers electronically monitor their employees. The AMA's 2007 data indicate that 43 percent of employers monitored employee's e-mail and computer files, 66 percent monitored the Internet, 12 percent monitored the blogosphere, and ten percent monitored social networking sites.[26]

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 article that 14 million of these employees were under continuous surveillance, a number that excluded spot-checking and reasonable suspicion surveillance.[27] He estimated that 12 percent of employers did not inform employees of their policies regarding electronic monitoring.[28] 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.[29]

SpectorSoft is an example of the type of software that employers might use to monitor their employees.[30] 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."[31] 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 . . . ."[32]

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.[33] The tort requires a reasonable expectation

---

[26] AMA/EPOLICY INST. RESEARCH, AM. MGMT. ASS'N, 2007 ELECTRONIC MONITORING & SURVEILLANCE SURVEY (2008) *available at* http://www.amanet.org/research/pdfs/electronic-monitoring-surveillance-survey08.pdf.
[27] Matthew W. Finkin, *Information Technology and Workers' Privacy: The United States Law*, 23 COMP. LAB. L. & POL'Y J. 471, 474 (2002).
[28] *Id.*
[29] Rustad, *supra* note 13, at 830 (citing *Survey: Most Employers Monitor E-mail, Internet Use*, SACREMENTO BUS. J., Oct. 8, 2003, *available at* http://www.bizjournals.com/sacramento/stories/2003/10/06/daily20.html).
[30] Hayes v. Spectorsoft Corp., No. 1:08-cv-187, 2009 U.S. Dist. LEXIS 102637, at *7 (E.D. Tenn. Nov. 3, 2009).
[31] *Id.* at *6.
[32] *Id.* at *3. For a detailed and comprehensive description of other types of monitoring done by employers see Corey Ciocchetti, *The Eavesdropping Employer: A Twenty-First Century Framework for Employee Monitoring* (May 2010), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1617785.
[33] *See* Ariana R. Levinson, *Carpe Diem: Privacy Protection in Employment Act*, 43 AKRON L. R. 331, 337, n.18 (2010) (listing scholars).

of privacy, which is normally found to be reduced in the employment setting.[34] It also requires the invasion of privacy to be offensive, and courts often find that employers' rights outweigh those of employees to privacy protection.[35] 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.[36]

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 companies to adopt adequate safeguards, 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.[37]

Thus, the likelihood of employers obtaining communications that employees' consider private has risen substantially as technology has advanced. And there is a need for the law to adapt to address the problem.

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.[38] For instance, one recent decision

---

[34] MATTHEW W. FINKIN, PRIVACY IN EMPLOYMENT LAW, 346 (2d ed. 2003).
[35] *Id*. at 346; Clyde W. Summers, *Individualism, Collectivism and Autonomy in American Labor Law*, 5 EMPLOYEE RTS. & EMP. POL'Y J. 453, 469 (2001).
[36] *See* Levinson, *supra* note 33, at 340, n.37 (listing scholars).
[37] *Id*. at 385-86.
[38] 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. United States v. Councilman, 418 F.3d 67, 80 (1st Cir. 2005) (intercepting includes acquiring a communication in "transient electronic storage that is intrinsic to the communication process for such communication."); Global Policy Partners v. Yessin, No. 1:09cv859, 2009 U.S. Dist. LEXIS 112472, at *15 (E.D. Va. Nov. 24, 2009) (concluding that "interception includes accessing messages in transient storage on a server during the course of transmission. . . ."); Pietrylo v. Hillstone Restaurant Group, No. 06-5754, 2009 WL 3128420 (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 (S.D.N.Y.) (requiring that employee have 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 exclude stored communications); Fischer v. Mt. Olive Lutheran Church, Inc., 207 F. Supp. 2d 914 (W.D. Wis. 2002) (reasoning that unauthorized access includes reading an employees' emails on password protected webbased account). *See also* Kelly Schoening & Kelli Kleisinger, *Off-Duty Privacy: How Far Can Employers Go?*, 37 N. KY. L. REV. 287, 315 (2010) ("recent cases have found [Title II of the ECPA] to be more beneficial to employees than originally thought.").

suggests that courts will interpret 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. [39] 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*,[40] the employer allegedly used a system to monitor an employee's keystrokes[41] on an employer-issued keyboard to discover an employee's personal e-mail password.[42] The employer then allegedly used the password to access the personal e-mail account.[43] The employee asserted that the employer unlawfully intercepted and used his personal password.[44] The court denied the employer's motion to dismiss these ECPA claims.[45] 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.*,[46] the employer, the Ontario Police Department, issued "two-way alphanumeric pagers" to its employees.[47] The city contracted with an outside service

[39] Stengart v. Loving Care Agency, 201 N.J. 300 (S. Ct. 2010) (holding attorney-client privilege protects e-mails sent on company issued laptop through personal, password-protected, web-based e-mail account); Pure Power Boot Camp v. Warrior Fitness Boot Camp, 587 F. Supp. 2d 548, 555 (S.D.N.Y. 2008) (holding that an employee's e-mail sent from his personal e-mail account on a third party service provider system remains attorney-client privileged if the employee inadvertently leaves the login information on an employer computer when checking personal e-mail at work and the employer thereby obtains the password and reads the e-mail on the web-based system).
[40] Brahama v. Lembo, No. C-09-00106 RMW, 2009 WL 1424438 (N.D. Ca. May 20, 2009).
[41] The allegation was that the employer "used 'software and hardware monitoring tools such as local area network analyzers and key loggers' to obtain the password to his personal email account." *Id*. at *2.
[42] *Id*. at *1.
[43] *Id*. at *2.
[44] *Id*. at *2, n.1 , *3.
[45] Brahama v. Lembo, 2009 WL 1424438, at *3 No. C-09-00106 RMW (N.D. Ca. May 20, 2009). 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." The interstate commerce requirement is discussed *infra* Part VII.C..
[46] Quon v. Arch Wireless Operating Co., 529 F.3d 892 (9th Cir. 2008) *cert. denied* 130 S. Ct. 1011 (Dec. 4, 2009).
[47] *Id*. at 895.

provider, Arch Wireless Operating Co., to provide the pagers and the text messaging services on the devices.[48] 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.[49] But when the lieutenant tired of badgering people for payment, a higher level manager decided to investigate the plaintiff's personal use of the pager.[50] The employer then requested from the service provider a copy of plaintiff's text messages,[51] and the service provider released them.[52] Neither the manager nor the service provider notified the plaintiff that the lieutenant, the manager, and his supervisor would be reading his text messages, nor did they seek consent from the plaintiff. The court reversed the lower court's grant of summary judgment to the service provider.[53] 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.[54] Thus, to the extent that more employers are issuing hand-held 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.[55]

IV. Guiding Principles

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

---

[48] *Id*.
[49] *Id*. at 897.
[50] *Id*. at 897-98. Another employee with an overage was also investigated. *Id*. at 897-98.
[51] Quon v. Arch Wireless Operating Co., 529 F.3d 892, 898 (9th Cir. 2008).
[52] *Id*.
[53] *Id*. at 900.
[54] *Id*. (quoting Stored Communication Act, §2510 (15)).
[55] While difficult to quantify, popular perception indicates that the use of employer issued handheld devices is on the rise. *See e.g.* Stephanie Chen, *Personal Texting on a Work Phone? Beware your Boss*, CNN, Apr. 20, 2010, 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."); Tresa Baldas, *Overtime Suits May Ripen with BlackBerrys*, 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); KEVIN BURDEN, IDC, BUSINESS BENEFITS OF INDUSTRY-SPECIFIC MOBILE APPLICATIONS (2005), *available at* http://www.blackberry.com/solutions/pdfs/Business_Benefits_OISMA.pdf (discussing the growth and usage of BlackBerrys among various industries); *Customer Success*, BLACKBERRY, http://na.blackberry.com/eng/newsroom/success/ (last visited Oct. 18, 2010) (listing hundreds of employers' case studies regarding their use of BlackBerry smartphone devices for their employees). 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 (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 . . .").

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 below 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.[56] 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.[57]

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 employees.[58] The ECPA, however, is already titled toward employers' interests. For instance, the ECPA provides no protection at all for employees from several types of monitoring, including GPS[59] and silent video.[60] 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

---

[56] Blackowicz, Note, *supra* note 17, 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 33, at 422 n.532.

[57] *Cf.* Steven Winters, *The New Privacy Interest: Electronic Mail in the Workplace*, 8 HIGH TECH. L.J. 197, 232-33 (1993) (arguing that when development of new technology leaves a gap in protection of employee's privacy, courts should allow a cause of action).

[58] *See* Levinson *supra* note 33, at 403 (listing harms to employer that may justify monitoring with appropriate safeguards for employees' privacy).

[59] Jill Yung, *Big Brother is Watching: How Employee Monitoring in 2004 Brought Orwell's 1984 to Life and What the Law Should Do About It*, 36 SETON HALL L. REV. 163, 195 (2005).

[60] Thompson v. Johnson Cnty. Cmty. Coll., 930 F. Supp. 501 (D. Kan. 1996). Recently, a suburban school district issued students laptops and then used webcams to photograph certain students' activities, including when "partially undressed or sleeping. . . ." Changes to the ECPA have been proposed as a result of the incident. Maryclaire Dale, *Family: Pa. School Snared 1,000s of Webcam Images*, ABC NEWS, Apr. 16, 2010, *available at* http://abcnews.go.com/Technology/wireStory?id=10391728.

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.[61] 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.[62] The precedents also illustrate how the basic right to privacy extends to protection from electronic surveillance and to searches of employees by 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.[63]

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,[64] and to protect against electronic eavesdropping.[65] While decades before that the Court had found no such protection,[66] 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.[67]

As for workplace privacy, in *O'Conner v. Ortega*,[68] the Court recognized that employees have a right to privacy even from their employers. The employer searched the employee's employer-

---

[61] 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. . . .").
[62] *See* Joseph R. Grodin, *Constitutional Values in the Private Sector Workplace*, 13 INDUS. REL. L.J. 1, 2, 25-29 (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).
[63] 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 12, at 800; *see also* Avner Levin, *Is There A Global Approach to Workplace Privacy?*, at *2, *available at* http://ssrn.com/abstract=988105 (describing rights approach to privacy in the employment relationship that focuses on dignity).
[64] Katz v. United States, 389 U.S. 347 (1967).
[65] Berger v. New York, 388 U.S. 41 (1967).
[66] 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").
[67] *See* Mitchell Waldman, *Expectation of Privacy in Computer Files and Internet Communications; Effect Thereof*, AM JUR. 2D COMPUTERS AND THE INTERNET § 22 (2010) (citing cases protecting the privacy of computer files and text messages, and also those finding no reasonable expectation of privacy); Robin Miller, *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); Mitchell Waldman, *Expectation of Privacy in Internet Communications*, 92 A.L.R. 5TH 15, §§ 3[a], 3[b] (2001) (citing cases finding expectation of privacy in e-mail message, and those that did not).
[68] O'Conner v. Ortega, 480 U.S. 709 (1987).

issued desk and file cabinets, removing personal items.[69] 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 did not share them and used them to store personal materials.[70] The lack of a policy prohibiting storing personal items was also significant.[71] Yet, *Ortega* demonstrates overall that the right to privacy is basic enough to apply in the workplace and even to private information stored in employer property.

At issue in the more recent *Quon* decision was the intersection of the rights to privacy in the workplace and from electronic surveillance. While the Court did not ultimately decide that an employee has a reasonable expectation in electronic communications made on employer-issued devices, it did so assume.[72] Thus the Constitutionally-protected right to privacy indicates that employee privacy in electronic communications is a basic right deserving of a high level of protection.

2. International Precedent

The basic nature of the right to privacy and its extension to employees is also illustrated by international law. Both the United Nations' Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights[73] recognize privacy as a basic human right. Each states that, "[n]o one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence . . . ."[74]

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.[75] 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

---

[69] *Id*. at 713.

[70] *Id*. at 718 ("We recognize that the undisputed evidence suggests that Dr. Ortega had a reasonable expectation of privacy in his desk and file cabinets.").

[71] *Id*. ("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 . . .").

[72] City of Ontario v. Quon, 130 S. Ct. 2619, 2630 (2010) ("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.").

[73] The United States has not, to date, ratified the convention.

[74] International Covenant on Civil and Political Rights, G.A. Res. 2200 (XXI), art. XVII, U.N. Doc. A/RES/2200(XXI) (Dec, 16, 1966); Universal Declaration of Human Rights, G.A. Res. 217 (III) A, art. XII, U.N. Doc. A/RES/217(III) (Dec. 10, 1948).

[75] 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 33, at 255.

and family life, his home and correspondence."[76] The Charter of Fundamental Rights of the European Union substitutes the term "communications" for the term "correspondence."[77]

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.[78] 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 personal reasons.[79] While in both cases the employer was a public entity, the Convention applies to public and private employers.[80]

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[81] designed to respect the basic right of privacy when processing personal data. A Working Party[82] was established to administer the Directive.[83] The Working Party has issued several detailed documents providing the specific manner in which privacy of employees' electronic communications must be protected.[84]

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.[85]

---

[76] Convention for the Protection of Human Rights and Fundamental Freedoms, art. VIII, ¶ 1, *opened for signature* Nov. 4, 1950, C.E.T.S. No. 005 (entered into force Sept. 3, 1953).
[77] Article 29 Data Protection Working Party, *Working Document on the Surveillance of Electronic Communications in the Workplace 10* (May 29, 2002), *available at* http://ec.europa.eu/justic_home/fsj/privacy/docs/wpdocs/2002/wp55_en.pdf.
[78] Halford v. United Kingdom, 24 Eur. Ct. H.R. 523 (1997).
[79] Copland v. United Kingdom, 45 Eur. Ct. H.R. 37 (2007).
[80] William A. Herbert, *Workplace Electronic Privacy Protections Abroad: The Whole Wide World is Watching*, 19 U. FLA. J.L. & PUB. POL'Y 379, 386 (2008); see also Fred H. Cate, *European Court of Human Rights Expands Privacy Protections: Copland v. United Kingdom*, AM. SOC. INTL. L. INSIGHTS (Aug. 6, 2007), http://www.asil.org/insights070806.cfm.
[81] Council Directive 95/46, 1995 O.J. (L 281) (EC), *available at* http:ec.europa.eu/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf. & at http:ec.europa.eu/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part2_en.pdf.
[82] *Id*. at art. 29.
[83] Some even refer to this Directive as the "Privacy Directive." *See* Herbert, *supra*, note 81.
[84] Article 29 Data Protection Working Party, *Opinion 8/2001 on the Processing of Personal Data in the Employment Context* (Sept. 13, 2001), *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2001/wp48en.pdf; Article 29 Data Protection Working Party, *Working Document on the Surveillance of Electronic Communications in the Workplace* (May 29, 2002), *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2002/wp55_en.pdf.
[85] Richard J. Link, *Postal Service and Offenses against Postal Laws*, 72 C.J.S. POSTAL SERVICE § 79 (May 2010).

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[86] and the protection extends against employers even when an employee's personal mail is delivered to the employer's address.[87] The statute protects against theft of mail,[88] but its protections extend 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.[89] Moreover, the statute creates a misdemeanor offense for any unauthorized person to open or destroy another's mail.[90] On their face, these prohibitions apply in the employment setting to employers who might otherwise read their employees' personal mail.[91] 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.[92] 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 is stated numerous times in the Senate and House reports. [93] Before enactment of the ECPA, the provisions of the Wiretap Act covered only common carriers, and Congress recognized that with changes in technology many

---

[86] 18 U.S.C. §1691 et seq.

[87] 2 MERRICK T. ROSSEIN, 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 violate the statute. *See* 8 ROBERT J. NOBILE, MONITORING EMPLOYEE MAIL, ESSENTIAL FACTS: EMPLOYMENT 13 (2010); Richard A. Bales & Richard O. Hamilton, *Workplace Investigations in Kentucky*, 27 N. KY. L. REV. 201, 252-53 (2000).

[88] 18 U.S.C. §1708; Link, *supra* note 85, §77

[89] 18 U.S.C. §1702; Link, *supra* note 85, § 80.

[90] 18 U.S.C. §1703; Link, *supra* note 85, § 78.

[91] *See* WILLIAM E. HARTSFIELD, ELECTRONIC AND OTHER SURVEILLANCE METHODS: MAIL COVERS, IN INVESTIGATING EMPLOYEE CONDUCT §6:32 (2010).

[92] 18 U.S.C. §1703; Link, *supra* note 85, § 78.

[93] S. REP. NO. 99-541, at 1 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3555 ("[T]o protect against the unauthorized interception of electronic communications"); S. REP. NO. 99-541, at 3 ("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."); H.R. REP. NO. 99-647, 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."); H.R. REP. NO. 99-647, 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.").

communications system options beyond the common carrier were available.[94] Congress's intent to protect the privacy of individual's electronic communications sent through these other systems, including internal company systems, is clear.[95]

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."[96]

Thus, the basic purpose of the ECPA is to protect individual's privacy in their electronic communications.[97] The legislative history manifests no intent to exclude employees from the

---

[94] S. REP. NO. 99-541, at 1 ("[I]n light of dramatic changes in new computer and telecommunications technologies"); S. REP. NO. 99-541, 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.").

[95] S. REP. NO. 99-541, at 2-3 ("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."); H.R. REP. NO. 99-647, at 17-18 ("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, videotext 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 31 ("As a result of this change, a company whose activities affect interstate commerce and which installs its own private telephone or communication system would have that system covered by the statute."). *See* Baumhart, *supra* note 16, 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."); 132 CONG. REC. H4039-01(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."); *see also* Robert W. Kastenmeier, et al., *Communications Privacy: A Legislative Perspective*, 1989 WIS. L. REV. 715, 739 (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.").

[96] 132 CONG. REC. H4039-01(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 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.").

[97] *See* Baumhart, *supra* note 16, at 926 ("Statements indicative of protecting corporate privacy do not exclude protecting employee privacy, and to some extent protecting corporate privacy from outside hackers serves to protect employee privacy.").

protections of the ECPA.[98] There is no explicit mention of employer monitoring of employees electronic communications in the Senate[99] 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.[100] But before the ECPA amendments, the Wiretap act clearly applied to employers and had been so construed by the courts; nothing indicates that the ECPA was intended to change that reality.[101] 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.[102] There are several instances when certain canons are helpful to discern the meaning of the ECPA. 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;[103] 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 protection.[104] Overall, however, the application of the canons supports an

---

[98] Howard, *supra* note 10, at 512 (2008) ("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."); Droke, *supra* note 16, at 182 (1992) (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."). A statement by an advocate from one organization cannot be taken as determinative of legislative intent. *See* Baumhart, *supra* note 16, at 926 n.19 (citing Ruel Torres Hernandez, *ECPA and Online Computer Privacy*, 41 FED. COMM. L.J. 17, 40 (1988) as 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.").

[99] Baumhart, *supra* note 16, at 926; Gantt, *supra* note 13, at 352.

[100] Baumhart, *supra* note 16, at 926 (citing Senate Report for 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.").

[101] Baumhart, *supra* note 16, 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.").

[102] WILLIAM N. ESKRIDGE, JR., ET AL., CASES AND MATERIALS ON LEGISLATION STATUTE AND THE CREATION OF PUBLIC POLICY 847-48 (Thomson West, 4th ed. 2007).

[103] *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, 401-06 (1950)) ("Hence there are two opposing canons on almost every point.").

[104] *See e.g,.infra* Part V.A.I.a., notes 143-144, and accompanying text discussing courts reliance on the canon suggesting interpreting a statute as a whole to interpret intercept not to include stored communications.

interpretation of the statute that protects employees' basic right to privacy of their electronic communications.

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.[105] The statute should be interpreted as a whole.[106] When comparing similar provisions, differences in drafting indicate differences in meaning.[107] *Expressio unius*: "expression . . . of one thing indicates exclusion of the other."[108]

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.[109] They have also reasoned that "efficiency and productivity levels are at their highest in workplaces that recognize and respect employee privacy."[110] 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[111] and that, for certain employees, monitoring might decrease efficiency.[112]

---

[105] ESKRIDGE, *supra* note 102, at 849 ("Typically, courts will assume that the legislature uses words in their ordinary sense"); NORMAN J. SINGER & SHAMBIE SINGER, SUTHERLAND STATUTORY CONSTRUCTION, § 47:27, 443 (Thomson West, 7th ed. 2007); *see infra* Parts V.A.I.b (interpreting term "intercept") and V.A.I.c.i (interpreting terms "device" and "apparatus").

[106] ESKRIDGE, *supra* note 102, at 862; NORMAN J. SINGER & SHAMBIE SINGER, SUTHERLAND STATUTORY CONSTRUCTION, §46:5, 189-90 (Thomson West, 7th ed. 2007); *see infra* Part V.B.I. (interpreting "stored" in light of interpretation of suggested interpretation "intercept").

[107] *See* ESKRIDGE, *supra* note 102, 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."); *infra* Part V.A.I.b, notes 194—95 and accompanying text (comparing language of different provider exceptions).

[108] *See* ESKRIDGE, *supra* note 102, at 854; NORMAN J. SINGER & SHAMBIE SINGER, SUTHERLAND STATUTORY CONSTRUCTION, §45:14, 134 (Thomson West, 7th ed. 2007); *infra* Part V.A.I.a., note 117 and accompanying text (interpreting intercept to include certain stored communications).

[109] Julie A. Flanagan, Note, *Restricting Electronic Monitoring in the Private Workplace*, 43 DUKE L.J. 1256, 1263 (1994) (citing Michael J. Smith et al., University of Wis.-Madison Dep't of Indus. Eng'g, *Electronic Performance Monitoring and Job Stress in Telecommunications Jobs* 1 (1990) &, Occupational Health & Safety Letter, Electronic Monitoring Blamed for Increased Workplace Stress (June 12, 1991)); Hornung, Note, *supra* note 4, at 124 (2005) (citing Micah Echols, *Striking a Balance Between Employer Business Interests and Employee Privacy: Using Respondeat Superior to Justify the Monitoring of Web-Based, Personal Electronic Mail Accounts of Employees in the Workplace*, 7 COMP. L. REV. & TECH. J. 273, 279 (2003)).

[110] Kopp, *supra* note 16, at 182 (1998) (citing Gantt, *supra* note 13, at 349); *See also* Hornung, *supra* note 4, at 129 (2005) (noting that monitoring may lead to a perceived lack of trust and lower morale causing less efficiency).

[111] John R. Aillo & Kathryn J. Kolb, *Electronic Performance Monitoring and Social Context: Impact on Productivity and Stress*, 80 J. APPLIED PSYCHOL. 339, 349 (1995) (testing 202 undergraduate students in a laboratory setting and finding that monitored subjects felt higher stress levels); Pascale Carayon, *Effects of Electronic Performance Monitoring on Job Design and Worker Stress: Results of Two Studies*, 6 INT'L J. HUM.—COMPUTER INTERACTION 177, 185, 186 (1994) (discussing studies by self-reporting of 171 clerical office workers

V. The Electronic Communications Privacy Act

The ECPA is divided into parts, two of which are relevant to the protection of privacy of employee's electronic communications.[113] Title I prohibits intentional interception of electronic communications[114] 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 damages[115] and is subject to an interpretation that provides for more limited exceptions to liability than the SCA,[116] 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.[117]

---

and 745 telecommunications workers finding monitoring increased physical discomfort for both groups and telecommunication workers had increased mental stress).

[112] Aillo, *supra* note 111, at 347 (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).

[113] Title III addresses pen registers and trap and trace devices.

[114] 18 U.S.C. § 2511 (1)(a) (2008) ("intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication."). ECPA also provides punishment for disclosure and use of such intercepted communications. 18 U.S.C. § 2511 (1)(b)-(d) (2008). *See also* 18 U.S.C. § 2511 (4)(a)(2008) (providing for some exceptions from punishment or difference in type of punishment).

[115] 18 U.S.C. § 2520 (c)(2)(2001) (providing for greater of actual damages and profits or statutory damages of $100 a day of violation up to $10,000); 18 U.S.C. § 2707 (c)(2002) (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.'"). 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, Lmtd., 560 F.3d 199 (4th Cir. 2009). But other lower courts have held differently. *Id*. at 206.

[116] Compare *infra* Part V.A.2.b (Wiretap provider exception) to Part V.B.3.a. (SCA provider exception).

[117] 18 U.S.C. § 2511 (1)(b)-(d)(2008). In § 2702, the SCA does place restrictions on disclosure by entities providing "services 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. 99-647at 48. 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 17, at 98. And in some employment law contexts, such as suits for the tort of public disclosure of embarrassing private facts, the public has been found to encompass employees. *See e.g.*, Miller v. Motorola, Inc., 560 N.E.2d 900, 903 (Ill. App. 1990). Nevertheless, § 2702 likely will be found by the courts only to apply to services such as AOL or Yahoo or to companies that perform word processing and storage, like cloud computing, for individuals or another company. Indeed, one court has "declared the word ["public"] unambiguous and applied

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 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."[118]

Contents "include[] any information concerning the substance, purport, or meaning of that communication."[119] 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.[120] While at first glance an interpretation 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.[121] An analogy to phone conversations is appropriate;

---

it to mean the community at large, not simply employees." Anderson Consulting LLP v. UOP, 991 F. Supp. 1041, 1042 (N.D. Ill. 1998); Blackowicz, Note, *supra* note 17, at 98.

[118] 18 U.S.C. § 2510 (4) (2008).

[119] 18 U.S.C. §2510(8) (2008).

[120] Myrna L. Wigod, *Privacy in Public and Private E-Mail and On-Line Systems*, 19 PACE L. REV. 95, 113 (1998) (contents does not include e-mail title headers); Blackowicz, Note, *supra* note 17, 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 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 27, at 479 ("Thus, it remains to be seen whether or not tracking of addressees alone works a statutory 'interception.'").

[121] *See infra* Parts V.A.2.b, discussing provider exception, and section, V.A.2.c, discussing ordinary course of business exception.

generally when an employer hears a personal call, the employer must stop monitoring or it violates the Wiretap Act.[122]

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.[123] 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.[124] To do otherwise renders the protection of the Wiretap Act generally inapplicable to e-mail and text messaging use 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,[125] and 5) while being stored by the recipient for a reasonable time period after opening the communication necessary to insure 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 insure that the employer was not engaging in the practical equivalent to an interception by simply waiting to retrieve the received, stored, but not yet deleted communication .[126] This latter period should include the time in which the employer-provided equipment acquires and records the communication.[127]

---

[122] *See infra* Part V.A.2.c.

[123] 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).

[124] Blackowicz, *supra* note 17, 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.").

[125] Hall v. Earthlink Network, Inc., 396 F.3d 500, 504 n.1, 505 (2d Cir. 2005) (suggesting service providers continued receipt constitutes an interception, unless it falls within the ordinary course of business exception).

[126] Kerr suggests that "when 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 intercepted. Kerr, *supra* note 3, 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.

[127] *See* Shefts v. Petrakis, 2010 U.S. Dist. LEXIS 129974, at * 19 (C.D. Ill. Dec. 9, 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 applies to any claim involving a computer that records a message sent on that computer).

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. Nothing in the language of the definition indicates that stored communications are somehow exempt from acquisition.[128] The definition of electronic communications excludes various communications but does not exclude stored communications.[129] Thus, on its face, the Wiretap Act includes interception of stored electronic communications.[130]

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.[131] 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.[132] Employers can easily acquire the 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 *Councilman*, while not an employment case, is instructive on why the term intercept should be interpreted to include stored communications.[133] 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."[134] His company provided e-mail service to book dealer customers.[135] His IT department arranged to intercept all e-mails from Amazon.com to the dealers before delivery to the recipient.[136] The intercepted e-mails were copied, and the copy was placed "in a separate mailbox that

---

[128] 18 U.S.C. § 2510 (4)(2008).
[129] 18 U.S.C. § 2510 (12)(2008).
[130] United States v. Szymuszkiewicz, No. 07-CR-171, 2009 WL 1873657, at *9 (E.D.N.Y. 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.").
[131] *See supra* Part IV.B.
[132] Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 886-87 (9th Cir. 2002) (J. Reinhardt, dissenting) ("Electronic communications spend infinitesimal amounts of time in transmission so by definition, to intercept one, involves obtaining a copy made en route or at the destination.").
[133] *See also id*. at 886-87 (J. Reinhardt, dissenting) (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) *withdrawn 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 (S.D. Ohio Feb. 14, 2007) (relying on the dissent in *Konop* and *Councilman* to adopt the position that interception need not exclude stored communications).
[134] United States v. Councilman, 418 F.3d 67, 70 (1st Cir. 2005).
[135] *Id*.
[136] *Id*.

Councilman could access."[137] He and his employees read the e-mails to try to gain a commercial advantage.[138] 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."[139] The court held that intercepting includes acquiring a communication in "transient electronic storage that is intrinsic to the communication process for such communications."[140] The court first reasoned that a contrary interpretation would require an inferential leap rather than "a plain text reading of the statute."[141] 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.[142]

Several Circuits have, however, interpreted the term intercept to exclude stored communications.[143] They rely primarily on the structure of the ECPA being divided between prohibitions on interception and prohibitions on unauthorized access to stored communications.[144] 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.[145] 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.[146]

---

[137] *Id*.
[138] *Id*. at 70-71.
[139] United States v. Councilman, 418 F.3d 67, 71 (1st Cir. 2005).
[140] *Id*. at 79. *See also* Potter v. Havlicek, No. 3:06-cv-211, 2007 WL 539534, at *7(S.D. Ohio 2007) (stating that *Councilman* is the better reasoned decision).
[141] *Councilman*, 418 F.3d at 73.
[142] *Id*. at 75.
[143] Fraser v. Nationwide Mutual Ins. Co., 352 F.3d 107 (3d Cir. 2004); United States v. Steiger, 318 F.3d 1039, 1049 (11th Cir. 2003); Konop v. Hawaiian Airlines, Inc., 302 F.3d 868 (9th Cir. 2002); Steve Jackson Games, Inc. v. U.S. Secret Serv., 36 F.3d 457 (5th Cir. 1994). Lower courts have also so held, including in some employment cases. Hudson v. Goldman Sachs & Co., 283 A.D.2d 246, 247 (N.Y.S.C. 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"); Wesley College v. Pitts, 974 F. Supp. 375, 384-389 (D. Del. 1997) (discussing how employees could not have intercepted e-mails unless they were in transit and not stored).
[144] *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 definition of stored as including "temporary, intermediate storage.").
[145] 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. H.R. REP. NO. 99-647, 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.").
[146] *See also Konop*, 302 F.3d at 889-90 (Reinhardt, J., dissenting) (reasoning that the SCA provides liability for computer hackers who acquire no content, permits law enforcement to seek contents through service providers rather than through direct wiretapping, and permits a means to police unauthorized access).

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.[147]

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.[148] 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.[149] On the other hand, the definition of electronic communication was added to the Wiretap Act by the ECPA.[150] 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.[151] 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.[152] Thus, interpreting the term intercept to encompass not only acquisition while in transit, but also acquisition for a reasonable

---

[147] 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 Department of Justice objected to the broad definition and desired to obtain e-mail that was sent but in storage pre-delivery with an ordinary search warrant. United States v. Councilman, 418 F.3d 67, 77 (1st Cir. 2005). While addressing some of DOJ's concerns, but not this particular one, Congress "added electronic communications to the Wiretap Act's existing prohibitions on interception of wire communications." *Id.*

[148] *See e.g.*, Fraser v. Nationwide Mutual Ins. Co., 352 F.3d 107, 113(3d Cir. 2004). Relatedly, the Ninth Circuit has asserted that Congress's failure to amend the definition of electronic communication since enactment means the interpretation excluding stored communications has been implicitly approved. Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 878 (9th Cir. 2002). But Congress is a busy body that tends to focus on high publicity or imminent problems, rendering Congress's intent at time of enactment a better indicator of statutory meaning than later inactivity. *See Konop*, 302 F.3d at 891 n.2 (Reinhardt, J., dissenting) (quoting United States v. Price, 361 U.S. 304, 313 (1960)) ("the views of a subsequent Congress form a hazardous basis for inferring the intent of an earlier one").

[149] *Councilman*, 418 F.3d at 78.

[150] *Id*. at 75.

[151] Konop v. Hawaiian Airlines, Inc., 236 F.2d 1035, 1044 (9th Cir. 2001) *withdrawn by* 262 F.3d 972.

[152] *Intercept Definition*, MERRIAM-WEBSTER.COM, http://www.merriam-webster.com/dictionary/intercept (last visited Nov. 11, 2010)("2a: to stop, seize, or interrupt in progress or course of before arrival b: to receive (a communication or signal directed elsewhere) usually secretly."); *Intercept Definition*, THE FREE DICTIONARY.COM BY FARLEX, http://www.thefreedictionary.com/intercept (last visited Nov. 11, 2010)("1. to take, seize, or halt (someone or something on the way from one place to another); cut off from an intended destination: to intercept a messenger 2. to see or overhear (a message, transmission, etc., meant for another): We intercepted the enemy's battle plan."; "To stop, deflect, or interrupt the progress or intended course of" Free Dictionary by Farlex.

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.[153] 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.[154] This would lessen the incentive for employers to provide employees notice of the monitoring policy because of the Wiretap Act's consent requirement.[155] 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,[156] a number of methods currently used by employers to monitor employees' electronic communications will fall within the definition of an interception.[157] Spyware such as Spectorsoft software that acquires electronic communications while in

---

[153] Potter v. Havlicek, 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). 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 16, at 930 n.37 (relying on quoted portion of OTA report to argue that interception need not be simultaneous with transmission).

[154] *See infra* Part V.B.3.a. (discussing SCA provider exception).

[155] *See infra* Part (Wiretap consent exception).

[156] *See* Global Policy Partners v. Yessin, No. 1:09cv85, 2009 U.S. Dist. LEXIS 112472, at *16 (E.D. Va. Nov. 24, 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 also* 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 email use-names and passwords over a time when the communications were not in "flight" is not an intercept).

[157] *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).

transmission[158] and keyloggers that record keystrokes as electronic communications are devised[159] would both run afoul of the Wiretap Acts prohibitions, unless an exception applies.

While some circuit courts have asserted prior to the enactment of the ECPA the term interception had been interpreted to mean contemporaneous acquisition,[160] only one cited circuit decision appears to have so held.[161] There is no indication in the House or Senate reports or in statements on the floor that the legislators were aware of the case.[162] The clarification of the definition of the term wire communication to include stored communications indicates Congress did not agree with the case.[163]

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.[164] 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 insures that an employer's initial acquisition of an electronic communication will constitute an intercept, thereby 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,[165] 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 insure 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

---

[158] Hornung, *supra* note 4, at 152 (2005) (citing Doug Fowler, President of SpectorSoft Corp., speaking about his email monitoring program eBlaster) (The manufacture of one such type of software "has characterized the new software as 'almost a wiretap.'"). 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 (D. Ct. App. Fl. 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.").

[159] *See, e.g.*, Brahama v. Lembo, No. C-09-00106 RMW, 2009 WL 1424438 (N.D. Ca. May 20, 2009).

[160] *See, e.g.*, Steve Jackson Games, Inc. v. U.S. Secret Service, 36 F.3d 457, 462 (5th Cir. 1994).

[161] United States v. Turk, 526 F.2d 654 (5th Cir. 1976).

[162] Konop v. Hawaiian Airlines, Inc., 236 F.2d 1035, 1046 (9th Cir. 2001) *withdrawn by* 262 F.3d 972 (9th Cir. 2001) ("The Fifth Circuit case that adopted the contemporaneity requirement had not been widely adopted by other courts when Congress passed the ECPA.").

[163] 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.

[164] 18 U.S.C. § 2703(a) (2009).

[165] *Id*.

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.[166] The exception has been and should be interpreted to require knowing assent to monitoring.[167] 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 acknowledgement forms and electronic notices to try to insure employees are aware of the monitoring and the policies.

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.[168] 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 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

---

[166] 18 U.S.C. § 2511 (2)(e) (2008) ("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.

[167] *See, e.g.*, Jandak v. Village 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.").

[168] Article 29 Data Protection Working Party, *Opinion 8/2001 on the Processing of Personal Data in the Employment Context* (Sept. 13, 2001), *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2001/wp48en.pdf.

situations where they "should have known"[169] they were monitored or based on law, such as an employer's property right in an employer-issued computer.[170] 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.[171] 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,[172] several decisions dealing with the similar user authorization exception under the SCA do adopt an interpretation of consent similar to the European view.[173] For instance, in one case, managers accessed a chat group which was by invitation only and required a password.[174] 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 would not have given him the password if he had not been a manager.[175] The jury could infer that she was pressured or coerced into providing the password and as such did not authorize the use.[176]

Absent the likelihood 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.[177] 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

---

[169] *Jandak*, 520 F. Supp. at 820 n.5 (Consent will not be implied by law, "if the party reasonably should have known.").

[170] *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 where, 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 is she continued to use the phone for personal calls).

[171] *See* Chivvis, *supra* note 12 (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).

[172] 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.

[173] *See e.g.*, Pure Power Boot Camp. v. Warrior Fitness Boot Camp., 587 F. Supp. 2d 548, 552 (S.D.N.Y. 2008) (requiring that employee have opportunity to refuse or withdraw consent to monitoring); *see infra*Part VI.B.3.b (user authorization section).

[174] Pietrylo v. Hillstone Restaurant Group, No. 06-5754 (FSH), 2009 WL 3128420, at *1 (D.N.J. Sept. 25, 2009).

[175] *Id*. at *3.

[176] *Id*.

[177] 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 . . . .").

conduct.[178] While a requirement of express consent would be most protective of employees' rights, the legislative history to the original Wiretap Act manifests Congress' intent that consent may be implied, at least in limited circumstances.[179] These circumstances should be extremely limited in the employment context, due to the general imbalance in power between the parties.[180]

Few employment cases address the issue of consent to interception of electronic communications,[181] 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.[182] On the other hand, other pre-ECPA courts, most notably the Second Circuit,[183] 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

---

[178] *See e.g.*, *id*. at 117 (holding that when landlord told a lodger she was recording all calls, he had impliedly consented to her listening to one of his calls).

[179] 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) (emphasis added)). ("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.'"); Jandak v. Village 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). 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. Levinson, *supra* note 25, at 652; Ciocchetti, *supra* note 32.

[180] 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 prison setting); Briggs v. Am. Air Filter Co., 630 F.2d 414 (5th Cir. 1980) (suggesting that cases involving domestic disputes are not helpful in applying the ordinary course of business exception in employment setting).

[181] 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 (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).

[182] Hay v. Burns Cascade Co., Inc., No. 5:06-CV-0137 (NAM/DEP), 2009 WL 414117 at * (N.D.N.Y. Feb. 18, 2009) ("Implied consent should not be casually inferred and may be limited."); In re Pharmatrack, Inc., 329 F.3d 9, 20 (1st Cir. 2003) ("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 title 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. . . .).

[183] United States v. Amen, 831 F.2d 373, 378 (2d Cir. 1987) (relying on S. REP. NO. 90-1097 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2182 providing for implied consent)).

cases have been based on facts that illustrate that the person monitored knew the monitoring was taking place and assented to it.[184]

Knowledge of monitoring requires notice that the monitoring is actually taking place.[185] One First Circuit case illustrates this principle.[186] The defendants, agents of the employer, set up a system "for electronically monitoring employee phone calls."[187] The system was meant to reduce the cost of telephone bills and to decrease employee theft.[188] The defendants informed all the managers that telephone calls "would be subject to random monitoring and recording" and instructed them to inform their subordinates.[189] Employees were also directed "to record long distance phone calls on provided telephone logs."[190] 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.[191] The court also found that the district court did not err by determining that he did not know.[192] Without that level of minimal knowledge, the court concluded, consent cannot be inferred.[193]

---

[184] 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. First, the Code of Federal Regulations provides notice "of the possibility of monitoring." Second, inmates received actual notice because the monitoring and taping system was discussed at an admission and orientation lecture. Third, the inmates received actual notice because the inmate handbook stated, "[t]hese phones utilized by the inmates are MONITORED and TAPED . . . ." 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." 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*. at 379. *See also, e.g*., Sporer v. UAL Corp., 2009 WL 2761329 (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 o.k. 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).

[185] 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.").

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

[187] *Id*. at 275.

[188] *Id*.

[189] *Id*.

[190] *Id*. at 276.

[191] Williams v. Poulos, 11 F.3d 271, 281-82 (1st Cir. 1993).

[192] *Id*. at 282.

[193] *Id*.

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.[194] One non-employment case is illustrative of this approach. The defendant argued that his wife had consented to him accessing her electronic communications. The defendant gathered the electronic communications from a computer that his wife knew he could access.[195] His wife used a "remember me" feature on her e-mail account despite knowing the defendant had access to the computer.[196] 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.[197] The court interpreted consent not to include constructive consent, but rather to include implied consent.[198] 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.[199] 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.[200]

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.[201] 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.[202] 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.

---

[194] *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) ("consent 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.").
[195] Potter v. Havlicek, No. 3:06-cv-211, 2007 WL 539534, at *8 (S.D. Ohio Feb. 14, 2007).
[196] *Id*.
[197] *Id*.
[198] *Id*. at *8.
[199] *Id*. at *9.
[200] *See* Pure Power Boot Camp v. Warrior Fitness Boot Camp., 587 F. Supp. 2d 548, 552 (S.D.N.Y. 2008) (discussed in detail *infra* Part V.B.II.B.).
[201] *Contra* Hornung, Note, *supra* note 4, at 129 (2005) (Hornung, who despite acknowledging that some courts hold that "consent 'is not to be cavalierly implied," advocates that "in the email context the sender knows that the nature of sending an email is that a record of it can be downloaded, printed, saved, and stored on the company email system. Accordingly, by the act of sending an email via the Internet, the sender 'expressly consents by conduct to the recording of the message.'").
[202] Bohach v. City of Reno, 932 F. Supp. 1232, 1236 (D. Nev. 1996).

Additionally, notice of one type or method of monitoring should not indicate consent to a different type or method of monitoring. Several cases illustrate this principle.[203] For instance, in *Dukes v. ADS Alliance Data Systems, Inc.*,[204] 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."[205] 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.'"[206] The plaintiff had signed two consent forms. The consent form stated the employer would periodically record phone calls between employees and customers.[207] Employees could also use the phones for a minimal amount of personal use.[208] There were also pay phones available to use for personal calls.[209] Supervisors listened to two of the plaintiff's personal calls with her husband where she discussed work-related incidents.[210] The court held that the acknowledgments signed by the plaintiff did not express consent to monitoring of personal calls.[211] The policy and acknowledgments provided for monitoring of calls with customers whereas these supervisors decided to monitor knowing that the plaintiff was speaking with her husband.[212] The court determined that she had consented only to a more limited monitoring, that of periodic monitoring of calls with customers.[213] By analogy, if an employee has consented to monitoring of business-related e-mail that does not constitute consent to 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 the call by extension phone. The prison relied on the common practice to monitor such calls by having a guard actually listen to what the inmate was saying. 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." 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

---

[203] *See e.g.*, In re Pharmatrak, 329 F.3d 9, 20 (1st Cir. 2003) (consent to collect certain data did not provide consent to collect web page visitors personal data).
[204] Dukes v. ADS Alliance Data Sys., Inc., No. 2:03-CV-00784, 2006 WL 3366308 (S.D. Ohio 2006).
[205] *Id*. at *4.
[206] *Id*.
[207] *Id*.
[208] *Id*.
[209] Dukes v. ADS Alliance Data Sys., Inc., No. 2:03-CV-00784, 2006 WL 3366308, at *4 (S.D. Ohio 2006).
[210] *Id*.
[211] *Id*.at *12. *See also* Watkins 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).
[212] *Dukes*, 2006 WL 3366308, at *12.
[213] *Id*. at *13.

consent."[214] The court summarily held this did not amount to implied consent.[215] 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,[216] courts should consider not only employer's promulgated policies but also 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.[217] 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.[218]

b. Provider Exception

Another exception exempts providers from the prohibition on interception in specified circumstances.[219] 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 insure that the

[214] Campiti v. Walonis, 611 F.2d 387, 393 (1st Cir. 1979).
[215] *Id*. at 394.
[216] Jandak v. Village 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.").
[217] Ciocchetti, *supra* note 32.
[218] Levinson, *supra* note 25, at 652.
[219] 18 U.S.C. §2511(2)(a)(i) (2008).

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. Second, the interception must take place "in the normal course of" employment. 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."[220] Very similar language is used in one provider exception in the SCA[221] whereas broader language that simply exempts conduct authorized by a provider is used in another section of the SCA.[222] 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[223] or even broadly to protect against monetary loss[224] 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.[225] For instance, the Senate Report in related discussion mentions monitoring "to

---

[220] 18 U.S.C. §2511(2)(a)(i) (2008) (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 . . .").

[221] 18 U.S.C. §2702(b)(5) (2008) (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.").

[222] 18 U.S.C. §2701(c)(1) (2008) (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.

[223] Ideal Aerosmith, Inc. v. Acutronic USA, Inc., No. 07-1029, 2007 WL 4394447, at *4, *6 (E.D. Pa. Dec. 13, 2007) (company that bought another company at bankruptcy and continued to receive e-mails intended for prior employees, transferred them to its server, and reviewed them thereby obtaining competitor's confidential information fell within the provider exception as successor-in-interest).

[224] Schmidt v. Ameritech Illinois, 329 Ill. App. 3d 1020, 1025, 1033-34 (Ill. Ct. App. 2002) (reasoning that the exception extends to protection against any monetary loss).

[225] *Cf.* Chivvis, *supra* note 12 (critiquing a decision for failing to incorporate a legitimate business interests test into the provider exception); Droke, Comment, *supra* note 16, at 182 (1992) (suggesting the courts could use a strict business interest test pursuant to the provider exception). *But see* Gruber & Maltby, *supra* note 5, at 44 (private employers will be exempt from ECPA liability as long as they are the provider of the electronic system); Newman & Crase, *supra* note 19, (suggesting that the exception is broad); *see also* Hash & Ibrahim, *supra* note 10, 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 4, at 138 (2005) (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, Comment, *supra* note 16, at 872 (1998) (suggesting based on unpublished California trial level court decision that employer-providers are exempt even if they read everything on the system); Anne L. Lehman, Comment, *E-mail in the Workplace: Question of Privacy, Property or Principle?*, 5 COMMLAW

properly route, terminate, or otherwise manage . . . individual messages."[226] 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."[227]

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.[228] 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 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 insure the proper working of the electronic communications system, others certainly are not.[229] 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.[230] 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

---

CONSPECTUS 99, 102 (1997) (suggesting exception be broadly interpreted to include "the owner and operator of a private network-such as within a company").

[226] 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. S. REP. NO. 99-541, at 20 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3574.

[227] Beeson, *supra* note 16, at 189.

[228] *See* Berry v. Funk, 146 F.3d 1003, 1010 (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").

[229] 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 13, 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 16, at 193 (suggesting that the courts should "require employers to limit their monitoring to the message's address").

[230] *Cf.* Blackowicz, Note, *supra* note 17, at 98 (suggesting "the argument that personal information in employee e-mail messages is related to a business interest seems unlikely to succeed.") (discussing similar language in the SCA, 18 U.S.C. §2702(b)(5) (2008)).

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.[231] Interceptions necessary to protect against those threats should fall within the exception.[232] 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 protect against those threats should not fall within the exception.[233] 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 in any circumstances 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.[234] The common understanding of an agent does not extend to a subscriber to another's communications service, and such a broad interpretation

---

[231] 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").

[232] *See* Kaplan, *supra* note 10, at 297 (relying on Beeson, *supra* note 16, to suggest that "courts are likely to allow employer-providers to monitor, but only when employing the least intrusive means possible.").

[233] 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. *Cf.* O'Grady v. Superior Court, 139 Cal. App. 4th 1423, (2006) (interpreting 18 U.S.C. §2702(b)(5) (2008), 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). *But see* Kinesis Adver., Inc. v. Hill, 652 S.E.2d 284, 297, 18 (N.C. Ct. App. 2007) (reviewing a past employees' business-related correspondence for support for claims of breach of covenant not to compete and related claims falls within the exception for protecting rights and property); Freedom Calls Found. v. Bukstel, No. 05CV5460(SJ)(VVP), 2006 WL 845509 (E.D.N.Y. Mar. 3, 2006) (employer can intercept former employee's e-mails to "ensure that current and prospective" client's "email messages are answered in a timely fashion); Alexander I. Rodriquez, Comment, *All Bark, No Byte: Employee E-Mail Privacy Rights in the Private Sector Workplace*, 47 EMORY L.J. 1439, 1451 (1998) ("Presumably, a private provider could always justify an intrusion into employee communications to protect against breaches of confidentiality, trade secret theft, or system maintenance.").

[234] Baumhart, *supra* note 16, 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 and Maltby, *supra* note 5, at 44 (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"); Rodriquez, Comment, *supra* note 233, at 1452 ("At a minimum, the provider exception should not be able to be utilized by employers who furnish networks through public providers.").

would be contrary to the legislative intent and the basic nature of employees' privacy.[235] 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.[236] Additionally, the exception 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.[237] The definition of intercept requires acquisition through a device,[238] and a device is defined to exclude certain equipment used in the ordinary course of business.[239]

As to many interceptions by employers of electronic communications, the exception should not apply because it requires the use of telephone or telegraph equipment.[240] 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.[241] One exception is for "any telephone or telegraph instrument, equipment or facility" being used in the "ordinary course of business."[242]

---

[235] *But see* Lehman, Comment, *supra* note 225, at 102-103 (1997) (suggesting that when public network is the provider, a subscribing employer should constitute an agent and fall within the exception); *see also* Hash & Ibrahim, *supra* note 10, 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.").

[236] *Cf.* McClelland v. McGrath, 31 F. Supp. 2d 616, 619 (N.D. Ill. 1998) (phone company motivated by desire to help officers with kidnapping investigation was not protecting its own property).

[237] Deal v. Spears, 980 F.2d 1153, 1157 (8th Cir. 1992) (states really a "restrictive definition").

[238] 18 U.S.C. § 2510 (4) (2002) ("'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.").

[239] 18 U.S.C. § 2510 (5)(a) ("'electronic, mechanical, or other device' means 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 . . .").

[240] 18 U.S.C. § 2510 (5)(a); Lieutenant Colonel LeEllen Coacher, *Permitting Systems Protection Monitoring: When the Government Can Look and What It Can See*, 46 A.F.L. REV. 155, at 175 (1999) ("The third exception, often called the telephone extension exception, does not apply to computer-based communication.").

[241] 18 U.S.C. § 2510 (5)

[242] 18 U.S.C. § 2510 (5) (a).

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.[243] The plain language is easily susceptible to such an interpretation and limiting the exception narrowly to telephone or telegraph equipment provides a high level of protection for the privacy of employees' electronic communications.[244] Indeed, the legislative history indicates that the Senate understood the term 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.[245]

Moreover, even pre-ECPA courts interpreted the exception narrowly to apply only to telephone and telegraph equipment. [246] 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.[247] The recordings were erased weekly. 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."[248]

---

[243] Court & Warmington, *supra* note 10, at ("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 11, at 901 (1996) ("The first provision has been relied upon in telephone extension monitoring cases, but may not pertain to E-mail monitoring unless telephone equipment or facilities are specifically involved."); Lori E. Lesser, *Social Networks and Blogs*, 1001 PLI/PAT 101 (April-May 2010) (stating that the business use exception in 2510(5)(a) does not apply to e-mail); Lee, *supra* note 13, 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."); Lisa Smith-Butler, *Workplace Privacy: We'll Be Watching You*, 35 OHIO N.U. L. REV. 53, 67 n.128 (2009) (noting that the ordinary course of business exception has been applied only to telephone monitoring and not extended to e-mail);; White, *supra* note 10, 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.").

[244] *See* Blackowicz, *supra* note 17, at 103 (arguing that to protect the privacy of employee's e-mail, computers should not constitute "an excepted interception device.").

[245] S. REP. NO. 99-541, at 13 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3567 (The report indicates 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.).

[246] United States v. Murdock, 63 F.3d 1391, 1396 (6th Cir. 1995) (holding that a recording mechanism is not telephone equipment); Beeson, *supra* note 16, 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.").

[247] Sanders v. Robert Bosch Corp., 38 F.3d 736, 737 (4th Cir. 1994).

[248] *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.*, Sanders v. Robert Bosch Corp., 38 F.3d 736, 740 (4th Cir. 1994), Deal v. Spears, 980 F.2d 1153, 1158 (8th Cir. 1992), or the telephone extension that intercepts, *see, e.g.*, United States v. Harpel, 493 F.2d 346, 351 (10th Cir. 1974), Epps v. St. Mary's Hosp., 802 F.2d 412, 415-16 (11th Cir. 1986), there is no dispute in the circuit courts that a recorder would not constitute telephone equipment. *But see e.g.*, Dillon v. Mass. Bay Transp. Auth., 729 N.E.2d 329, 335 (2000) (holding that recorder is telephone equipment); In re State Police

Thus, courts that construe the terms "telephone" and "telegraph" not to modify equipment and facility unnecessarily undermine the employees' basic right to privacy.[249] 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.[250] The court then reasons that the legislative history exhibits an intent to include ISP providers. The court reasons that the legislature understood e-mail to be transmitted over telephone lines because that was the only technology available in 1986. 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. Yet, as discussed above, the legislative history indicates Congress did use the term "telephone" to modify the term "equipment."[251] 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 "device" not to include a computer[252] have

---

Litigation, 888 F. Supp. 1235, 1265 (D. Conn. 1995) (holding recording equipment constituted telephonic components).

[249] *But see* Newman & Crase, *supra* note 19 (reading exception to apply to "any equipment or component used in the ordinary course of business"); Hornung, *supra* note 4, at 138 (asserting that company email system is a "component used in the ordinary course of business" and, thus, not "an electronic device for the purpose of the statute."); Rodriquez, *supra* note 233, at 1452-53 (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").

[250] Hall v. Earthlink Network, Inc., 396 F.3d 500, 504 (2d Cir. 2005).

[251] *See supra* note 245 and accompanying text. *Cf.* Beeson, *supra* note 16, at 184-85 (arguing that 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.").

[252] Modrowski v. Pigatto, No. 09 C 7002, 2010 WL 2610656 (N.D. Ill. June 25, 2010) (employer who opened former employee's email account did not use a device); Conte v. Newsday, Inc., No 06-CV-4859 (JFB) (ETB), 2010 U.S. Dist. LEXIS 28502, at *31 (E.D.N.Y. Mar. 25, 2010) (dicta stating 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, Comment, *supra* note 225, at 102 ("It is unclear from this definition whether a modem, software, or the specific computer system or organization used by the

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,[253] pager, or handheld device[254] or a keylogger or spyware program.[255] 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 requirement before falling within the exception for ordinary course of business.[256] Indeed, the exception requires that the equipment be used in the ordinary course of business.[257] Because the term "ordinary course of its business" is not defined, many telephone wiretap cases have addressed the exception,[258] including a number dealing with employer monitoring of employees.

---

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.").

[253] United States v. Szymuszkiewicz, No. 07-CR-171, 2009 WL 1873657, at * (E.D. Wis. 2009) (holding statutory definition of term "device" is broad enough to include two computers).

[254] Commonwealth v. Cruttenden, 976 A.2d 1176 (Sup. Ct. Pa. 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).

[255] Device is defined in the following ways: "[A] plan, procedure, technique . . . a piece of equipment or mechanism designed to serve a special purpose or perform a special function [i.e.] 'an electronic device'" *Device Definition*, MERRIAM-WEBSTER.COM, http://www.merriam-webster.com/dictionary/device (last visited Dec. 29, 2010); "A contrivance or an invention serving a particular purpose, especially a machine used to perform one or more relatively simple tasks . . . a technique or means," *Device Definition*, THE FREE DICTIONARY.COM BY FARLEX, http://www.thefreedictionary.com/device (last visited Dec. 29, 2010). Apparatus is even more broad being defined in the following ways: "1. a group or combination of instruments, machinery, tools, materials, etc., having a particular function or intended for a specific use[, i.e. o]ur town has excellent fire-fighting apparatus 2. any complex instrument or mechanism for a particular purpose," *Apparatus Definition*, DICTIONARY.COM, http://dictionary.reference.com/browse/apparatus (last visited Dec. 29, 2010); "1.a. a set of materials or equipment designed for a particular use . . . c. an instrument or appliance designed for a specific operation," *Apparatus Definition*, MERRIAM-WEBSTER.COM, http://www.merriam-webster.com/dictionary/apparatus (last visited Dec. 29, 2010); "1.a. [a]n appliance or device for a particular purpose b. An integrated group of materials or devices used for a particular purpose," *Apparatus Definition*, THE FREE DICTIONARY.COM BY FARLEX, http://www.thefreedictionary.com/apparatus (last visited Dec. 29, 2010).

[256] Beeson, *supra* note 16, at 175 ("The first relevant exception to the ECPA is commonly known as the 'business – extension,' 'business use,' or 'ordinary course of business exception.'").

[257] 18 U.S.C. § 2510(5) (2008) ("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.").

[258] 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).

The exception should be interpreted to require an employer to act in a routine manner with a legitimate business purpose[259] and to provide notice to the employee of the monitoring. [260] 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.[261]

One Sixth Circuit case illustrates the proposed approach to interpreting the term "in its ordinary course of business." [262] 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."[263] 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.'"[264] It determined that while actual consent is not required, notice is required.[265] 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."[266] 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."[267] It further reasoned that the plaintiff did not impliedly consent to the interceptions "simply because he accepted and

[259] 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 4, at 151-52 (2005). 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 email in a routine manner because of a legitimate business concern and with notice to employees.

[260] 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.").

[261] 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 19, this proposal synthesizes both approaches by using a "context approach" with an additional requirement that further limits the monitoring of personal electronic communications.

[262] Adams v. City of Battle Creek, 250 F.3d 980, 982 (6th Cir. 2001).

[263] *Id*. at 984.

[264] *Id*.

[265] *Id*.

[266] *Id*.

[267] Adams v. City of Battle Creek, 250 F.3d 980, 984 (6th Cir. 2001).

used a department-issued pager."[268] A policy prohibiting personal use of employer issued equipment does not constitute the necessary notice.[269] 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."[270]

The requirement that the monitoring be routine necessitates that the monitoring must be the type normally engaged in by the employer.[271] 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.[272] By analogy, an employer who normally uses keyword searches to determine whether employees are sending pornographic 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.[273]

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.[274] *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.[275] 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."[276] But recording

[268] *Id*.
[269] *Id*.
[270] *Id*.
[271] *But see* Epps v. St. Mary's Hosp., 802 F.2d 412, 417 (11th Cir. 1986) (holding that co-employee who recorded call between two other employees who were making negative remarks about a supervisor and another employee acted within the ordinary course of business).
[272] Campiti v. Walonis, 611 F.2d 387, 392 (1st Cir. 1979).
[273] 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.
[274] *See* Sanders v. Robert Bosch Corp., 38 F.3d 736, 743 (4th Cir. 1994). The court held that a voicelogger 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 743. 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.
[275] Deal v. Spears, 980 F.2d 1153, 1158 (8th Cir. 1992).
[276] *Id*.

for twenty-two hours and listening to all the calls was not in the ordinary course of business. The suspicions did not "justify the extent of the intrusion."[277] 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.

The notice requirement insures that employers provide sufficient notice of the type of monitoring being engaged in that employees should know of the monitoring.[278] Many cases will be relatively clear-cut because employees have actual notice of the monitoring[279] or because the employer has failed to provide the employees any notice of monitoring.[280] Some cases, however, will involve an employer who has provided notice, despite an employees' claim of lacking knowledge of the monitoring. The notice requirement insures that in such cases an employer must have made such 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.[281] 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.[282] 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."[283]

---

[277] *Id*.

[278] *But see* Arias v. Mut. Cent. Alarm Serv. Inc., 202 F.3d 553, 559 (8th 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).

[279] James v. Newspaper Agency Corp., 591 F.2d 579, 581-82 (10th Cir. 1979) (an employer who provides notice in writing in advance to its employees that it will monitor phone calls for abusive customers and to help train employees on dealing with the public, acts in the ordinary course of business).

[280] Sanders v. Robert Bosch Corp., 38 F.3d 736, 741 (4th Cir. 1994) (Most important to finding a voicelogger 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.").

[281] Jandak v. Village of Brookfield, 520 F. Supp. 815 (N.D. Ill. 1981).

[282] *Id*. at 824.

[283] *Id*. 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," was not the purpose for which the supervisor

The notice requirement serves to protect employees in a manner similar to the consent exception.[284] 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.[285] 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, applying 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 they can modify their 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.[286] 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 when an employer will be unable to stop problematic communications only without notice of monitoring falling outside the provider exception.[287] 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.[288]

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

---

appeared to listen in – personal use and conduct unbecoming. But the case remains a useful illustration of the level of notice required to insure employees' should know of the monitoring.

[284] *See supra* Part V.A.2.a.

[285] *See supra* Part V.A.2.a (discussing imbalance of power making true consent difficult in employment setting).

[286] Adams v. City of Battle Creek, 250 F.3d 980, 992 (6th Cir. 2001) (Krupansky, J., dissenting) (because the consent exception is satisfied when a party receives advance notice of monitoring, requiring notice as part of the ordinary course of business exception renders the consent exception superfluous); Amati v. City of Woodstock, 176 F.3d 952, 955 (7th Cir. 1999)("If there is actual notice . . . there will normally be implied consent," rendering the consent exception superfluous.). *Cf.* Briggs v. Am. Air Filter Co., Inc., 630 F.2d 414, 419 (5th Cir. 1980) (requiring consent in order for the ordinary course of business exception to apply would read the exception out of the statute).

[287] For instance, by having a policy under which employees consent to monitoring for unacceptable pornographic images, sexual terms, or terms that would indicate confidential information is included in a communication, an employer can likely satisfactorily resolve such situations.

[288] *See supra* Part IV.

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.[289] 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.[290] "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."[291]

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 business reason.[292] 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.

---

[289] *See e.g.*, 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."); Cady v. IMC Mortgage Co., 862 A.2d 202, 214 (R.I. Sup. Ct. 2004) (employer listening in on personal conversations was not acting in course of ordinary business); Ali v. Douglas Cable Commc'ns, 929 F. Supp. 1362, 1380 (D. Kan. 1996) (citing to *Watkins* as applying the accepted rule); In re State Police Litigation, 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."); 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.") *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.").

[290] Fischer v. Mt. Olive Lutheran Church, Inc., 207 F. Supp. 2d 914, 923 (W.D. Wis. 2002).

[291] *Id*.

[292] *See supra* Part IV.

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. . ."[293] 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.[294] 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.[295] 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 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.[296] 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

[293]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) (2008) (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 17.

[294] United States v. Ropp, 347 F. Supp. 2d 831 (C.D. Cal. 2004). *See also* Lee, *supra* note 14, 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").

[295] 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.

[296] Epps v. St. Mary's Hospital, 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").

than merely 'affecting' interstate commerce."[297] Indeed, the use of the term "affect" indicates that communications intended for transmission through the Internet or other global systems fall within the requirement.[298]

Moreover, interpreting the interstate commerce requirement less restrictively furthers the legislative intent. The primary intent of the legislation was to protect the privacy of individual's electronic communications, and electronic mail was clearly intended to be protected.[299] 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."[300] 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. 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.[301] 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.[302]

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

---

[297] 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* Brahana v. Lembo, No. C-09-00106 RMW, 2009 WL 1424438 (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).

[298] White, *supra* note 10, at 1088 (stating that 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").

[299] *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 ("The term 'electronic communication' . . .includes electronic mail.").

[300] H.R. REP. NO. 99-647, at 35 (1986). ("The term 'electronic communication' is intended to cover a broad range of communication activities that affect interstate or foreign commerce.").

[301] *Id*. (While in 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.).

[302] *Id*.

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.[303] The SCA remains an important source of protection for communications not covered by the Wiretap Act, such as 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 or for a personal electronic message sent on an employer system provided by 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.[304] 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.

---

[303] 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) (2002). 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) (2002). 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).

[304] There has not been much, if any, controversy over the requirement that a person who accesses a stored communications 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).

1. Electronic Storage

The SCA protects communications that are "in electronic storage."[305] A debate exists over whether the definition of "electronic storage" should be interpreted broadly or narrowly.[306] Once the definition of "intercept" is clarified to include acquisition of certain stored communications, then an equally broad interpretation of the meaning of electronic storage makes sense.[307] 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.[308] The fundamental purpose of protecting employees'

[305] 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).

[306] 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 "back-up" e-mails. *Id*. at 1075. The court reasoned 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 more broad 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).

[307] 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 16, 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").

[308] Jennings v. Jennings, No. 4711, 2010 WL 2813307, at *6 (S.C. App. July 14, 2010) (holding that emails on an internet service provider's servers are stored for the purposes of backup protection); White, *supra* note 10, 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 backup copies because they are the only copy); Flagg v. City of Detroit, 252

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."[309] The intent was to protect these records,[310] specifically including those for backup protection to maintain the system,[311] preserve the integrity of the system,[312] or preserve the property of the user.[313] Congress intended that a wide breadth of stored materials would be covered.[314] 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."[315] 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."[316]

Indeed, several courts have interpreted the definition broadly in the employment context.[317] 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.

F.R.D. 346, 363 (E.D. Mich. 2008) (reasoning that text messages that remain archived, or stored, on the service system are not backup copies because they are the only copy).

[309] [309] H.R. REP. NO. 99-647, at 26 (1986).

[310] S. REP. NO. 99-541, at 3 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3557 (discussing how computers are used to store information for later reference and to ensure system integrity).

[311] 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.").

[312] *Id*. at 22 & n. 34 (discussing how an e-mail provider "may retain copies of transmission and how "e-mail systems are designed to provide access to contents and copies of messages in case of system failure"); H.R. REP. NO. 99-647, at 68 (noting in discussion of different government procedures to access stored communications depending on amount of time stored that "back up protection preserves the integrity of the electronic communications system and to some extent preserves the property of the users of such as system").

[313] *Id*.

[314] *Id*. at 39 (noting the definition is not intended to limit coverage "to any particular medium of storage")

[315] S. REP. NO. 99-541, at 16 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3570.

[316] *Id*. at 35.

[317] *See* 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."); Cardinal Health 414, Inc. v. Adams, 582 F. Supp. 2d 967, 976 n.2 (M.D. Tenn. 2008) (When prior employee continued to read another employee's e-mail, the court reasoned that whether or not the e-mail had been opened, the e-mails remained in electronic storage.); *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, No. C-09-01922 RMW, 2010 WL 1912029, at *8 (N.D. Cal. May 11, 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 backup protection, the e-mails on the employer's server were not in "electronic storage").

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.[318] 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' systems. Either of those actions, if done without authorization, would be a violation of the SCA."[319] 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 "back-up storage."[320]

Some electronic communications, however, will be outside the protections of the SCA either because they are not stored by "an electronic communication service"[321] or because the employer did not access "a facility through which an electronic communication service is provided."[322] 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.[323] While at first glance this appears problematic, recognizing that the employer would

[318] Fischer v. Mt. Olive Lutheran Church, Inc., 207 F. Supp. 2d 914, 925 (W.D. Wis. 2002).
[319] Pure Power Boot Camp v. Warrior Fitness Boot Camp, 587 F. Supp. 2d 548, 555-56 (S.D.N.Y. 2008).
[320] Fraser v. Nationwide Mutual Ins. Co., 352 F.3d 107, 114 (3d Cir. 2004).
[321] 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) (2008).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). *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 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) (email stored on hard drive of personal laptop is not in electronic storage); Hilderman v. Enea Teksci, Inc., 551F. Supp. 2d 1183, 1204 (S.D. Cal. 2008) (E-mails stored on employer issued laptop computer are not stored by an electronic communication service).
[322] 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) (2002). It could be possible to interpret a "provider of an electronic communications service" and "entity providing a . . . 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.
[323] *But see* Devine v. Kapasi, No. 09 C 6164, 2010 WL 2293461, at *4 (N.D. Ill. June 7, 2010) (employer who pleads it stores electronic equipment on its own systems is an electronic communications service for purposes of §2701); Expert Janitorial v. Williams, No. 3:09-CV-283, 2010 WL 908740, at *5 (E.D. Tenn. March 12, 2010)

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 employee's electronic communications.[324]

2. Access and Authorization

The SCA prohibits accessing a facility through which an electronic communication service is provided without authorization.[325] No employment case located by the author discusses the term "access."[326] Generally, the term access should be interpreted broadly for several reasons noted by Orin Kerr.[327] 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."[328] Additionally, due to the rapid rate of technological change, carving out types of interaction would "prove highly unstable and ultimately arbitrary."[329] 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.[330] An employer should be found to have acted "without authorization" or to have "exceeded" authorization when it circumvents a code-based restriction[331] or acts without a legitimate business reason. Scholars

---

(pleading that employer "stored data regarding employee email accounts, user-names, and passwords" sufficient to plead computer is a "facility through which an electronic communication is provided.").

[324] 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 *infra* Part V.A.2.b.

[325] 18 U.S.C. §2701(a).

[326] 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).

[327] Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U.L. REV. 1596, 1647 (2003) (addressing computer misuse statutes and interpreting access to include "any time the user sends a command to that computer that the computer executes").

[328] *Id*. at 1647-48.

[329] *Id*. at 1648.

[330] *See e.g.*, Monson v. Whitby School, Inc., No. 3:09CV1096 (MRK), 2010 WL 3023873 (D. Conn. Aug. 2, 2010) (question of whether employee was authorized to view and delete other employees e-mails is fact-intensive inquiry); Bloomington-Normal Seating Co. v. Albritton, No. 09-1073, 2009 WL 1329123, at *4 (D.C. Ill. May 13, 2009) (discussing that an employee who read manager's e-mail lacked authorization to do so); Borninski v. Williamson, No. Civ.A.3:02CV1014-L, 2005 WL 1206872 (N.D. Tex. May 17, 2005) (reasoning employer was authorized to access employees personal information stored on "company-issued computer hard drive"); Sherman & Co. v. Salton Maxim Housewares, Inc., 94 F. Supp. 2d 817, 821 (E.D. Mich. 2000) ("At a minimum, there must be a clearer and more explicit restriction on the authorized access" to constitute exceeding authorization).

[331] *See* Kerr, *supra* note 327. 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

and courts generally agree that a person who circumvents a code-based restriction, such as by guessing a password to an employee's personal electronic mail, accesses the electronic communications without authorization.[332] That interpretation protects employees' personal structurally protected electronic communications from prying from employers.[333] 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 non-employer provided electronic mail are protected from employers who attempt end-runs around the structural protections. [334]

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.[335] When an employee uses employer issued equipment

---

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) .

[332] *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 Technology Corp. v. Smithson, No. CV 05-1309 DT (RZx), 2006 WL 5668246, at *9 (C.D. Cal. Aug. 14, 2006) (holding company monitored personal email account without authorization) *affirmed in relevant part* 345 Fed. Appx. 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 327, at 1649.

[333] 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) (2008). While 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 (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).

[334] Paul & Chung, *supra* note 10, at ("[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).

[335] *But see* People v. Klapper, 902 N.Y.S.2d 305 (N.Y. City Crim. Ct. April 28, 2010) (holding that, under New York statute that defines authorization, an employee must plead with specificity that the employee and not the

to access electronic communications, those communications may then be stored on the employer's computer, server, or other equipment.[336] While 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;[337] 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 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.[338] The husband had somehow obtained the plaintiff's e-mail password and reviewed messages, some that she had not yet read,[339] once they were in her mailbox. The husband claimed he was authorized to do so because he was a manager of the company.[340] The court, however, declined to grant the husband's motion to dismiss.[341] 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.[342] 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.[343]

---

employer owned a personal e-mail account and that the employee used a password or security device to protect the personal account).

[336] 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.

[337] 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.

[338] Global Policy Partners v. Yessin, No. 1:09cv859, 2009 U.S. Dist. LEXIS 112472, at *1 (E.D. Va. Nov. 24, 2009).

[339] *Id*. at *19.

[340] *Id*. at *9.

[341] *Id*. at *13.

[342] *Id*. at *10. The court relied on cases under the Computer Fraud and Abuse Act, 18 U.S.C. §1030(a) (2008), to so hold.

[343] Global Policy Partners v. Yessin, No. 1:09cv859, 2009 U.S. Dist. LEXIS 112472, at *11 (E.D. Va. Nov. 24, 2009); *See also* KLA-Tencor Corp., No. C-09-01922 RMW, 2010 WL 1912029, at * 9 (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).

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.[344]

a. Provider Exception

The provider exception occurs "with respect to conduct authorized . . . by the person or entity providing a wire or electronic communications service;"[345] 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. [346] Excluding such employers from the exception insures 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 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.[347] 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.[348]

---

[344] 18 U.S.C. §2701(c) (2002). 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.

[345] *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) (2008).

[346] *See* note 234 and accompanying text; Kesan, *supra* note 10, 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 17, 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, 1233, 1234 (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 10, 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).

[347] 18 U.S.C. § 2702 (b)(3) (2008); Quon v. Arch Wireless Operating Co., 529 F.3d 892 (9th Cir. 2008). 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. *Id*. The decision is flawed for several reasons, including that it does not mention that electronic communications service is defined by the act, it 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. *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. *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); *see also* Thayer v. Chiczewski, No. 07 C 1290, 2009 U.S. Dist. LEXIS 84176 (Sept. 11, 2009) (implying that court could order plaintiff in civil suit to consent to disclosure).

[348] *See supra* note 55.

When an employer is the provider of the electronic communications system, [349] such as with an internal electronic mail system, despite the breadth of the exception permitting the employer to authorize anyone, including its own agents, to access the stored communications,[350] the Wiretap Act continues to provide protection. The initial acquisition of the communication is governed by it and by the exceptions which require consent or very limited acquisition without consent under the provider exception.[351]

b. User Exception

The SCA also excepts conduct authorized by a user.[352] The exception raises issues similar to those raised by the consent exception to the Wiretap Act.[353] 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.[354] As noted by one court, carelessness that enables an employer to access an employee's electronic communications does not amount to knowing assent.[355] Additionally, valid authorization is only given when the employee has the opportunity to refuse or withdraw assent to the monitoring[356] and was not pressured into providing the employer a password or assenting to monitoring. [357] Moreover, the authorization should be valid only for the time and purpose and to the extent agreed to.[358]

---

[349] Some scholars have suggested that an employer should not fall within the provider exception. MARK A. ROTHSTEIN & LANCE LIEBMAN, 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, *supra* note 10, 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). *Cf.* Beeson, *supra* note 16, 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 ECPA's reach all types of providers of electronic communication systems, including intra-company systems.

[350] *See* Fraser v. Nationwide Mutual Ins. Co., 352 F.3d 107 (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 (E.D.N.Y. March 3, 2006) (employer can access former employee's stored messages where employer provides ability to send and receive electronic communications).

[351] *See supra* Part V.A.

[352] 18 U.S.C. §2701(c) (2002).

[353] *See supra* Part V.A.2.a.

[354] *See* Pure Power Boot Camp v. Warrior Fitness Boot Camp., 587 F. Supp. 2d 548, 559 (S.D.N.Y. 2008) (The court interpreted 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.").

[355] *Id*. at 561 ("The Court rejects the notion that carelessness equals consent.").

[356] *Id*. at 562 (requiring opportunity to refuse or withdraw consent to monitoring).

[357] Pietrylo v. Hillstone Restaurant Group, No. 06-5754 (FSH), 2009 WL 3128420, at *1 (D.N.J. Sept. 25, 2009) (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 174-176 and accompanying text.

[358] *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-workers e-mail account the password to which was provided by the co-worker

One case nicely illustrates the application of an understanding of user authorization that provides a high level of protection for employees' privacy.[359] 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 webbased Hotmail account.[360] 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."[361] 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. [362]

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."[363]

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

---

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).

[359] 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.* Pure Power Boot Camp. v. Warrior Fitness Boot Camp., 587 F. Supp. 2d 548, 561 (S.D.N.Y. 2008) ("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*. at 561 ("Because [the employee] had a reasonable expectation of privacy in his e-mail accounts, [the employer] could only be authorized to access those accounts if [the employee] had given consent.").

[360] Pure Power Boot Camp, 587 F. Supp. 2d 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.").

[361] *Id*. at 559.

[362] *Id*. at 560.

[363] *Id*. at 561.

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 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. 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.